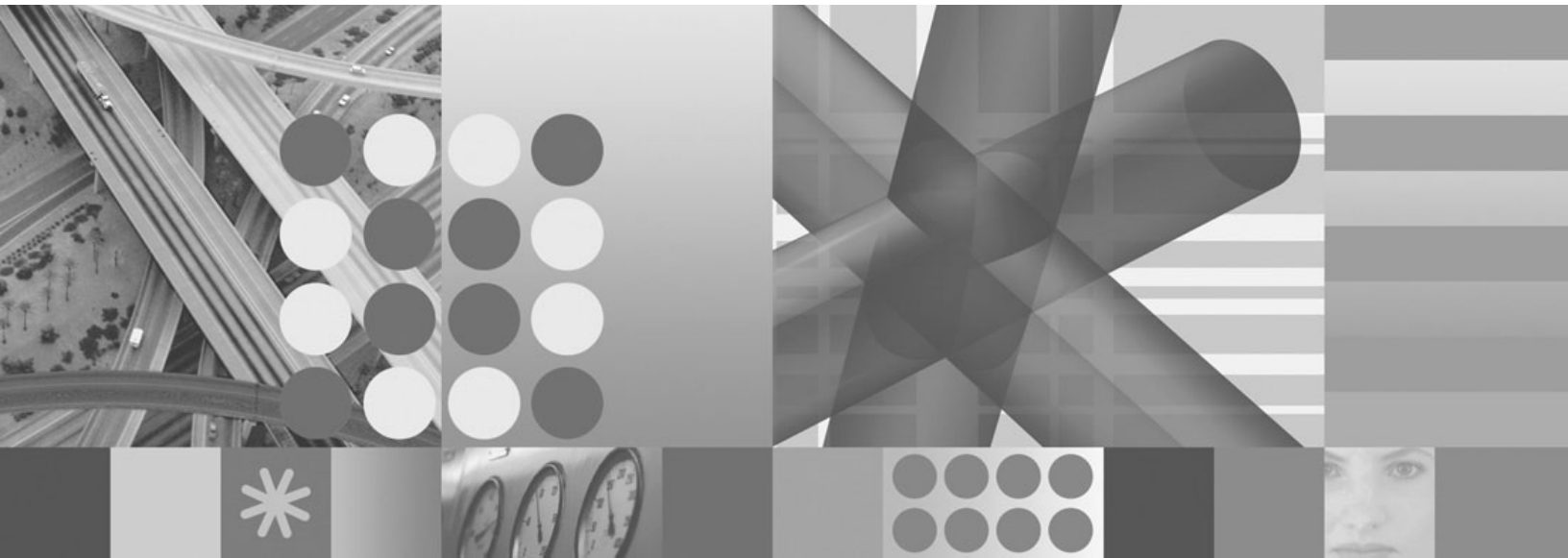




**IBM Tivoli Directory Integrator 6.1.1:  
Reference Guide**





**IBM Tivoli Directory Integrator 6.1.1:  
Reference Guide**

**Note**

**Note:** Before using this information and the product it supports, read the general information under Appendix E, "Notices," on page 519.

**Second Edition (February 2007)**

This edition applies to version 6.1.1 of the IBM Tivoli Directory Integrator and to all subsequent releases and modifications until otherwise indicated in new editions.

© Copyright International Business Machines Corporation 2003, 2007. All rights reserved.

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

---

## Preface

This document contains the information that you need to develop solutions using components that are part of the IBM® Tivoli® Directory Integrator.

---

## Who should read this book

This book is intended for those responsible for the development, installation and administration of solutions with the IBM Tivoli Directory Integrator.

IBM Tivoli Directory Integrator components are designed for network administrators who are responsible for maintaining user directories and other resources. This document assumes that you have practical experience installing and using both IBM Tivoli Directory Integrator, and the reader should be familiar with the concepts and the administration of the systems that the developed solution will connect to. Depending on the solution, these could include, but are not limited to, one or more of the following products, systems and concepts:

- IBM Directory Server
- IBM Tivoli Identity Manager
- IBM Java™ Runtime Environment (JRE) or Sun Java Runtime Environment
- Microsoft® Active Directory
- PC and UNIX® operating systems
- Security management
- Internet protocols, including HTTP, HTTPS and TCP/IP
- Lightweight Directory Access Protocol (LDAP) and directory services
- A supported user registry
- Authentication and authorization
- SAP R/3.

---

## Publications

Read the descriptions of the IBM Tivoli Directory Integrator library and the related publications to determine which publications you might find helpful. After you determine the publications you need, refer to the instructions for accessing publications online.

### IBM Tivoli Directory Integrator library

The publications in the IBM Tivoli Directory Integrator library are:

*IBM Tivoli Directory Integrator 6.1.1: Getting Started*

A brief tutorial and introduction to IBM Tivoli Directory Integrator 6.1.1.

*IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*

Includes complete information for installing the IBM Tivoli Directory Integrator. Includes information about migrating from a previous version of IBM Tivoli Directory Integrator. Includes information about configuring the logging functionality of IBM Tivoli Directory Integrator. Also includes information about the security model underlying the Remote Server API.

*IBM Tivoli Directory Integrator 6.1.1: Users Guide*

Contains information about using the IBM Tivoli Directory Integrator 6.1.1 tool. Contains instructions for designing solutions using the IBM Tivoli Directory Integrator tool (**ibmditk**) or running the ready-made solutions from the command line (**ibmdisrv**). Also provides information

about interfaces, concepts and AssemblyLine/EventHandler creation and management. Includes examples to create interaction and hands-on learning of IBM Tivoli Directory Integrator 6.1.1.

*IBM Tivoli Directory Integrator 6.1.1: Reference Guide*

Contains detailed information about the individual components of IBM Tivoli Directory Integrator 6.1.1 AssemblyLine (Connectors, EventHandlers, Parsers, Plug-ins, and so forth).

*IBM Tivoli Directory Integrator 6.1.1: Problem Determination Guide*

Provides information about IBM Tivoli Directory Integrator 6.1.1 tools, resources, and techniques that can aid in the identification and resolution of problems.

*IBM Tivoli Directory Integrator 6.1.1: Messages Guide*

Provides a list of all informational, warning and error messages associated with the IBM Tivoli Directory Integrator 6.1.1.

*IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*

Includes complete information for installing and configuring each of the five IBM Password Synchronization Plug-ins: Windows Password Synchronizer, Sun ONE Directory Server Password Synchronizer, IBM Directory Server Password Synchronizer, Domino Password Synchronizer and Password Synchronizer for UNIX and Linux®. Also provides configuration instructions for the LDAP Password Store and MQe Password Store.

*IBM Tivoli Directory Integrator 6.1.1: Release Notes*

Describes new features and late-breaking information about IBM Tivoli Directory Integrator 6.1.1 that did not get included in the documentation.

## Related publications

Information related to the IBM Tivoli Directory Integrator is available in the following publications:

- IBM Tivoli Directory Integrator 6.1.1 uses the JNDI client from Sun Microsystems. For information about the JNDI client, refer to the *Java Naming and Directory Interface™ 1.2.1 Specification* on the Sun Microsystems Web site at <http://java.sun.com/products/jndi/1.2/javadoc/index.html>.
- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: <http://www.ibm.com/software/tivoli/library/>
- The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available on the World-Wide Web, in English only, at <http://publib.boulder.ibm.com/tividd/glossary/tivoliglossarymst.htm>

## Accessing publications online

The publications for this product are available online in Portable Document Format (PDF) or Hypertext Markup Language (HTML) format, or both in the Tivoli software library: <http://www.ibm.com/software/tivoli/library>.

To locate product publications in the library, click the **Product manuals** link on the left side of the Library page. Then, locate and click the name of the product on the Tivoli software information center page.

Information is organized by product and includes READMEs, installation guides, user's guides, administrator's guides, and developer's references as necessary.

**Note:** To ensure proper printing of PDF publications, select the **Fit to page** check box in the Adobe Acrobat Print window (which is available when you click **File->Print**).

---

## Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use information technology products successfully. With TDI 6.1.1, you can use assistive technologies to hear and navigate the interface. After installation you also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

### Accessibility features

The following list includes the major accessibility features in TDI 6.1.1:

- Supports keyboard-only operation.
- Supports interfaces commonly used by screen readers.
- Discerns keys as tactually separate, and does not activate keys just by touching them.
- Avoids the use of color as the only way to communicate status and information.
- Provides accessible documentation.

### Keyboard navigation

This product uses standard MicrosoftWindows® navigation keys for common Windows actions such as access to the File menu, copy, paste, and delete. Actions that are unique to TDI use TDI keyboard shortcuts. Keyboard shortcuts have been provided wherever needed for all actions.

### Interface Information

The following points include accessibility features of the TDI 6.1.1 user interface and documentation:

- Steps for changing fonts, colors, and contrast settings in the Config Editor (CE):
  1. Type **Alt-F** to access the CE **File** menu. Using the downward arrow, select **Edit Preferences** and press **Enter**.
  2. Under the **Appearance** tab, select **Theme** settings to change the font.
  3. Under **Theme Colors**, select the colors for the CE, and by selecting colors, you can also change the contrast.
- The TDI 6.1.1 Information Center and its related publications are accessibility-enabled for the JAWS screen reader and the IBM Home Page Reader. You can operate all documentation features using the keyboard instead of the mouse.

### Vendor software

The IBM Tivoli Directory Integrator installer uses the FLEXnet Publisher Installation Module (FNPIM).

### Related accessibility information

Visit the *IBM Accessibility Center* at <http://www.ibm.com/able> for more information about IBM's commitment to accessibility.

---

## Contacting IBM Software support

Before contacting IBM Tivoli Software support with a problem, refer to IBM System Management and Tivoli software Web site at:

<http://www.ibm.com/software/sysmgmt/products/support/>

If you need additional help, contact software support by using the methods described in the *IBM Software Support Handbook* at the following Web site:

<http://techsupport.services.ibm.com/guides/handbook.html>

The guide provides the following information:

- Registration and eligibility requirements for receiving support
- Telephone numbers and e-mail addresses, depending on the country in which you are located
- A list of information you must gather before contacting customer support



# Contents

|  |            |  |    |
|--|------------|--|----|
| <b>Preface</b> . . . . .                             | <b>iii</b> | Examples . . . . .                               | 27 |
| Who should read this book . . . . .                  | iii        | See also. . . . .                                | 27 |
| Publications . . . . .                               | iii        | Direct TCP /URL scripting . . . . .              | 29 |
| IBM Tivoli Directory Integrator library . . . . .    | iii        | TCP . . . . .                                    | 29 |
| Related publications . . . . .                       | iv         | URL . . . . .                                    | 29 |
| Accessing publications online . . . . .              | iv         | Domino/Lotus Notes Connectors . . . . .          | 31 |
| Accessibility . . . . .                              | v          | Session types . . . . .                          | 31 |
| Accessibility features . . . . .                     | v          | Java Class loader issue . . . . .                | 33 |
| Keyboard navigation . . . . .                        | v          | Supported versions of Lotus Notes and Lotus      |    |
| Interface Information . . . . .                      | v          | Domino . . . . .                                 | 33 |
| Vendor software . . . . .                            | v          | Native API call threading. . . . .               | 33 |
| Related accessibility information. . . . .           | v          | The nco.jar file . . . . .                       | 33 |
| Contacting IBM Software support . . . . .            | v          | Domino Change Detection Connector. . . . .       | 35 |
|  |            | Domino Users Connector. . . . .                  | 45 |
|  |            | Lotus Notes Connector . . . . .                  | 57 |
| <b>Chapter 1. Introduction</b> . . . . .             | <b>1</b>   | ITIM DSMLv2 Connector. . . . .                   | 61 |
|  |            | Using the Connector with ITIM Server . . . . .   | 61 |
| <b>Chapter 2. Connectors</b> . . . . .               | <b>3</b>   | HTTPS (SSL) Support . . . . .                    | 61 |
| Connector availability and reference . . . . .       | 3          | Configuration . . . . .                          | 62 |
| Connector Interfaces. . . . .                        | 3          | See also. . . . .                                | 62 |
| Script-based Connectors . . . . .                    | 6          | DSMLv2 SOAP Connector . . . . .                  | 63 |
| Configurations. . . . .                              | 6          | Supported Connector Modes . . . . .              | 63 |
| Connector re-use . . . . .                           | 6          | Extended Operations . . . . .                    | 63 |
| ACT Connector . . . . .                              | 9          | Configuration . . . . .                          | 64 |
| Introduction . . . . .                               | 9          | DSMLv2 SOAP Server Connector . . . . .           | 67 |
| Configuration . . . . .                              | 9          | Extended operations . . . . .                    | 67 |
| Using the Connector . . . . .                        | 11         | Configuration . . . . .                          | 68 |
| Sending a notification from a rule . . . . .         | 11         | Exchange Changelog Connector . . . . .           | 71 |
| Programmatic Interface (API) . . . . .               | 12         | Behavior . . . . .                               | 71 |
| See Also . . . . .                                   | 12         | Using the Exchange Changelog Connector . . . . . | 71 |
| Active Directory Changelog (v.2) Connector . . . . . | 13         | The Is-Deleted attribute in Exchange . . . . .   | 72 |
| Tracking changes in Active Directory . . . . .       | 13         | Accessing the USN synchronization values in the  |    |
| Behavior . . . . .                                   | 15         | User Property Store. . . . .                     | 73 |
| Using the Active Directory Changelog V2              |            | Accessing the runtime Connector's USN            |    |
| Connector . . . . .                                  | 16         | synchronization values . . . . .                 | 74 |
| Configuration . . . . .                              | 16         | Configuration . . . . .                          | 74 |
| Migration from Active Directory Changelog            |            | Migration . . . . .                              | 76 |
| EventHandler to Active Directory Changelog (v.2)     |            | See Also . . . . .                               | 76 |
| Connector . . . . .                                  | 18         | File system Connector . . . . .                  | 77 |
| See also. . . . .                                    | 18         | Configuration . . . . .                          | 77 |
| AssemblyLine Connector . . . . .                     | 19         | See also. . . . .                                | 77 |
| Configuration . . . . .                              | 19         | FTP Client Connector . . . . .                   | 79 |
| Using the Connector . . . . .                        | 20         | Configuration . . . . .                          | 79 |
| Axis Easy Web Service Server Connector . . . . .     | 21         | See also. . . . .                                | 79 |
| Hosting a WSDL file . . . . .                        | 22         | GLA Connector . . . . .                          | 80 |
| Configuration . . . . .                              | 22         | Introduction . . . . .                           | 80 |
| Connector Operation . . . . .                        | 24         | Configuration . . . . .                          | 80 |
| See also. . . . .                                    | 24         | Configuring the TDIOutputter . . . . .           | 80 |
| Btree Object DB Connector . . . . .                  | 25         | Using the Connector . . . . .                    | 81 |
| Configuration . . . . .                              | 25         | Schema. . . . .                                  | 81 |
| Btree object . . . . .                               | 25         | See Also . . . . .                               | 82 |
| Command line Connector . . . . .                     | 26         | HTTP Client Connector . . . . .                  | 83 |
| Native-encoded output on some operating              |            | Modes . . . . .                                  | 83 |
| systems. . . . .                                     | 26         | Special attributes . . . . .                     | 84 |
| Some words on quoting . . . . .                      | 26         | Configuration . . . . .                          | 84 |
| Configuration . . . . .                              | 27         | Examples . . . . .                               | 85 |

|  |     |  |     |
|--|-----|--|-----|
| See also . . . . .                                 | 85  | Configuration . . . . .                              | 134 |
| Old HTTP Client Connector . . . . .                | 87  | Virtual List View Control . . . . .                  | 136 |
| Modes . . . . .                                    | 87  | Handling memory problems in the LDAP                 |     |
| Special attributes . . . . .                       | 87  | Connector . . . . .                                  | 137 |
| Configuration . . . . .                            | 88  | LDAP Connector methods (API) . . . . .               | 137 |
| Examples . . . . .                                 | 88  | See also . . . . .                                   | 139 |
| See also . . . . .                                 | 89  | LDAP Server Connector . . . . .                      | 141 |
| HTTP Server Connector . . . . .                    | 91  | Scripting . . . . .                                  | 141 |
| Connector structure and workflow . . . . .         | 91  | Returning the LDAP message returned values           | 141 |
| Connector Client Authentication . . . . .          | 92  | Error handling . . . . .                             | 141 |
| Chunked Transfer Encoding . . . . .                | 92  | Configuration . . . . .                              | 142 |
| Configuration . . . . .                            | 92  | See also . . . . .                                   | 142 |
| Connector Schema . . . . .                         | 94  | Lotus Notes Connector . . . . .                      | 143 |
| See also . . . . .                                 | 94  | Mailbox Connector . . . . .                          | 145 |
| Old HTTP Server Connector . . . . .                | 95  | Configuration . . . . .                              | 145 |
| Configuration . . . . .                            | 95  | Predefined properties and attributes . . . . .       | 146 |
| See also . . . . .                                 | 95  | See also . . . . .                                   | 147 |
| IBM Directory Server Changelog Connector . . . . . | 97  | Memory Queue Connector . . . . .                     | 149 |
| Configuration . . . . .                            | 97  | Memory queue components . . . . .                    | 149 |
| See also . . . . .                                 | 98  | High level workflow . . . . .                        | 150 |
| ITIM Agent Connector . . . . .                     | 100 | Configuration . . . . .                              | 150 |
| Setting up SSL for the ITIM Agent Connector        | 100 | Accessing the Memory Queue programmatically          | 151 |
| Configuration . . . . .                            | 100 | Memory Stream Connector . . . . .                    | 153 |
| Known Issues . . . . .                             | 101 | Configuration . . . . .                              | 153 |
| See also . . . . .                                 | 101 | MQe Password Store Connector . . . . .               | 155 |
| JDBC Connector . . . . .                           | 103 | PKCS7 Encryption support . . . . .                   | 156 |
| Connector structure and workflow . . . . .         | 103 | MQe Password Store Connector Entry structure         | 158 |
| Understanding JDBC Drivers . . . . .               | 103 | Configuration . . . . .                              | 158 |
| Specifying ODBC database paths . . . . .           | 107 | See Also . . . . .                                   | 159 |
| Configuration . . . . .                            | 108 | Netscape/iPlanet/Sun Directory Changelog             |     |
| Customizing select, insert, update and delete      |     | Connector . . . . .                                  | 161 |
| statements . . . . .                               | 110 | Configuration . . . . .                              | 161 |
| Additional JDBC Connector functions . . . . .      | 111 | See also . . . . .                                   | 163 |
| Timestamps . . . . .                               | 112 | Properties Connector . . . . .                       | 165 |
| Calling Stored Procedures . . . . .                | 112 | Configuration . . . . .                              | 165 |
| SQL Databases: column names with special           |     | Server Notifications Connector . . . . .             | 167 |
| characters . . . . .                               | 113 | Encryption and Cryptography . . . . .                | 167 |
| Using prepared statements . . . . .                | 113 | Authentication . . . . .                             | 167 |
| On Multiple Entries . . . . .                      | 114 | Configuration . . . . .                              | 167 |
| JMS Connector . . . . .                            | 115 | System Queue Connector . . . . .                     | 171 |
| Introduction . . . . .                             | 115 | Introduction . . . . .                               | 171 |
| JMS message flow . . . . .                         | 115 | Configuration . . . . .                              | 171 |
| WebSphere MQ and JMS/non-JMS consumers of          |     | Security, Authentication and Authorization . . . . . | 172 |
| messages . . . . .                                 | 116 | MQe Initialization . . . . .                         | 173 |
| JMS message types . . . . .                        | 116 | Windows Users and Groups Connector . . . . .         | 175 |
| Iterator mode . . . . .                            | 118 | Preconditions . . . . .                              | 175 |
| Lookup mode . . . . .                              | 118 | Character sets . . . . .                             | 178 |
| Add Only mode . . . . .                            | 118 | Examples . . . . .                                   | 178 |
| Call/Reply mode . . . . .                          | 118 | Windows Users and Groups Connector                   |     |
| JMS headers and properties . . . . .               | 119 | functional specifications and software               |     |
| Configuration . . . . .                            | 120 | requirements . . . . .                               | 178 |
| Examples . . . . .                                 | 122 | System Store Connector . . . . .                     | 179 |
| External System Configuration . . . . .            | 122 | Configuration . . . . .                              | 180 |
| JMX Connector . . . . .                            | 125 | Using the Connector . . . . .                        | 181 |
| Connector Schema . . . . .                         | 125 | See also . . . . .                                   | 182 |
| Configuration . . . . .                            | 126 | RAC Connector . . . . .                              | 183 |
| JNDI Connector . . . . .                           | 129 | Introduction . . . . .                               | 183 |
| Configuration . . . . .                            | 129 | Configuration . . . . .                              | 184 |
| Setting the Modify operation . . . . .             | 130 | Using the Connector . . . . .                        | 184 |
| See also . . . . .                                 | 132 | See Also . . . . .                                   | 186 |
| LDAP Connector . . . . .                           | 133 | RDBMS Changelog Connector . . . . .                  | 187 |

|  |     |   |     |
|--|-----|---|-----|
| Configuration . . . . .                        | 187 | Passing input/output file names to an             |     |
| Change table format . . . . .                  | 189 | AssemblyLine . . . . .                            | 236 |
| Creating change tables in DB2 . . . . .        | 189 | EventHandler availability . . . . .               | 237 |
| Creating change tables in Oracle . . . . .     | 190 | Migration of Changelog EventHandlers . . . . .    | 237 |
| Creating Change table and triggers in MS SQL   | 191 | Active Directory Changelog EventHandler . . . . . | 239 |
| Creating change table and triggers in Informix | 193 | Behavior . . . . .                                | 239 |
| Creating change table and trigger for SYBASE   | 196 | Access to the USN synchronization values in the   |     |
| runtime-provided Connector . . . . .           | 199 | User Property Store . . . . .                     | 239 |
| Configuration . . . . .                        | 199 | Access to the runtime EventHandler's USN          |     |
| See also . . . . .                             | 199 | synchronization values . . . . .                  | 240 |
| Script Connector . . . . .                     | 201 | Configuration . . . . .                           | 240 |
| Predefined script objects. . . . .             | 201 | See also . . . . .                                | 241 |
| Functions. . . . .                             | 201 | Connector EventHandler . . . . .                  | 243 |
| Configuration . . . . .                        | 203 | Configuration . . . . .                           | 243 |
| Examples. . . . .                              | 203 | Objects/properties/attributes . . . . .           | 243 |
| See also . . . . .                             | 203 | See also . . . . .                                | 243 |
| SNMP Connector . . . . .                       | 205 | DSMLv2 EventHandler . . . . .                     | 245 |
| Configuration . . . . .                        | 205 | Transportation (binding). . . . .                 | 245 |
| Examples. . . . .                              | 205 | EventHandler Workflow. . . . .                    | 245 |
| SNMP Server Connector. . . . .                 | 207 | Operations . . . . .                              | 245 |
| Connector Schema. . . . .                      | 207 | Configuration . . . . .                           | 245 |
| Configuration . . . . .                        | 208 | Exchange Changelog EventHandler . . . . .         | 249 |
| TAM Connector . . . . .                        | 209 | Behavior . . . . .                                | 249 |
| Introduction. . . . .                          | 209 | Access to the USN synchronization values in the   |     |
| Connector Modes . . . . .                      | 209 | User Property Store . . . . .                     | 249 |
| Configuration . . . . .                        | 209 | Access to the runtime EventHandler's USN          |     |
| Using the Connector . . . . .                  | 211 | synchronization values . . . . .                  | 250 |
| Troubleshooting . . . . .                      | 217 | Configuration . . . . .                           | 250 |
| Connector Input Attribute Details . . . . .    | 217 | See also . . . . .                                | 251 |
| TCP Connector . . . . .                        | 221 | HTTP EventHandler . . . . .                       | 253 |
| Iterator Mode . . . . .                        | 221 | Example . . . . .                                 | 253 |
| AddOnly Mode . . . . .                         | 221 | Configuration . . . . .                           | 253 |
| Configuration . . . . .                        | 221 | See also . . . . .                                | 254 |
| See also . . . . .                             | 222 | IBM Directory Server EventHandler . . . . .       | 255 |
| TCP Server Connector . . . . .                 | 223 | Configuration . . . . .                           | 256 |
| Configuration . . . . .                        | 223 | See also . . . . .                                | 257 |
| Connector Schema. . . . .                      | 223 | LDAP EventHandler . . . . .                       | 259 |
| See Also . . . . .                             | 224 | Object Added (_objAdded) . . . . .                | 259 |
| Timer Connector . . . . .                      | 225 | Object Rename (_objRenamed) . . . . .             | 259 |
| Configuration . . . . .                        | 225 | Object Modified (_objModified) . . . . .          | 260 |
| URL Connector. . . . .                         | 227 | Object Removed (_objRemoved) . . . . .            | 260 |
| Configuration . . . . .                        | 227 | Error Encountered (_handleError) . . . . .        | 260 |
| Supported URL protocol. . . . .                | 227 | Configuration . . . . .                           | 260 |
| See also . . . . .                             | 227 | See also . . . . .                                | 261 |
| Web Service Receiver Server Connector. . . . . | 229 | LDAP Server EventHandler . . . . .                | 263 |
| Hosting a WSDL file . . . . .                  | 229 | Scripting . . . . .                               | 263 |
| Configuration . . . . .                        | 230 | Returning the LDAP message returned values        | 263 |
| Connector Operation . . . . .                  | 231 | Error handling . . . . .                          | 263 |
| See also . . . . .                             | 231 | Configuration . . . . .                           | 263 |
| z/OS Changelog Connector . . . . .             | 233 | Mailbox EventHandler . . . . .                    | 265 |
| Configuration . . . . .                        | 233 | Configuration . . . . .                           | 265 |
| See also . . . . .                             | 234 | Objects/properties/attributes . . . . .           | 265 |
|  |     | Examples. . . . .                                 | 266 |
|  |     | See also . . . . .                                | 266 |
|  |     | SNMP EventHandler . . . . .                       | 267 |
|  |     | Scripting the desired action. . . . .             | 267 |
|  |     | Error handling . . . . .                          | 268 |
|  |     | Returning the SNMP packet returned values         | 268 |
|  |     | Configuration . . . . .                           | 268 |
|  |     | TCP Port EventHandler . . . . .                   | 269 |
|  |     | Configuration . . . . .                           | 269 |

**Chapter 3. EventHandlers . . . . . 235**

|   |     |
|---|-----|
| Migration from ChangeLog EventHandlers to |     |
| ChangeLog Connectors . . . . .            | 235 |
| EventHandler types . . . . .              | 235 |
| When are they started? . . . . .          | 236 |
| What do they do? . . . . .                | 236 |
| Data flow . . . . .                       | 236 |

|   |     |
|---|-----|
| Objects/properties/attributes . . . . .               | 269 |
| Examples . . . . .                                    | 269 |
| See also . . . . .                                    | 270 |
| Generic thread (primitive EventHandler) . . . . .     | 271 |
| Configuration . . . . .                               | 271 |
| See also . . . . .                                    | 271 |
| Timer EventHandler (primitive EventHandler) . . . . . | 273 |
| Configuration . . . . .                               | 273 |
| Examples . . . . .                                    | 273 |
| z/OS LDAP Changelog EventHandler . . . . .            | 275 |
| Configuration . . . . .                               | 275 |
| Polling logic . . . . .                               | 276 |
| See also . . . . .                                    | 276 |

## Chapter 4. Parsers . . . . . 277

|  |     |
|--|-----|
| Base Parsers . . . . .                               | 277 |
| Character Encoding conversion . . . . .              | 277 |
| Availability . . . . .                               | 277 |
| CSV Parser . . . . .                                 | 279 |
| Configuration . . . . .                              | 279 |
| DSML Parser . . . . .                                | 281 |
| Configuration . . . . .                              | 281 |
| Examples . . . . .                                   | 281 |
| See also . . . . .                                   | 282 |
| DSMLv2 Parser. . . . .                               | 283 |
| Modes . . . . .                                      | 283 |
| Operations . . . . .                                 | 283 |
| Binary and non-String Attributes . . . . .           | 289 |
| Optional Attributes . . . . .                        | 289 |
| Setting result code and result description . . . . . | 290 |
| Multiple Attribute modifications . . . . .           | 290 |
| Configuration . . . . .                              | 290 |
| Examples . . . . .                                   | 291 |
| Fixed Parser . . . . .                               | 295 |
| Configuration . . . . .                              | 295 |
| HTTP Parser . . . . .                                | 297 |
| Configuration . . . . .                              | 297 |
| Attributes or properties . . . . .                   | 297 |
| Character sets/Encoding . . . . .                    | 298 |
| See also . . . . .                                   | 299 |
| LDIF Parser . . . . .                                | 301 |
| Configuration . . . . .                              | 301 |
| See also . . . . .                                   | 302 |
| Line Reader Parser . . . . .                         | 303 |
| Configuration . . . . .                              | 303 |
| Script Parser. . . . .                               | 305 |
| Objects . . . . .                                    | 305 |
| Functions (methods) . . . . .                        | 306 |
| Configuration . . . . .                              | 306 |
| Example . . . . .                                    | 307 |
| See also . . . . .                                   | 307 |
| Simple Parser . . . . .                              | 309 |
| Configuration . . . . .                              | 309 |
| SOAP Parser. . . . .                                 | 311 |
| Example Entry . . . . .                              | 311 |
| Example SOAP document . . . . .                      | 311 |
| Configuration . . . . .                              | 311 |
| Parser-specific calls . . . . .                      | 312 |
| Examples . . . . .                                   | 312 |
| XML Parser . . . . .                                 | 313 |
| Configuration . . . . .                              | 313 |

|  |     |
|--|-----|
| Character Encoding in the XML Parser . . . . . | 314 |
| Examples . . . . .                             | 314 |
| Additional Examples . . . . .                  | 316 |
| See also . . . . .                             | 316 |
| XML SAX Parser . . . . .                       | 317 |
| Configuration . . . . .                        | 318 |
| See also . . . . .                             | 318 |
| XSL based XML parser . . . . .                 | 319 |
| Introduction . . . . .                         | 319 |
| Configuration . . . . .                        | 319 |
| Using the Parser . . . . .                     | 319 |
| See also . . . . .                             | 321 |
| User-defined parsers . . . . .                 | 323 |

## Chapter 5. Function Components . . . . . 325

|   |     |
|---|-----|
| Castor Java to XML FC . . . . .                 | 327 |
| Castor Overview . . . . .                       | 327 |
| Configuration . . . . .                         | 327 |
| Using the FC . . . . .                          | 328 |
| Castor XML to Java FC . . . . .                 | 329 |
| Configuration . . . . .                         | 329 |
| Using the FC . . . . .                          | 330 |
| XMLToSDO FC. . . . .                            | 331 |
| Example . . . . .                               | 331 |
| Configuration . . . . .                         | 332 |
| Migration . . . . .                             | 332 |
| SDOToXML FC. . . . .                            | 335 |
| Configuration . . . . .                         | 336 |
| Using the FC . . . . .                          | 336 |
| Migration . . . . .                             | 336 |
| AssemblyLine FC . . . . .                       | 339 |
| Configuration . . . . .                         | 339 |
| Using the FC . . . . .                          | 339 |
| Java Class Function Component . . . . .         | 341 |
| Schema . . . . .                                | 341 |
| Configuration . . . . .                         | 341 |
| Parser FC. . . . .                              | 343 |
| Configuration . . . . .                         | 343 |
| Using the FC . . . . .                          | 343 |
| Scripted FC . . . . .                           | 345 |
| Configuration . . . . .                         | 345 |
| Using the FC . . . . .                          | 345 |
| See also . . . . .                              | 345 |
| CBE Generator Function Component . . . . .      | 347 |
| Common Base Event (CBE). . . . .                | 347 |
| The Common Event Infrastructure (CEI) . . . . . | 347 |
| CBE FC Configuration . . . . .                  | 347 |
| Input and Output Map Attributes . . . . .       | 347 |
| Function Component API . . . . .                | 349 |
| Generating a CBE Log XML . . . . .              | 350 |
| See also . . . . .                              | 350 |
| SendEmail Function Component . . . . .          | 351 |
| Configuration . . . . .                         | 351 |
| Memory Queue FC . . . . .                       | 353 |
| Configuration . . . . .                         | 353 |
| Using the FC . . . . .                          | 353 |
| See also . . . . .                              | 354 |
| Axis Java To Soap FC. . . . .                   | 355 |
| Configuration . . . . .                         | 355 |
| Using the FC . . . . .                          | 356 |
| WrapSoap FC . . . . .                           | 359 |

|   |     |
|---|-----|
| Configuration . . . . .                       | 359 |
| Using the FC . . . . .                        | 360 |
| InvokeSoap WS FC . . . . .                    | 361 |
| Introduction . . . . .                        | 361 |
| Authentication . . . . .                      | 361 |
| Configuration . . . . .                       | 361 |
| Using the FC . . . . .                        | 362 |
| See also . . . . .                            | 363 |
| Axis Soap To Java FC. . . . .                 | 365 |
| Configuration . . . . .                       | 365 |
| Using the FC . . . . .                        | 365 |
| Axis EasyInvoke Soap WS FC. . . . .           | 367 |
| Authentication . . . . .                      | 367 |
| Configuration . . . . .                       | 367 |
| Using the FC . . . . .                        | 368 |
| See also . . . . .                            | 369 |
| Complex Types Generator FC . . . . .          | 371 |
| Configuration . . . . .                       | 371 |
| Function Component Input and Output . . . . . | 371 |
| Troubleshooting . . . . .                     | 372 |
| Remote Command Line FC. . . . .               | 373 |
| Configuration . . . . .                       | 373 |
| Function Component Input. . . . .             | 374 |
| Function Component Output . . . . .           | 375 |
| Using the FC . . . . .                        | 375 |
| See also . . . . .                            | 376 |
| z/OS TSO/E Command Line FC. . . . .           | 377 |
| Configuration . . . . .                       | 377 |
| Using the FC . . . . .                        | 377 |
| Setting up the native part of the FC. . . . . | 378 |
| See also . . . . .                            | 379 |

## Chapter 6. SAP R/3 Component Suite 381

|  |     |
|--|-----|
| Who should read this chapter . . . . .                                       | 381 |
| Component Suite Installation . . . . .                                       | 381 |
| Software Requirements . . . . .  | 381 |
| Verifying the Component Suite for SAP R/3 . . . . .                          | 382 |
| Checking the Version Numbers . . . . .                                       | 383 |
| Uninstallation . . . . .   | 383 |
| Function Component For SAP R/3 . . . . .                                     | 385 |
| Function Component Introduction . . . . .                                    | 385 |
| Configuration . . . . .  | 385 |
| Using the Function Component . . . . .                                       | 387 |
| User Registry Connector for SAP R/3 . . . . .                                | 389 |
| Introduction . . . . .   | 389 |
| Configuration . . . . .  | 390 |
| Using the User Registry Connector for SAP R/3 . . . . .                      | 393 |
| Human Resources/Business Object Repository Connector for SAP R/3 . . . . .   | 397 |
| Introduction . . . . .   | 397 |
| Configuration . . . . .  | 399 |
| Using the Human Resources Connector for SAP R/3 . . . . .                    | 402 |
| ALE Intermediate Document (IDOC) Connector for SAP R/3 and SAP ERP . . . . . | 407 |
| Introduction . . . . .   | 407 |
| Configuration . . . . .  | 408 |
| Using the SAP ALE IDOC Connector . . . . .                                   | 410 |
| Troubleshooting the SAP R/3 Component Suite . . . . .                        | 419 |
| Supplemental information for the SAP R/3 Component Suite . . . . .           | 421 |

|   |     |
|---|-----|
| Example User Registry Connector XML Instance Document . . . . . | 421 |
| XSchema for User Registry Connector XML . . . . .               | 422 |

## Chapter 7. Script languages . . . . . 433

|                               |     |
|-------------------------------|-----|
| JavaScript . . . . .          | 433 |
| Java and JavaScript . . . . . | 433 |

## Chapter 8. Objects . . . . . 435

|   |     |
|---|-----|
| The AssemblyLine Connector object . . . . .             | 435 |
| The attribute object . . . . .                          | 435 |
| Examples. . . . .                                       | 435 |
| See also . . . . .                                      | 436 |
| The Connector Interface object. . . . .                 | 436 |
| Methods . . . . .                                       | 436 |
| The Entry object . . . . .                              | 436 |
| Global Entry instances available in scripting . . . . . | 437 |
| See also . . . . .                                      | 437 |
| The FTP object . . . . .                                | 437 |
| Example . . . . .                                       | 437 |
| Main object . . . . .                                   | 438 |
| The Search (criteria) object . . . . .                  | 438 |
| Operands. . . . .                                       | 438 |
| Example . . . . .                                       | 438 |
| The shellCommand object . . . . .                       | 438 |
| The status object . . . . .                             | 439 |
| The system object . . . . .                             | 439 |
| The task object . . . . .                               | 439 |

## Appendix A. Password Synchronization plug-ins . . . . . 441

## Appendix B. AssemblyLine and Connector mode flowcharts . . . . . 443

|                                     |     |
|-------------------------------------|-----|
| AssemblyLine flow . . . . .         | 444 |
| Connector initialization . . . . .  | 445 |
| Close flow . . . . .                | 446 |
| AddOnly mode. . . . .               | 447 |
| Call/Reply mode . . . . .           | 448 |
| Delete mode. . . . .                | 449 |
| Delta Mode . . . . .                | 451 |
| Iterator mode . . . . .             | 455 |
| Lookup mode . . . . .               | 456 |
| Server Mode . . . . .               | 457 |
| Update mode . . . . .               | 459 |
| End-of-flow for all modes . . . . . | 462 |
| Connector Reconnect . . . . .       | 463 |
| Function Components . . . . .       | 464 |

## Appendix C. Server API . . . . . 465

|  |     |
|--|-----|
| Overview. . . . .                                | 465 |
| Sample use case . . . . .                        | 466 |
| Local and Remote Server API interfaces . . . . . | 466 |
| Server API structure . . . . .                   | 467 |
| Security . . . . .                               | 467 |
| Configuring the Server API. . . . .              | 468 |
| Configuring the Server API properties . . . . .  | 468 |
| Setting up the User Registry . . . . .           | 468 |
| Remote client configuration . . . . .            | 468 |

|  |     |
|--|-----|
| Using the Server API . . . . .                 | 470 |
| Creating a local Session . . . . .             | 470 |
| Creating a remote Session . . . . .            | 470 |
| Working with Config Instances . . . . .        | 470 |
| Working with AssemblyLines . . . . .           | 471 |
| Working with EventHandlers . . . . .           | 474 |
| Editing configurations . . . . .               | 474 |
| Working with the System Queue . . . . .        | 477 |
| Working with the Tombstone Manager . . . . .   | 478 |
| Working with TDI Properties . . . . .          | 482 |
| Registering for Server API event notifications | 482 |
| Getting access to log files . . . . .          | 484 |
| Server Info . . . . .                          | 485 |
| Using the Security Registry . . . . .          | 486 |
| Custom Method Invocation . . . . .             | 486 |
| The JMX layer . . . . .                        | 488 |
| Local access to the JMX layer . . . . .        | 488 |
| Remote access to the JMX layer . . . . .       | 489 |
| MBeans and Server API objects . . . . .        | 489 |
| JMX notifications . . . . .                    | 490 |
| JMX Example - TDI 6.1.1 and MC4]               |     |
| configuration . . . . .                        | 490 |
| Backward compatibility . . . . .               | 493 |
| Scenarios overview . . . . .                   | 493 |
| Server API changes in TDI 6.1.1 . . . . .      | 496 |
| Known issues . . . . .                         | 500 |

**Appendix D. Implementing your own Components . . . . . 503**

|   |     |
|---|-----|
| Support materials for Component development     | 503 |
| Developing a Connector . . . . .                | 503 |
| Implementing the Connector's Java source code   | 503 |
| Building the Connector's source code . . . . .  | 509 |
| Implementing the Connector's GUI                |     |
| configuration form . . . . .                    | 509 |
| Packaging and deploying the Connector . . . . . | 516 |
| Developing a Function Component . . . . .       | 516 |
| Implementing Function Component Java source     |     |
| code . . . . .                                  | 516 |
| Building the Function Component source code     | 517 |
| Implementing the Function Component GUI         |     |
| configuration form . . . . .                    | 517 |
| Packaging and deploying the Function            |     |
| Component . . . . .                             | 518 |
| See also . . . . .                              | 518 |

**Appendix E. Notices . . . . . 519**

|   |     |
|---|-----|
| Third-Party Statements . . . . .            | 520 |
| ICU License - ICU 1.8.1 and later . . . . . | 520 |
| Trademarks . . . . .                        | 521 |

---

## Chapter 1. Introduction

To work with examples complementing this manual, you must refer back to the installation package to download the necessary files.

To access these example files, go to the *root\_directory/examples* directory in the installation directories.





---

## Chapter 2. Connectors

---

### Connector availability and reference

The following is a list of all Connector Interfaces included with the IBM Tivoli Directory Integrator. The Connector Interface is the part of the Connector that implements the actual logic to communicate with the Data Source it is supposed to handle.

You can also make your own Connector Interfaces if needed (the AssemblyLine wraps them so they are available as AssemblyLine Connectors).

All following AssemblyLine Connectors have access to the methods described in the `com.ibm.di.server.AssemblyLineComponent` in addition to the methods and properties of the Connector Interface. For documentation of the methods, see the Javadocs (from the CE, choose **Help>Low Level API.**)

### Connector Interfaces

For a list of Supported Modes, see “Legend for the Supported Mode columns” on page 6.

For each Connector Interface listed, see the documentation outlined in this chapter.

“ACT Connector” on page 9

A

“Active Directory Changelog (v.2) Connector” on page 13

I

“AssemblyLine Connector” on page 19

I

“Axis Easy Web Service Server Connector” on page 21

S

“Btree Object DB Connector” on page 25

A D I L U

“Command line Connector” on page 26

A I C

“Direct TCP /URL scripting” on page 29

custom

“Domino Change Detection Connector” on page 35

I

“Domino Users Connector” on page 45

A D I L U

“DSMLv2 SOAP Connector” on page 63

A D I L U C Δ

“DSMLv2 SOAP Server Connector” on page 67

S

“Exchange Changelog Connector” on page 71

I

“File system Connector” on page 77

A I

**"FTP Client Connector" on page 79**  
A I

**"GLA Connector" on page 80**  
I

**"Old HTTP Client Connector" on page 87**  
A D I L U C Δ S

**"HTTP Client Connector" on page 83**  
A I L C

**"Old HTTP Server Connector" on page 95**  
A I

**"HTTP Server Connector" on page 91**  
I S

**"Human Resources/Business Object Repository Connector for SAP R/3" on page 397**  
A D I L U

**"IBM Directory Server Changelog Connector" on page 97**  
I

**IBM MQ Connector**  
A I L C

**"JDBC Connector" on page 103**  
A D I L U Δ

**"JMS Connector" on page 115**  
A I L C

**"JMX Connector" on page 125**  
I

**"JNDI Connector" on page 129**  
A D I L U Δ

**"LDAP Connector" on page 133**  
A D I L U Δ

**"LDAP Server Connector" on page 141**  
S

**"Lotus Notes Connector" on page 57**  
A D I L U

**"Mailbox Connector" on page 145**  
I L D

**"Memory Queue Connector" on page 149**  
A I

**"Memory Stream Connector" on page 153**  
A I

**"MQe Password Store Connector" on page 155**  
I

**"Netscape/iPlanet/Sun Directory Changelog Connector" on page 161**  
I

**"System Store Connector" on page 179**  
A D I L U

**“RAC Connector” on page 183**

A I

**“RDBMS Changelog Connector” on page 187**

I

**“runtime-provided Connector” on page 199**

A D I L U C A S

A runtime provided Connector is a Connector sent to the AssemblyLine as a parameter when the AssemblyLine is started. We cannot say in advance what modes that Connector supports since you wrote it and the available modes are not visible to TDI. Also see “runtime-provided Connector” on page 199.

**“Script Connector” on page 201**

custom

You write the Script Connector yourself, and it provides the modes you write into it.

**“Server Notifications Connector” on page 167**

A I

**“SNMP Connector” on page 205**

A I L

**“SNMP Server Connector” on page 207**

S

**“Properties Connector” on page 165**

A I U L D

**“System Queue Connector” on page 171**

A I

**“TAM Connector” on page 209**

A I D L U

**“TCP Connector” on page 221**

A I

**“TCP Server Connector” on page 223**

I S

**“ITIM Agent Connector” on page 100**

A D I L U

**“ITIM DSMLv2 Connector” on page 61**

A D I L U

**“Timer Connector” on page 225**

I

**“URL Connector” on page 227**

A I

**“User Registry Connector for SAP R/3” on page 389**

A D I L U

**“Web Service Receiver Server Connector” on page 229**

S

**“Windows Users and Groups Connector” on page 175**

A D I L U

**“z/OS Changelog Connector” on page 233**

I

## Legend for the Supported Mode columns

- A-AddOnly
- D-Delete
- I-Iterator
- L-Lookup
- U-Update
- Δ-Delta
- C-Call/Reply
- S-Server
- +-Newer version support exists

## Script-based Connectors

A potential source of problems exists if you made direct Java calls into the same libraries as IBM Tivoli Directory Integrator. A new version of IBM Tivoli Directory Integrator might have updated libraries (with different semantics), or you might have upgraded your libraries since the last time you used your Connector.

For a list of Supported Modes, see “Legend for the Supported Mode columns.” The Script Connector enables you to write your own Connector in JavaScript™.

### Generic Connector

custom

You write the Script Connector yourself in JavaScript, and it provides the modes you write into it. See “JavaScript Connector” in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.

## Configurations

For a list of Supported Modes, see “Legend for the Supported Mode columns.”

## Connector re-use

When a Connector is instantiated, usually it allocates a certain amount of resources to communicate with a particular system (connection objects, session objects, result sets ...). When multiple Connectors of the same type are connected to the same system, often it is reasonable to share the underlying resources. This means that a single connection to the given system will be re-used by multiple Connectors.

TDI allows Connector re-use to happen within an AssemblyLine. For a given AssemblyLine the you have the option to re-use an already configured Connector from the same AssemblyLine.

With regards to the TDI Server, when re-using a Connector, a single physical Connector object is instantiated and a number of logical Connectors share it.

With regards to configuration, Connector re-using is a master-slave relation: the re-used (“master”) Connector has a full connection and parser configuration and all re-using Connectors have references to the master Connector. All re-using Connectors share the connection and parser settings of the Connector they re-use. Although connection and parser settings are fixed for re-using Connectors, certain other features are configured separately (if any parameter is not configured separately, it is inherited from the master Connector):

- Input/Output Map
- Link Criteria
- Hooks
- Delta settings
- Reconnect settings

Generally, a Connector can be re-used in the same mode (except for Iterator and Server) without any problem. This means that, for example, you can safely re-use a Connector in Lookup mode as many times as you wish.

A problem can potentially arise when a Connector is re-used in different modes. The shared physical Connector object is initialized and terminated only once. So the Connector's initialization and termination procedure must be common for all supported modes.

The following is a list of TDI Connectors which can be re-used in different modes:

- Domino Users Connector
- DSMLv2 SOAP Connector
- HTTP Client Connector
- IBM MQ Connector
- ITIM Agent Connector
- JDBC Connector
- JMS Connector
- JNDI Connector
- LDAP Connector
- Lotus Notes Connector
- Mailbox Connector
- Properties Connector
- SAP R/3 Business Object Repository Connector
- SAP R/3 User Registry Connector
- Script Connector (depends on the user-supplied Javascript)
- SNMP Connector
- System Queue Connector
- System Store Connector
- TAM Connector
- TCP Connector
- ITIM DSMLv2 Connector
- URL Connector
- Windows Users and Groups Connector

Any Connector not in this list can not be re-used in the same AssemblyLine; either because it makes no sense, or because the Connector's internal logic does not allow it.

For configuring a Connector for re-use in an AssemblyLine, refer to *IBM Tivoli Directory Integrator 6.1.1: Users Guide*. In the configured AssemblyLine, the re-used Connectors will show up with their name prepended with '@'.



---

# ACT Connector

## Introduction

The execution of assembly lines on a TDI server may produce some events. Events can also be produced by other sources. external to TDI.

An mechanism which can process these events is available in the TDI Server. When an event pattern is matched, the engine will fire a TDI server event, thus notifying any listeners. Events can then be caught using the “Server Notifications Connector” on page 167, for example and then further processed.

ACT (Active Correlation Technology) is a technology designed to build and execute rules for correlation of events, and especially the events conforming to the Common Base Events (CBE) specification. This technology provides a toolkit (in the form of an Eclipse plug-in) for rule creation and compilation. It also provides a Java software component, the ACT Engine.

**Note:** Only the ACT Engine, wrapped in a TDI module, is proved with TDI. In order to meaningfully deploy, and be able to define rules, you need to license the IBM Autonomic Computing Toolkit, and be provided with the Active Correlation Technology package.

In TDI, the ACT Engine has been integrated in the TDI Server. The ACT Engine has the following characteristics:

- The engine can be fed with events through the Server API (for example by a script component in an AssemblyLine) and will act according to its configured rules. Each rule is able to send a TDI Server notifications
- From an architectural point of view it is a sibling of the System Queue and the Tombstone Manager. It lives in the same JVM as the TDI Server.

The ACT Engine provides a programming interface through the Server API. The Server API is accessed through a network connection, using the RMI protocol.

The ACT Engine will consume events, and interested parties can pass events to this engine through the Server API. The engine will then match these events against the configured matching rules. From time to time some of these events will trigger a matching rule which will result in a TDI server event being fired. This event can, for example, be caught using the “Server Notifications Connector” on page 167 and then processed further.

ACT Engine processing rules are defined by means of an Eclipse plug-in, part of the Autonomic Computing Toolkit. For more information, refer to the Developer's Guide at [http://www-128.ibm.com/developerworks/autonomic/books/fpy0mst.htm#ToC\\_91](http://www-128.ibm.com/developerworks/autonomic/books/fpy0mst.htm#ToC_91).

To ease the use of the ACT engine, a Connector, which operates in AddOnly mode is provided – the ACT Connector.

## Configuration

The Connector's title is “Active Correlation Technology Connector”. Its parameters are:

### Connection Type

This parameter determines whether the ACT Connector will send events to the local or a remote ACT engine. The available values for this parameter are “remote” and “local”.

**local** The Connector will send events to the ACT engine in the local TDI server

### remote

The Connector will connect to a remote TDI Server system and send events its ACT engine.

Default value is "local".

### **RMI URL**

This parameter is only taken into account if the **Connection Type** parameter is set to "remote". This is the RMI URL used to connect to the remote TDI Server..

Default value is "rmi://127.0.0.1:1099/SessionFactory".

### **Username**

This parameter is only taken into account if the **Connection Type** parameter is set to "remote". This is the username parameter is used to authenticate to the TDI server (using Remote API authentication).

### **Password**

This parameter is only taken into account if the **Connection Type** parameter is set to "remote". This is the password parameter used to authenticate to the TDI server.

### **Detailed Log**

If checked, more log messages will be generated.

In order for an instance of an ACT Connector to talk to a TDI Server's ACT Engine, that TDI Server must have its ACT Engine enabled and configured. This is done by setting system properties in `global.properties` and/or `solution.properties`:

#### **act.engine.on**

This is a boolean property (true/false) which enables/disables the ACT Engine.

#### **act.engine.rule.set.file**

This contains the path of the rule file, which will be used by the ACT engine; the rule file must be COMPILED (with the "ACT Rule Builder" Eclipse plugin – the Rule Builder can compile rule sets).

For example, if you want to enable the ACT feature of TDI and set the ACT engine to use the rules in the "myrules.acts" file, you can specify the following properties in `global.properties/solution.properties`:

```
act.engine.on=true
act.engine.rule.set.file=myrules.acts
```

## **ACT Rule Builder**

The rules files themselves are created by means of an Eclipse plug-in, part of the Active Correlation Technology technology. The Eclipse version on which to install it has to match specific requirements, and the software has to be installed as recommended in the ACT documentation. The document called *Developer's Guide for Active Correlation Technology V0[1].1.doc*, in sections 15.1 through 15.3, describes how to complete these steps. Part 15.1 describes the prerequisites, and the 15.2.3 part describes the process for the installation of the plug-in itself.

After having installed the ACT Rule Builder software, Eclipse allows the creation of a Rule Set file within an Eclipse project. When trying to create a new component in a project, only the most common types (Class, Interface,...) appear. Choose "Other" in this menu. This opens the exhaustive list of component types. In this list, choose "Active Correlation Technology > Rule Set File".

The created component then appears in the project. A rule set comprises several rule blocks, and each rule block gathers rules. The UI of the plug-in allows you to easily create a new rule block and a rule inside this block, by right-clicking in the outline panel.

The document called "Rule Writer's Guide and Reference" describes the possibilities of the ACT Rule Builder software in detail.



## Using the Connector

This Connector can feed events to a TDI Server's ACT Engine for processing. The Connector uses the Server API to send events to the ACT engine; it operates in AddOnly mode. The Connector works synchronously – that is each output operation returns only after the event has been completely processed by the target ACT engine.

Currently only Common Base Events are supported. A `CommonBaseEvent` can be passed to the ACT Connector either as a raw Java object or as a set of *work* Entry attributes.

The Connector embeds the “CBE Generator Function Component” on page 347 to help with the conversion of the work Entry attributes into a `CommonBaseEvent` object, if required.

A `CommonBaseEvent` in the form of a raw Java object is supplied to the Connector as an optional work Entry attribute:

### **\$rawCBE**

optional attribute; must be of type `org.eclipse.hyades.logging.events.cbe.CommonBaseEvent`; if this attribute is provided, all other attributes are ignored and the Connector operates on the CBE, which is the attribute's value

If the `$rawCBE` attribute is missing, a set of attributes which describe a `CommonBaseEvent` is expected. For this Connector, only Output Map attributes are applicable.

## Sending a notification from a rule

In this section we will focus on the definition and the usage of a simple filter rule. This case is sufficient to describe how to send a notification to the Server API when a rule is matched. All the template rules proposed by the ACT Rule Builder are a priori usable.

The ACT compiler of the ACT Rule Builder must be set in order to recognize the `TDIFunctions` interface. For that, we have to open the panel accessible via “Window > Preferences...”. If the installation of the plugin was done correctly, an “Active Correlation Technology” option should be accessible in the left side bar. Click on the underlying “compiler” option. This opens a panel where we can add JAR file paths. Then add the file containing the interface `TDIFunctions` and its implementation – *diserverapi.jar*.

Then, create a rule set file, a rule block, a “filter” rule and open it. A specific editor should be associated.

Several panels are accessible. The document about rule writing indicates how to fill the required parameters, depending on the aim wished by the developer for his rule. In case of a filter rule it is rather simple, we just have to specify the single event that will trigger the rule.

We will focus here on the “Rules responses” panel, which is the most relevant in our case. This is where the action to be triggered is defined.

Here we can write pieces of code that will be executed when the rule is triggered. In most cases, the rule designer will only have to write this piece of code:

```
com.ibm.di.api.act.TDIFunctions util = (com.ibm.di.api.act.TDIFunctions)
    act_lib.getExternalContext("TDIFunctions");

util.sendNotification("myevent", "myid", act_event);
```

The first line shows the method to invoke in order to get a `TDIFunctions` instance. Then the `sendNotification` invocation fires a TDI server notification. The issued notification will be of type “user.act.myevent” (after the `TDIFunctions` implementation and the Server API add their prefixes).

The `sendNotification` call passes the current event, which triggered the rule (`act_event`) as user data of the notification.

The rule writer must keep in mind that the ACT engine and the listeners of server notifications execute in different threads. So the code in the rules should not pass as notification's user data some of the internal objects, which the ACT engine may modify (for example `act_lib`). If passing such an object is necessary, the rule writer may create a deep clone of the object and pass the clone as user data. In this way race conditions between the ACT engine and notification listeners will be safely avoided.

## Programmatic Interface (API)

Events can be passed to the ACT engine of TDI through the Server API. A method is available in both the local and the remote Server API session interfaces:

```
/**
 * Processes an event by the Active Correlation Technology engine of the TDI server.
 * The method returns when the engine has completely processed the event.
 */
public void sendEventToACT(Serializable event)
```

Currently the method operates only on events of type `org.eclipse.hyades.logging.events.cbe.CommonBaseEvent`.

## See Also

An example demonstrating the use of the ACT Connector, in folder `<TDI_installation_folder>/examples/ACT`,

“CBE Generator Function Component” on page 347,

“GLA Connector” on page 80

---

## Active Directory Changelog (v.2) Connector

The Active Directory Changelog (v.2) Connector (hereafter referred to as ADCLV2) is a specialized instance of the LDAP Connector. It reports changed Active Directory objects so that other repositories can be synchronized with Active Directory.

The LDAP protocol is used for retrieving changed objects.

When run the Connector reports the object changes necessary to synchronize other repositories with Active Directory regardless of whether these changes occurred while the Connector has been offline or they are happening as the Connector is online and operating.

This connector also supports Delta Tagging, at the Entry level only.

The ADCLV2 Connector operates in Iterator mode.

### Notes:

1. This Connector is a replacement for the Active Directory Changelog Connector; usage of the latter is deprecated.
2. This version of the Connector is able to process huge AD Servers (millions of entries) regardless of the administrative time limit for executing a query on AD (the MaxQueryDuration setting). In comparison the old version of the Connector could fail with TimeLimitExceeded error when run against big AD Servers.
3. It uses a simpler algorithm for retrieving changes and uses only one USN number to represent the synchronization state. In comparison the old Connector uses 4 USN numbers and a fairly complex algorithm.
4. It does not distinguish between "add" and "modify" operations - both are reported as "modify"; delete operations are reported as "delete". Not being able to distinguish between "add" and "modify" is not a serious restriction because the TDI Update Connector mode natively handles "add" and "modify" operations.
5. It might report "delete" operations for entries that have not been added to the repository being synchronized with AD (this will happen when an entry is added and deleted in AD while the Connector has been offline). It is something to be aware of, but it is not a serious restriction because TDI Delete Connector mode first checks if the entry to be deleted exists and if it does not exist, the "On No Match" hook is called - this is where you can place code to handle/ignore such unnecessary deletes.
6. The parameter **Page Size** specifies the size of the pages AD will return entries on (default value is 500).

## Tracking changes in Active Directory

Active Directory does not provide a Changelog as IBM Directory Server and some other LDAP Servers do.

The ADCLV2 Connector uses the **uSNChanged** Active Directory attribute to detect changed objects.

Each Active Directory object has an **uSNChanged** attribute that corresponds to a directory-global USN (Update Sequence Number) object. Whenever an Active Directory object is created, modified or deleted, the global sequence object value is increased, and the new value is assigned to the object's **uSNChanged** attribute.

On each AssemblyLine iteration (each call of the getNextEntry() Connector's method) it delivers a single object that has changed in Active Directory. It delivers the changed Active Directory objects as they are,

with all their current attributes and also reports the type of object change – whether the object was updated (added or modified) or deleted. The Connector does not report which attributes have changed in this object and the type of attribute change.

Synchronization state is kept by the Connector and saved in the User Property Store – after each reported changed object the Connector saves the USN number necessary to continue from the correct place in case of interruption and restart; when started, the ADCLV2 Connector reads from the IBM Tivoli Directory Integrator's User Property Store this USN value stored from the most recent ADCLV2 Connector session.

## Deleted objects in Active Directory

When an object is deleted from the directory, Active Directory performs the following steps:

- The object's **isDeleted** attribute is set to TRUE. Objects where **isDeleted==TRUE** are known as tombstones (not related to TDI tombstones).
- All attributes that are not needed by Active Directory are removed. A few key attributes, including **objectGUID**, **objectSID**, **nTSecurityDescriptor**, and **uSNChanged** are preserved.
- Moves the tombstone to the Deleted Objects container, which is a hidden container within the directory partition.

Tombstones or deleted objects are garbage collected some time after the deletion takes place. Two settings on the "cn=Directory Service,cn=Windows NT,cn=Service,cn=Configuration,dc=ForestRootDomain" object determine when and which tombstones are deleted:

- The "garbage collection interval" determines the number of hours between garbage collection on a domain controller. The default setting is 12 hours, and the minimum setting is 1 hour.
- The "tombstone lifetime" determines the number of days that tombstones persist before they are vulnerable to garbage collection. The default setting is 60 days, and the minimum setting is 2 days.

The above specifics imply the following requirements for synchronization processes that have to handle deleted objects:

- Synchronization has to be run on intervals shorter than the "tombstone lifetime" Active Directory setting.
- The **objectGUID** attribute has to be used for object identifier during synchronization. The object's **distinguishedName** attribute which uniquely identifies the position of an object in the directory tree, cannot be used because after the object is deleted it changes its place in the directory tree – it is moved in the Deleted Objects container and its old distinguished name is irrevocably lost. The **objectGUID** attribute is however never changed. When a deleted object is found during synchronization, a search in the other repository for an object with the same **objectGUID** should be made and the found object should be deleted.

## Moved objects in Active Directory

When an object is moved from one location of the Active Directory tree to another, its **distinguishedName** attribute changes. When this object change is detected based on the new increased value of the object's **uSNChanged** attribute, this change looks like any other modify operation - there is no information about the object's old distinguished name.

A synchronization process that has to handle moved objects properly should use the **objectGUID** attribute – it doesn't change when objects are moved. A search by the **objectGUID** attribute in the repository which is synchronized will locate the proper object and then the old and new distinguished names can be compared to check if the object has been moved.

## Use objectGUID as the object identifier

When tracking changes in Active Directory the **objectGUID** attribute should be used for object identifier and not the LDAP distinguished name. This is so because the distinguished name is lost when an object is deleted or moved in Active Directory. The **objectGUID** attribute is always preserved, it never changes and can be used to identify an object.

When the ADCLV2 Connector reports that an entry is changed, a search by **objectGUID** value should be performed in the other repository to locate the object that has to be modified or deleted. This means that the **objectGUID** attribute should be synchronized and stored into the other repository.

## Behavior

The ADCLV2 Connector detects and reports changed objects following the chronology of the **uSNChanged** attribute values: changed objects with lower **uSNChanged** values will be reported before changed objects with higher **uSNChanged** values.

The Connector executes an LDAP query of type (`usnChanged>=X`) where X is the USN number that represents the current synchronization state. Sort and Page LDAP v3 controls are used with the search operation and provide for chronology of changes and ability to process large result sets. The Show Deleted LDAP v3 request control (OID "1.2.840.113556.1.4.417") is used to specify that search results should include deleted objects as well.

The Connector might report "delete" operations for entries that have not been added to the repository being synchronized with Active Directory - this will happen when an entry is added and deleted in Active Directory while the Connector has been offline. This is not a serious restriction because IBM Tivoli Directory Integrator's Delete Connector mode first checks if the entry to be deleted exists and if it does not exist, the "On No Match" hook is called - this is where you can place code to handle/ignore such unnecessary deletes.

The ADCLV2 Connector consecutively reports all changed objects regardless of interruptions, regardless of when it is started and stopped and whether the changes happened while the Connector was online or offline. Synchronization state is kept by the Connector and saved in the User Property Store - after each reported changed object the Connector saves the USN number necessary to continue from the correct place in case of interruption and restart.

The Connector will signal end of data and stop (according to the timeout value) when there are no more changes to report.

When there are no more changed Active Directory objects to retrieve, the Active Directory Connector cycles, waiting for a new object change in Active Directory. The **Sleep Interval** parameter specifies the number of seconds between two successive polls when the Connector waits for new changes. The Connector loops until a new Active Directory object is retrieved or the timeout (specified by the **Timeout** parameter) expires. If the timeout expires, the Active Directory Connector returns a **null** Entry, indicating there are no more Entries to return. If a new Active Directory object is retrieved, it is processed as previously described, and the new Entry is returned by the Active Directory Connector.

The ADCLV2 Connector delivers changed Active Directory objects as they are, with all their current attributes. It does not determine which object attributes have changed, nor how many times an object has been modified. All intermediate changes to an object are irrevocably lost. Each object reported by the Active Directory Connector represents the cumulative effect of all changes performed to that object. The Active Directory Connector, however, recognizes the type of object change that has to be performed on the replicated data source and reports whether the object must be updated or deleted in the replicated data source.

**Note:** You can retrieve only objects and attributes that you have permission to read. The Connector does not retrieve an object or an attribute that you do not have permission to read, even if it exists in Active Directory. In such a case the ADCLV2 Connector acts as if the object or the attribute does not exist in Active Directory.

## Using the Active Directory Changelog V2 Connector

Each delivered entry by the Connector contains the **changeType** attribute whose value is either "update" (for newly created and modified objects) or "delete" (for deleted Active Directory objects). Each entry also contains 2 attributes that represent the objectGUID value:

- attribute **objectGUID** – contains a 16-byte byte array that represents the 128-bit objectGUID of the corresponding Active Directory object.
- attribute **objectGUIDStr** – contains the string representation of the hexadecimal value of the 128-bit objectGUID. It is delivered in the format {xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}, where each x represents a hexadecimal digit.

If you need to detect and handle moved or deleted objects, you must use the **objectGUID** value as object identifier instead of the LDAP distinguished name. The LDAP distinguished name changes when an object is moved or deleted, while the **objectGUID** attribute always remains unchanged. Store the objects' **objectGUID** attribute in the replicated data source and search by this attribute to locate objects.

**Note:** Deleted objects in Active Directory live for a configurable period of time (60 days by default), after which they are completely removed. To avoid missing deletions, perform incremental synchronizations more frequently.

The ADCLV2 Connector can be interrupted any time during the synchronization process. It saves the state of the synchronization process in the User Property Store of the IBM Tivoli Directory Integrator (after each Entry retrieval), and the next time the Active Directory Connector is started, it successfully continues the synchronization from the point the Active Directory Connector was interrupted.

This Connector supports the IBM Tivoli Directory Integrator 6.1.1 Checkpoint/Restart functionality. When a restart is requested and restart data is passed, the Connector retrieves the USN number from the restart data and starts synchronization from this USN number.

## Configuration

The Connector needs the following parameters:

### LDAP URL

The LDAP URL of the Active Directory service you want to access. The LDAP URL has the form `ldap://hostname:port` or `ldap://server_IP_address:port`. For example, `ldap://localhost:389`

**Note:** The default LDAP port number is 389. When using SSL, the default LDAP port number is 636.

### Login username

The distinguished name used for authentication to the service. For example, `cn=admin,dc=your_domain,dc=com`.

**Note:** If you use Anonymous authentication, you must leave this parameter blank.

### Login password

The credentials (password).

**Note:** If you use Anonymous authentication, you must leave this parameter blank.

### Authentication Method

The authentication method to be used. Possible values are:

- Anonymous (use no authentication)
- Simple (use weak authentication (cleartext password))

### Use SSL

Specifies whether to use Secure Sockets Layer for LDAP communication with Active Directory.

**Extra Provider Parameters**

Allows you to pass a number of extra parameters to the JNDI layer. It is specified as name:value pairs, one pair per line.

**Binary Attributes**

Specifies a list of parameters that are to be interpreted as binary values instead of strings. The default value for this parameter is **objectGUID objectSid**.

**LDAP Search Base**

The Active Directory sub-tree that is polled for changes. The search base should be an Active Directory Naming Context if detection of deleted objects is required. For example, **dc=your\_domain,dc=com**.

**Page Size**

Specifies the size of the pages AD will return entries on (default value is 500).

**Iterator State Key**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

**Start at**

Specifies either **EOD** or **0**. **EOD** means report only changes that occur after the Connector is started. **0** means perform full synchronization, that is, report all objects available in Active Directory Service. This parameter is taken into account only when the parameter specified by the **Iterator State Key** parameter is not found in the User Property Store.

**State Key Persistence**

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and the choices are:

**After read**

Updates the System Store when you read an entry from the Active Directory change log, before you continue with the rest of the AssemblyLine.

**End of cycle**

Updates the System Store with the change log number when all Connectors and other components in the AssemblyLine have been evaluated and executed.

**Manual**

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the ADCLV2 Connector's *saveStateKey()* method, somewhere in your AssemblyLine.

**Use Change Notifications**

Specifies whether to use notification when waiting for new changes in Active Directory. If not enabled, the Connector will poll for new changes. If enabled, the Connector will not sleep or timeout but instead wait for a Change Notification event (*Server Search Notification Control* (OID 1.2.840.113556.1.4.528)) from the Active Directory server.

**Timeout**

Specifies the maximum number of seconds the Connector waits for the next changed Active Directory object. If this parameter is **0**, then the Connector waits forever. If the Connector has not retrieved the next changed Active Directory object within *timeout* seconds, then it returns an empty (**null**) Entry, indicating that there are no more Entries to return. The default is 5.

**Sleep Interval**

Specifies the number of seconds the Connector sleeps between successive polls.

**Detailed Log**

If this field is checked, additional log messages are generated.

## Comment

Your comments here.

## Migration from Active Directory Changelog EventHandler to Active Directory Changelog (v.2) Connector

You need to do the following to reproduce an old EventHandler's configuration into an ADCLv2 Connector's implementation:

1. Create a new AssemblyLine and insert the Active Directory Changelog(v.2) Connector in it.
2. Set the ldapUrl, ldapUsername, ldapPassword, ldapAuthenticationMethod, ldapUseSSL, ldapSearchBase and Debug Connector parameters to the values of the corresponding EventHandler parameters.
3. Set the iteratorStateKey Connector parameter to the value of the persistentParameterName EventHandler parameter.
4. Set the useNotifications Connector parameter to "true".
5. When implementing the AssemblyLine flow consider that the Connector reports newly added entries as modify.

## See also

"LDAP Connector" on page 133,

"Exchange Changelog Connector" on page 71

"Netscape/iPlanet/Sun Directory Changelog Connector" on page 161,

"IBM Directory Server Changelog Connector" on page 97

"z/OS Changelog Connector" on page 233.



---

## AssemblyLine Connector

AssemblyLines are often called as compound functions from other AssemblyLines and EventHandlers. Setting up a call to perform a specific task and mapping in and out parameters can be tedious in a scripting environment. To ease the integration of AssemblyLines into a work flow, the AssemblyLine Connector provides a standard and familiar way of doing this; it wraps much of the scripting involved to execute an AssemblyLine. The AssemblyLine connector uses the AssemblyLine manual cycle mode for inline execution.

The AssemblyLine Connector supports Iterator mode only, except when calling another AssemblyLine which supports AssemblyLine Operations. See "AssemblyLine Operations" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for more information.

The server-server capability addresses security concerns when managers want TDI developers to access connected systems, but not to access the operational parameters of the Connector – or to impact its availability by deploying the new function on the same physical server.

**Note:** The return signature of previous versions of TDI is different, hence it is not possible to call AssemblyLines on a remote server from this version (TDI 6.1.1) to previous versions, like TDI 6.0.

## Configuration

The Connector needs the following parameters:

### AssemblyLine

The name of the AssemblyLine to be executed from this Connector. Choose from the drop-down list or enter the name.

### Remote Server

The TDI server on which to run the AssemblyLine. Use blank for local instance or *host[:port]*.

### Config Instance

The config instance ID or URL on the remote server.

### Keystores

Check this box to use the custom `api.remote.server.java` properties instead of standard `javax.net.ssl` properties for keystore configuration. If you do so, the following properties from `global.properties` become relevant (see also "global.properties" in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*):

`api.client.keystore`

Specifies the keystore file containing the client certificate

`api.client.keystore.pass`

Specifies the password of the keystore file specified by `api.client.keystore`

`api.client.key.pass`

The password of the private key stored in keystore file specified by `api.client.keystore`; if this property is missing, the password specified by `api.client.keystore.pass` is used instead.

`api.truststore`

Specifies the keystore file containing the TDI Server public certificate.

`api.truststore.pass`

Specifies the password for the keystore file specified by `api.truststore`.

### Detailed log

If this field is checked, additional log messages are generated.

## Using the Connector

The AssemblyLine Connector iterates on the result set from the target AssemblyLine which is always run synchronously in manual cycle mode by the AssemblyLine Connector. The target AssemblyLine can be local to the thread or on a remote server by use of the Server API.

### Attribute Mapping

The AssemblyLine Connector's input attribute map provides the returned attribute(s) from the target AssemblyLine; those returned attributes are set up in the Call/Return section of the target AssemblyLine.

You can retrieve those attributes by means of the Query Schema button in the Input Map section; also, a value of "\*" will map **all** attributes.

### AssemblyLine Parameters

The target AssemblyLine can be passed a Task Control Block (TCB) as a parameter. This parameter is runtime generated and the AssemblyLine Connector will use this to pass parameters to the target AssemblyLine.

---

## Axis Easy Web Service Server Connector

The Axis Easy Web Service Server Connector is part of the TDI Web Services suite. It is a simplified version of the “Web Service Receiver Server Connector” on page 229 in that it internally instantiates, configures and uses the AxisSoapToJava and AxisJavaToSoap FCs.

The functionality provided is the same as if you chain and configure these FCs in an AssemblyLine which hosts the “Web Service Receiver Server Connector” on page 229. When using this Connector you forgo the possibility of hooking custom processing before parsing the SOAP request and after serializing the SOAP response, that is, you are tied to the processing and binding provided by Axis, but you gain simplicity of setup and use.

The Axis Easy Web Service Server Connector operates in Server mode only.

AssemblyLines support an Operation Entry (op-entry). The op-entry has an attribute *\$operation* that contains the name of the current operation executed by the AssemblyLine. In order to process different web service operations easier, the Axis Easy Web Service Server Connector will set the *\$operation* attribute of the op-entry.

The Axis Easy Web Service Server Connector supports generation of a WSDL file according to the input and output schema of the AssemblyLine. As in TDI 6.1.1 AssemblyLines support multiple operations, the WSDL generation can result in a web service definition with multiple operations. There are some rules about naming the operations:

- Pre-6.1 TDI configuration files contain only one input and one output schema referred to as default operation schemas. When a pre-6.1 TDI configuration is used the only operation generated is named as the name of the AssemblyLine as in TDI 6.0.
- In TDI 6.1.1 configurations if there is an operation named “Default”, the corresponding operation in the WSDL file is named as the name of the AssemblyLine.
- In TDI 6.1.1 configurations if there is an operation named “Default” and there is also an operation with a name as the name of the AssemblyLine, both operations preserve their names in the WSDL file.
- In all other cases the operations appear in the WSDL file as they are named in the AssemblyLine configuration.

This Connector’s configuration is relatively simple. The Connector parses the incoming SOAP request, stores it (along with HTTP specific data) into the event Entry and then presents this Entry to the AssemblyLine for Attribute mapping. When the work Entry (now storing the Java representation of the SOAP response) is returned to the Connector in the Response phase, the Connector serializes the response and returns it to the Web Service client.

When this Connector receives a SOAP request, the connector parses it and sets the *\$operation* attribute of the op-entry. The name of the operation is determined by the name of the element nested in the Body element of the SOAP envelope. For parsing the SOAP messages, a SAX parser is used, which compared to a DOM parser adds less performance overhead.

There are several types of SOAP messages:

- When using RPC-style SOAP messages the name of the element is the same as the name of the operation.
- When using Document-style SOAP messages there are two scenarios:
  - Using Wrapped Document-style SOAP messages – in this case the body of the SOAP message looks like it is an RPC-style SOAP message; this is achieved by wrapping the contents of the SOAP Body in an element nested in the SOAP Body Element; the name of this element is the name of the SOAP operation.
  - Using ordinary, or unwrapped Document-style SOAP messages – in this case the notion of SOAP operation is not defined: the SOAP message is part of some SOAP message exchange. In this case,

the Connectors would set the \$operation attribute of the op-entry to the name of the element nested in the SOAP Body element and it is the responsibility of you as the TDI developer/deployer to make sure that a TDI solution handles this correctly. When using ordinary or unwrapped Document-style SOAP messages, it is best not to depend on the value of the \$operation attribute of the op-entry.

## Hosting a WSDL file

The Axis Easy Web Service Server Connector provides the *"wsdlRequested"* Connector Attribute to the AssemblyLine.

If an HTTP request arrives and the requested HTTP resource ends with *"?WSDL"* then the Connector sets the value of the *"wsdlRequested"* Attribute to **true** and reads the contents of the file specified by the **WSDL File** parameter into the *"soapResponse"* Connector Attribute; otherwise the value of this Attribute is set to **false**.

This Attribute's value thus allows you to distinguish between pure SOAP requests and HTTP requests for the WSDL file. The AssemblyLine can use a Branch Component to execute only the appropriate piece of logic – (1) when a request for the WSDL file has been received, then the AssemblyLine could perform some optional logic or read a different WSDL file and send it back to the web service client, or just rely on default processing; (2) when a SOAP request has been received the AssemblyLine will handle the SOAP request. Alternatively, you could program the `system.skipEntry()`; call at an appropriate place (in a script component, in a hook in the first Connector in the AssemblyLine, etc.) to skip further processing and go directly to the Response channel processing.

It is the responsibility of the AssemblyLine to provide the necessary response to a SOAP request.

The Connector implements a public method:

```
public String readFile (String aFileName) throws IOException;
```

This method can be used from TDI JavaScript in a script component to read the contents of a WSDL file on the local file system. The AssemblyLine can then return the contents of the WSDL in the *"soapResponse"* Attribute, and thus to the web service client in case a request for the WSDL was received.

## Configuration

### Parameters

#### TCP Port

The port number the service is running (listening) on.

#### Connection Backlog

This represents the maximum queue length for incoming connection indications (a request to connect). If a connection indication arrives when the queue is full, the connection is refused.

#### WSDL File

This parameter is required; its type is string. The value of this parameter must be the complete file system path to the WSDL document.

#### SOAP Operation

The name of the SOAP operation as described in the WSDL file.

#### Complex Types

This parameter is not required, but if specified it is a list of fully qualified Java class names (including the package name), where the different elements (Java classes) of this list are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

#### Tag Op-Entry

When this parameter is checked (that is, "true") the Connector will tag the op-entry only when

the executed operation is on the list of exposed operations in the AssemblyLine/WSDL. If the operation cannot be found in the WSDL then a SOAP Fault message will be generated and returned to the client.

**Note:** In TDI 6.0 the AxisEasyWSServerConnector required the **Soap Operation** parameter to be set. In TDI 6.1.1 when the **Tag Op-Entry** parameter is set to "true" the AxisEasyWSServerConnector will use the extracted operation name instead of the name specified with the **Soap Operation** parameter. In this case the **Soap Operation** parameter is not a required parameter, it can be left blank.

#### Use SSL

If checked the server will only accept SSL (https) connections. The SSL parameters (keystore, etc.) are specified as values of Java system properties in the `global.properties` file located in the TDI installation folder.

#### Require Client Authentication

Specifies whether this Connector will require clients to authenticate with client SSL certificates. If the value of this parameter is **true** (that is, checked) and the client does not authenticate with a client SSL certificate, then the Connector will drop the client connection. If the value of this parameter is **true** and the client does authenticate with a client SSL certificate, then the Connector will continue processing the client request. If the value of this parameter is **false**, then the Connector will process the client request regardless of whether the client authenticates with a client SSL certificate.

#### Auth Realm

This is the basic-realm sent to the client in case authentication is requested. The default is "IBM Tivoli Directory Integrator".

#### Use HTTP Basic Authentication

This connector supports HTTP basic authentication. To activate, check the "Use HTTP Basic Authentication" checkbox. If activated, the server checks if any credentials are already sent and if not, the server sends authorization request to client. After the client sends the needed credentials, the Connector then sets two attributes: "http.username" and "http.password". These two attributes contain the username and password of the client. It is responsibility of the AssemblyLine to check if this pair of username and password is valid. If the client is authorized successfully then "http.credentialsValid" work Entry Attribute must be set to true. If the client is not authorized then "http.credentialsValid" work Entry Attribute must be set to false. If the client is not authorized then the server sends a "Not Authorized" HTTP message.

#### Comment

Your own comments go here.

#### Detailed Log

If checked, will generate additional log messages.

#### WSDL Output to Filename

The name of the WSDL file to be generated when the "Generate WSDL" button is clicked. This parameter is only used by the WSDL Generation Utility – this parameter is not used during the Connector execution.

#### Web Service provider URL

The address on which web service clients will send web service requests. Also this parameter is only used by the WSDL Generation Utility – this parameter is not used during the Connector execution.

The **Generate WSDL** button runs the WSDL generation utility.

The WSDL Generation utility takes as input the name of the WSDL file to generate and the URL of the provider of the web service (the web service location). This utility extracts the input and output parameters of the AssemblyLine in which the Connector is embedded and uses that information to

generate the WSDL parts of the input and output WSDL messages. It is mandatory that for each Entry Attribute in the "Initial Work Entry" and "Result Entry" Schema the "Native Syntax" column be filled in with the Java type of the Attribute (for example, "java.lang.String"). The WSDL file generated by this utility can then be manually edited.

The operation style of the SOAP Operation defined in the generated WSDL is "rpc".

The WSDL generation utility cannot generate a <types...>...</types> section for complex types in the WSDL.

## Connector Operation

The Axis Easy Web Service Server Connector stores the following information from the HTTP/SOAP request into Connector Attributes, available to be mapped in (that is, if the request is a SOAP request):

- The name of the host to which the request is sent (the local host) – stored into the "host" Attribute.
- The requested HTTP resource – stored into the "requestedResource" Attribute.
- The value of the "soapAction" HTTP header – stored into the "soapAction" Attribute.
- The SOAP request message itself in text XML form – stored into the "soapRequest" Attribute.
- Whether the WSDL file was requested – in the "wsdlRequested" Attribute. In this case, the WSDL file is stored in the "soapResponse" Attribute, and none of the other Attributes are set.
- The parsed representation of the SOAP request in the "requestObjArray" Attribute.

This Connector parses the incoming SOAP request message and stores the Java representation of the SOAP request in the "requestObjArray" Connector Attribute. The Connector is capable of parsing both Document-style and RPC-style SOAP messages as well as generating (a) Document-style SOAP response messages, (b) RPC-style SOAP response messages and (c) SOAP Fault response messages. The style of the message generated is determined by the WSDL specified by the **WSDL File** Connector parameter.

The Connector is capable of parsing SOAP request messages and generating SOAP response messages which contain values of complex types which are defined in the <types> section of the WSDL document. In order to do that this Connector requires that (1) the **Complex Types** Connector parameter contains the names of all Java classes that implement the complex types used as request and response parameters to the SOAP operation and that (2) these Java classes' class files are located in the Java class path of TDI.

If during parsing the SOAP request an Exception is thrown by the parsing code, then the Connector generates a SOAP Fault Object (org.apache.axis.AxisFault) and stores it in the "soapFault" Connector Attribute.

This Connector is capable of parsing and generating SOAP response messages encoded using both "literal" encoding and SOAP Section 5 encoding. The encoding of the SOAP response message generated is determined by the WSDL specified by the **WSDL File** Connector parameter.

At the end of AssemblyLine processing in the Response channel phase, this Connector requires the Java representation (*Object[]*) of the SOAP response message from the "responseObjArray" Attribute of the *work* Entry to be mapped out. The Connector then serializes the SOAP response message, wraps it into an HTTP response and returns it to the web service client.

## See also

"Web Service Receiver Server Connector" on page 229.

---

## Btree Object DB Connector

The Btree Connector is a simple database capable of storing Java objects. Each object is uniquely identified by a value called the key. The Connector uses an underlying Btree implementation to store AssemblyLine **Entry** objects. This enables the user to store the **conn** and **work** entries using a unique key. This Connector is also used by the AssemblyLine's Delta feature, although in version 5.2 and later of the product the usage of the System Store is recommended for this purpose.

If you want to use the Btree implementation directly to store a Java object other than AssemblyLine entries, you must first get the Btree object and then use its methods directly.

### Notes:

1. The "Btree Object DB Connector" is deprecated with this release of IBM Tivoli Directory Integrator, and will be removed in a future version. Use the "System Store Connector" on page 179 instead, even for small data sets.
2. The "Btree Object DB Connector" creates a new Btree database if one does not exist. However, if you iterate on a non-existing database, it is created and the Iterator returns no values.
3. The Btree Connector excels at small, quick jobs, but because the Btree Connector does not automatically balance its data structures, it degrades significantly when sorted lists are entered containing a few thousand entries. For randomly-ordered data sets the limits are somewhat higher. For larger data sets, consider using the "System Store Connector" on page 179, or the bundled CloudScape™ database using a "JDBC Connector" on page 103 (also see "Using CloudScape database" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

## Configuration

The Connector needs the following parameters:

### DB Filename

The file path where the Btree data is stored.

### Key Attribute Name

The attribute name giving the unique value for the entry.

### Selection Mode

Specify **All**, **Existing** or **Deleted**. In order to use the **Existing** and **Deleted** keywords, the Connector (database) must have been used by an AssemblyLine with the delta enabled. When Delta is enabled on an Iterator using the Btree method, the AssemblyLine stores a sequence property in the database and also adds a sequence number to each entry read from the source.

### Detailed Log

If this field is checked, additional log messages are generated.

## Btree object

The `getDatabase()` method returns the underlying Btree object. This object can be used to store other Java objects than AssemblyLine entries. The following snippet shows how you can insert, search and replace objects in the database:

```
var bt = system.getConnector("btreedb");
bt.initialize (null);

var db = bt.getDatabase();
db.insert ("my key", new java.lang.String("my value"));
var value = db.search ("my key");
value = value + " - modified";
db.replace ("my key", value);
```

**Note:** The BTree Connector lets you Lookup or Update on the keyAttribute only. Also, the BTree Connector does not support the Advanced Link Criteria (see "Advanced link criteria" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

---

## Command line Connector

The command line Connector enables you to read the output from a command line or pipe data to a command line's standard input. Every command argument is separated by a space character, and quotes are ignored. The command is executed on the local machine.

**Note:** You do not get a separate shell, so redirection characters ( | > and so forth) do not work. To use redirection, make a shell-script (UNIX) or batch command (DOS) with a suitable set of parameters. For example, on a Windows system, type

```
cmd /c dir
```

to list the contents of a directory.

The Connector supports Iterator and AddOnly mode, as well as CallReply mode.

In Iterator and AddOnly mode, the command specified by the **Command Line** parameter is issued to the target system during Connector initialization, which implies it will only be issued once for the whole AssemblyLine lifetime.

However, in CallReply mode, the command is issued to the target system on each iteration of the AssemblyLine, after Output Attribute Mapping (call phase), and before Input Attribute Mapping (reply phase). In this mode, you must provide the command to be executed in an attribute called **command.line**; after it has executed you will find the output result in an attribute called **command.output**.

If a Parser is attached to the Command Line Connector, the output result will be parsed.

## Native-encoded output on some operating systems

When you use the Command Line Connector to run a program on a Windows operating system, the output from the program might be encoded using a DOS code page. This can cause unexpected results, because Windows programs usually use a Windows code page. Because a DOS code page is different from a Windows code page, it might be necessary to set the Character Encoding in the Command Line Connector's Parser to the correct DOS code page for your region; for example: cp850.

The same issue may arise on for example i5/OS®; here the output from commands is usually encoded in the IBM037 character set; and on z/OS® it could be EBCDIC.

Also see "Character Encoding conversion" on page 277.

## Some words on quoting

On Linux/Unix systems, this Connector has the capability to attempt to deal with the quoting of parameters that may contain lexically important characters. When the parameter **Use sh** is checked, TDI uses the sh program (e.g. the standard Linux shell) to run the command line, and sh will handle quoting as you expect. If you do not have sh on your operating system, do not check this box.

Without using sh, when the Command Line Connector is run on a Unix/Linux platform, it does not handle a command line with a parameter in quotes correctly. For example, the command:

```
Report -view fileView -raw -where "releaseName = 'ibmdi_60' and nuPathName like 'src/com/ibm/di%' "
```

This command should have the phrase "releaseName = 'ibmdi\_60' and nuPathName like 'src/com/ibm/di%' " as one parameter, but it does not. The reason is that TDI uses the Java Runtime exec() method, which splits all commands at spaces, and ignores all quoting. We would have liked this to be split according to the quotes. Checking **Use sh** (when possible) solves this problem.



## Configuration

The Connector needs the following parameters:

### Command Line

The command line to run. Used for Iterator and AddOnly modes only.

### Use sh

If enabled (by default it is not), will instruct the Connector to use sh-like parsing. Specifically, when this parameter is set to true the Connector is able to correctly parse quoted (using double-quotation marks) command line arguments which contain spaces.

This feature is only available on operating systems which provide the “sh” shell command interpreter (usually UNIX-like operating systems).

### Detailed Log

If this field is checked, additional log messages are generated.

**Parser** The Parser responsible for interpreting or generating entries.

## Examples

Refer to the *root\_directory/examples/commandLine\_connector* directory of your IBM Tivoli Directory Integrator installation.

## See also

“Remote Command Line FC” on page 373,

“z/OS TSO/E Command Line FC” on page 377



---

## Direct TCP /URL scripting

You might want to access URL objects or TCP ports directly, not using the Connectors. The following is example code that can be put in your Prolog:

### TCP

```
// This example creates a TCP connection to www.example_page_only.com
// and asks for a bad page

var tcp = new java.net.Socket ( "www.example_page_only.com", 80 );
var inp = new java.io.BufferedReader ( new java.io.InputStreamReader
    ( tcp.getInputStream() ) );
var out = new java.io.BufferedWriter ( new java.io.OutputStreamWriter
    ( tcp.getOutputStream() ) );

task.logmsg ("Connected to server");

// Ask for a bad page
out.write ("GET /smucky\r\n");
out.write ("\r\n");

// When using buffered writers always call flush to make sure data
// is sent on connection
out.flush ();

task.logmsg ("Wait for response");
var response = inp.readLine ();

task.logmsg ( "Server said: " + response );
```

### URL

```
// This example uses the java.net.URL object instead of the raw
// TCP socket object

var url = new java.net.URL("http://www.example_page_only.com");
var obj = url.getContent();

var inp = new java.io.BufferedReader ( new java.io.InputStreamReader
    ( obj ) );
while ( ( str = inp.readLine() ) != null ) {
task.logmsg ( str );
}
}
```



---

## Domino/Lotus Notes Connectors

In order to connect to a Domino Server or a Lotus Notes system, a discussion on what types of connections ("Session types" in Lotus Notes terminology) are possible, is appropriate. For these Connectors to operate, you will need to install a Domino/Lotus Notes client library, and the decision on which client library to install hinges on which Session Type is required.

### Session types

#### Local Client Session

Local client session calls to the Domino Server are based on Notes user ID.

A Notes client must be installed locally. This session type requires Notes.jar file to be present in the <TDI\_install\_folder>/jars/3rdparty/IBM folder and that the local client binaries are specified in the PATH system environment variable.

#### Local Server Session (Domino Local Session)

When creating this type of session, the ID file of the local server is used.

The host parameter in the Notes API method for creating session must be null. A reference to the current server such as a null server parameter in the session creation method means the local Domino environment is indicated. If a Local Client session is to be created, the user parameter is also required to be null which indicates to use the Notes user ID.

The local server is used only to create a session. However, servers connected to the local environment can still be accessed by specifying their names. The name is pointed as first parameter of the "getDatabase" methods of the lotus.domino.Session class.

For "Local Server" sessions you need to install Lotus Domino Server on the machine where TDI is installed.

#### IIOP Session and the IOR Parameter

An IIOP Session is a network based session, where the remote Domino server handles the client requests.

When an IIOP session is specified the Connector uses a Domino User Name and the Internet password of this user for authentication. The users' User Name and Internet password are parameters of the Connector. It is not necessarily the same user as the system local user ID. There are two approaches for the creation of an IIOP Session:

##### Provide the IOR String explicitly

The IOR is a text string required by the Domino Java API in order to establish an IIOP session to the Domino Server. The TDI 6.0 Domino Change Detection Connector uses a session creation method which obtains the IOR string from the Domino HTTP task. In TDI 6.1.1 Domino/Lotus Connectors the parameter "IOR String" is externalized. This parameter is optional. If this parameter is missing or has no value, IIOP sessions will be created as they used to in TDI 6.0. If this parameter is present in the Connector configuration the following methods from the Domino Java API will be used for session creation:

```
static public Session createSessionWithIOR(String IOR,
    String user, String passwd)
    throws NotesException

    static public Session createSessionWithIOR(String IOR,
    String args[], String user, String passwd)
    throws NotesException
```

Providing this Connector parameter improves the Connectors in two ways:

- It is no longer required that the Domino HTTP task be running in order for the Connector to function, thus lowering the Connector setup requirements.
- The Connector will be able to function when the Domino HTTP task is configured to use the SSL port only.

#### Get the IOR String from the HTTP task.

In this case, the **HTTP Port** parameter is used by the Connector to get the IOR String from the Domino Server using its HTTP task. If the Connector is to use the local client so as to create a session to the Domino Server, this port is not taken into account.

When creating an IIOP session SSL could be used. The Connector first tries to create a session using the value of the **IOR** parameter. If SSL is to be used, the Connector uses the session creation method that accepts an array of strings as a parameter. The **HTTP Port** parameter is used only when the **IOR** parameter is empty.

If SSL is used, the Connector tries to create a session using the following method:

```
static public Session createSession(String host, String args[],
String user, String password)
throws NotesException
```

In this case the value of the **HTTP Port** parameter is appended to the host. This method tries to get the IOR string from the Domino HTTP task that should run on this port. The task must not use this port to run SSL on it.

If SSL is not used, the Connector tries to create a session using the following method:

```
static public Session createSessionWithIOR(String host,
String user, String passwd)
throws NotesException
```

The port is appended to the host. The Domino HTTP task must run on this port without using SSL. The method will try to get the IOR string from the HTTP task and create an IIOP session.

These session types require `ncso.jar` file to be present in the `<TDI_install_folder>/jars/3rdparty/IBM` folder and that the local server binaries are specified in the `PATH` system environment variable.

### Supported session types by Connector

Table 1. Supported Domino/Lotus Notes Session types, per Connector

| Supported Sessions ►<br>Connectors ▼ | Local Client Session | Local Server Session | IIOP session |
|--------------------------------------|----------------------|----------------------|--------------|
| Domino Change Detection Connector    | Yes                  | No                   | Yes*         |
| Domino Users Connector               | Yes                  | Yes                  | No           |
| Lotus Notes Connector                | Yes                  | Yes                  | Yes          |

\*) The IIOP session connection type for the Domino Change Detection Connector is deprecated for this release, and may be removed in future versions of TDI.

**Note:** The Domino APIs for SSL are not JSSE compliant, and are instead Domino specific. This means that the TDI truststore and keystore do not play any part in SSL configuration for the Domino Change Detection Connector. For SSL configuration of the Domino Change Detection Connector, the `TrustedCerts.class` file that is generated every time the DIIOP process starts (in the Domino Server) must be in the classpath of TDI (`ibmditk` or `ibmdisrv`). You must copy the **TrustedCerts.class** to a local path included in the `CLASSPATH` or have the `Lotus\Domino\Data\Domino\Java` of your Domino installation

in the CLASSPATH. Whether the TDI Truststore or Keystore are set or not in the `global.properties` (or `solution.properties`) is of no consequence to this Connector.

## Java Class loader issue

Some of the classes in both the “Notes.jar” and “ncso.jar” libraries have exactly the same fully qualified Java class names. That is why if both jar files are in the Java class path, only one of them is loaded by the Java class loader. Since it is undefined which one will be loaded, one normally removes one of the jar files from the class path and leaves only the needed one. In this way only one type of Notes/Domino application session can be used at a time from a TDI component, because switching the type of the application session supported requires stopping the TDI server, changing the jar file and then starting the TDI server again.

The Domino Users Connector uses only the “Notes.jar” library as it does not create IIO sessions. That is why the “ncso.jar” library must not be in the Java class path. Thus other TDI components which need the “ncso.jar” library in order to establish an IIO session **cannot run** while the Domino Users Connector is running.

Correspondingly when the Connector runs with IIO sessions only “ncso.jar” must be presented in classpath and “Notes.jar” must be removed from it.

## Supported versions of Lotus Notes and Lotus Domino

These Connectors are supported on Domino R6, Domino R6.5 and Domino R7

## Native API call threading

When an AssemblyLine (containing Connectors) is executed by the TDI Server it runs in a single thread and it is only the AssemblyLine thread that accesses the AssemblyLine Connectors. The initializing Notes API, selecting entries, iterating through the entries and the termination of the Connector is performed by one worker thread.

A requirement of the Notes API is that when a **local session** is used each thread that executes Notes API functions must initialize the NotesThread object, before calling any Notes API functions. The Config Editor GUI threads do not initialize the NotesThread object and this causes a Notes exception.

There are several ways to initialize the NotesThread object. The way the Connectors use is to call the NotesThread.sinitThread method when a local session is created.

That is why the Domino Change Detection Connector and Domino Users Connector use their own internal thread to initialize the Notes runtime and to call all the Notes API functions. The internal thread is created and started on Connector initialization and is stopped when the Connector is terminated. The Connector delegates the execution of all native Notes API calls to this internal thread. The internal thread itself waits for and executes requests for native Notes API calls sent by other threads.

This implementation makes Connectors support the Config Editor GUI functionality and multithread access in general. The Lotus Notes Connector initializes the Notes runtime if local session is created.

## The ncso.jar file

In order to use IIO sessions, the TDI Lotus Notes/Domino components require the presence of the “ncso.jar” file.

From IBM Tivoli Directory Integrator 6.1.1, “ncso.jar” will no longer be shipped with the TDI product. You need to manually provide this file in order for the TDI Lotus/Domino components to function properly.

However, the "ncso.jar" file is shipped with the Domino Server. This file can be taken from the Domino installation (usually "<Domino\_root>\Data\domino\java\ncso.jar" on Windows platforms) and place it in the TDI\_root\jars\3rdparty\IBM folder, so that the TDI Server will load it on initialization. Since the "ncso.jar" will not be provided as part of the IBM Tivoli Directory Integrator 6.1.1 installation, some existing TDI 6.0 functionalities will change as follows.

## TDI Server

**The "-v" command-line option:** The TDI Server provides the "-v" command-line option which displays the versions of all TDI components. Since the "ncso.jar" file will not be provided as part of the TDI installation, if "ncso.jar" is not taken from the Domino server or Lotus Notes installation, messages like the following will be displayed (The components which do not rely on the "ncso.jar" have their versions displayed properly):

```
ibmdi.DominoUsersConnector:  
com.ibm.di.connector.dominoUsers.DominoUsersConnector:  
2006-03-03: CTGDIS001E The version number of the Connector is undefined
```

**The Server API `getServerInfo` method:** The Server API provides a method to request version information about TDI components (`Session.getServerInfo`). If version information is requested via the Server API about any of the Connectors which rely on "ncso.jar" and if this jar is not taken from the Domino server or Lotus Notes installation, an error is thrown. For example if the local Server API is accessed through a script like this:

```
session.getServerInfo().getInstalledConnectors()
```

the following error is displayed:

```
18:16:12 CTGDKD258E Could not retrieve version info for class  
'com.ibm.di.connector.DominoChangeDetectionConnector'.:  
java.lang.NoClassDefFoundError: lotus.domino.NotesException
```

## Running an AssemblyLine, IIOP Session

AssemblyLines which use a Connector (which uses an IIOP session) will fail to execute with a `NoClassDefFoundError` exception, if the "ncso.jar" file is not taken from the Domino Server or Lotus Notes installation.

## TDI Config Editor Aspects

**Component version table:** This is the table with the versions of all installed TDI components (available from menu "Help"->"About IBM Tivoli Directory Integrator Components"). This table will fail to display component versions for any of the Notes/Domino Connectors if neither the Notes.jar nor the ncso.jar is taken from the Domino/Notes installation

**Connector mode combo box:** The Connector mode combo box will display all existing TDI Connector modes (not only the supported ones) for the Notes/Domino Connectors, if neither the Notes.jar nor the ncso.jar is taken from the Domino/Notes installation.

**"Input Map" connection to the data source:** Attempting a connection to the data source from the "Input Map" tab for any of the Notes/Domino Connectors will display an error that the Connector could not be loaded, if the jar library is not taken from the Notes/Domino installation, whatever session is created.



## Domino Change Detection Connector

The Domino Change Detection Connector enables IBM Tivoli Directory Integrator 6.1.1 to detect when changes have occurred to a database maintained on a Lotus Domino server. The Domino Change Detection Connector retrieves changes that occur in a database (NSF file) on a Domino Server. It reports changed Domino documents so that other repositories can be synchronized with Lotus Domino.

**Note:** Refer to Supported session types by Connector for an overview of which session types are possible with this Connector.

When running the Connector reports the object changes necessary to synchronize other repositories with a Domino database, regardless of whether these changes have occurred while the Connector has been offline or they are happening while it runs.

The Domino Change Detection Connector operates in Iterator mode, and reports document changes at the Entry level only.

On each AssemblyLine iteration the Domino Change Detection Connector delivers a single document object which has changed in the Domino database. The Connector delivers the changed Domino document objects as they are, with all their current items and also reports the type of object change - whether the document was added, modified or deleted. The Connector does not report which items have changed in this document or the type of item change. After the Connector retrieves a document change, it parses it and copies all the document items to a new Entry object as Entry Attributes. This Entry object is then returned by the Connector.

This connector supports Delta Tagging at the Entry level only.

This Connector can be used in conjunction with the IBM Password Synchronization plug-ins. For more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.

The Connector stores locally, on the IBM Tivoli Directory Integrator 6.1.1 machine, the state of the synchronization. When started it continues from the last synchronization point and reports all changes after this point, including these changes that happened while the Connector was offline.

**Note:** Changed documents are not delivered in chronological order or in any other particular order, unless you check the "Deliver Sorted" checkbox in the configuration screen. Refer to "Sorting" on page 38 for more information. Without using this option, it means that documents changed later can be delivered before documents changed earlier and vice versa.

The Connector will signal end of data and stop when there are no more changes to report. It can however be configured not to exit when all changes have been reported, but stay alive and repeatedly poll Domino for changes.

### Using the Connector

**Document identification:** The Domino Change Detection Connector retrieves the Universal ID (UnID) of Domino documents. Use the UnID value to track document changes reported by the Connector.

For example, when a deleted document is reported, use its UnID value to lookup the object that has to be deleted in the repository you are synchronizing with. If you are synchronizing Domino users (Person documents), then you might need to find out when a user is renamed. When a user is renamed (the FullName item of the Person document is changed), the Connector will report this as a "modify" operation. When you lookup objects in the other repository by UnID, you will be able to find the original object, read its old FullName attribute, compare it against the new FullName value and determine that the user has been renamed.

**Deleted documents:** Documents that are deleted from a Domino database can be tracked by "deletion stub" objects. Deletion stubs provide the Universal ID and Note ID of the deleted document, but nothing more. That is why when the Connector comes across a deleted document, it returns an Entry which does not contain any document items, but only the following Entry Attributes added by the Connector itself:

- "\$\$UNID"
- "\$\$NoteID"
- "\$\$ChangeType"

**Minimal synchronization interval:** There is a parameter for each database called "Remove documents not modified in the last x days". Deletion stubs older than this value will be removed. If you are interested in processing deleted documents, you must synchronize (run the Connector) on intervals shorter than the value of this parameter.

On both Domino R6, Domino R6.5 and Domino R7, this parameter can be accessed from the Lotus Domino Administrator: open the database, then choose from the menu File|Replication|Settings..., select Space Savers – the parameter is called **Remove documents not modified in the last x days**.

The default value of this parameter is 90 days both on Domino R6, Domino R6.5 and Domino R7.

**Switching to a database replica:** UnIDs are the same across replicas of the same database. This allows you to switch to another replica of the Domino database in case the original database is corrupted or not available.

Document timestamps, however, are different for the different replicas. That is why when a switch to a replica is done, you must perform a full synchronization (use a new key for "Iterator State Key" and set the "Start At" parameter to "Start Of Data"). This will possibly report a lot of document additions and deletions which have already been applied to the other repository, but will guarantee that no updates are missed.

**The password prompt:** A password prompt blocks the Connector (and thus the AssemblyLine) until the password of the local Notes ID file is typed in.

**Note:** If the ID file has no password, then no password prompt is displayed. Thus it is possible to run an AssemblyLine that contains the Domino Change Detection Connector from within the Config Editor (without the password prompt blocking it).

**Structure of the Entries returned by the Connector:** All items contained in a document are mapped to Entry Attributes with their original item names.

All date values are returned as java.util.Date objects.

The following Entry Attributes are added by the Connector itself (their values are not available as document items):

- \$\$UNID – the Universal ID of the document (see "The \$\$UNID and \$\$NoteID Attributes")
- \$\$NoteID – the Note ID of the document (see "The \$\$UNID and \$\$NoteID Attributes")
- \$\$ChangeType – the type of document modification (see "The \$\$ChangeType Attribute")
- \$\$DateCreated – a java.util.Date object representing the time this document was created (this Attribute is available for non-deleted documents only).
- \$\$DateModified – a java.util.Date object representing the time of the last modification of this document (this Attribute is available for non-deleted documents only).

**The \$\$UNID and \$\$NoteID Attributes:** The Universal ID (UnID) is the value that uniquely identifies a Domino document. All replicas of the document have the same UnID and the UnID is not changed when the document is modified. This value should be used for tracking objects during synchronization. The

Universal ID value is mapped to the \$\$UNID Attribute of Entry objects delivered by the Connector. The value of the \$\$UNID Attribute is a string of 32 characters, each one representing a hexadecimal digit (0-9, A-F).

The Connector also returns the NoteID document values. This value is unique only in the context of the current database (a replica of this document will in general have a different NoteID). The Connector delivers the NoteID through the \$\$NoteID Entry's Attribute. The value of this Attribute is a string containing up to 8 hexadecimal characters.

**The \$\$ChangeType Attribute:** An Attribute named \$\$ChangeType is added to all Entries returned by the Domino Change Detection Connector.

The value of the \$\$ChangeType Attribute can be one of:

- **add** – means that the document reported is a newly added document in the Domino database
- **modify** – means that the document reported is an already existing document that has been modified
- **delete** – means that the document reported has been deleted from the Domino database

**Synchronization state values:** Several values are saved into the System Store and represent the current synchronization state. The Connector reads these values on startup and continues reporting changes from the right place.

Regardless of the mode in which the Connector is run two synchronization state values are stored in the User Property Store. These two values are stored in an Entry object as Attributes with the following names and meaning:

- **SYNC\_TIME** – this Attribute is a `java.util.Date` object representing the "since" value for the next poll of the Connector, that is, the next Connector's poll will return only database modifications that occurred at or after this time. In the special case when *Start Of Data* is used as a start condition, the `java.lang.String` value "NULL\_DATE" is stored.
- **SYNC\_CHECK\_DOCS** – this Attribute is a `java.lang.Boolean` object, which indicates whether the Connector must check for already processed documents in the Connector-specific System Store table (see below). This Attribute is only used when the Connector State Key Persistence parameter is set to *After read*. When the Connector State Key Persistence parameter is set to *End of cycle* the value of this Attribute is always **false**.

When the Connector is run, in addition to storing values in the User Property Store it creates (if not already created) a Connector-specific table in the System Store. The name of this table is the concatenation of "*domch\_*" and the value of the *Iterator State Key* Connector parameter. This Connector-specific table stores values with the following characteristics:

- The keys are the UnIDs of already delivered changed documents as `java.lang.String` objects
- The values are `java.util.Date` object representing the datetime for the next poll as it was at the time this document was delivered by the Connector; if however the UnID corresponds to a deleted document, the `java.lang.String` constant "NULL\_DATE" is stored instead.

The Connector-specific table is cleared each time the Connector successfully completes a synchronization session.

For each instance of the Domino Change Detection Connector executed on the same IBM Tivoli Directory Integrator Server there is a different Connector-specific table in the System Store.

**Accessing the Connector synchronization state:** While the Connector is offline you can access the "since" datetime that will be used on the next Connector run. This datetime is stored in the User Property Store.

This is how you can get the datetime value for the next synchronization:

```

var syncTime = system.getPersistentObject("dcd_sync");
var sinceDateTimeAttribute = syncTime.getAttribute("SYNC_TIME");
var sinceDateTime = sinceDateTimeAttribute.getValue(0);
if (sinceDateTime.getClass().getName().equals("java.util.Date")) {
main.logmsg("Start date: " + sinceDateTime);
}
else {
main.logmsg("Start date: Start Of Data");
}

```

"dcd\_sync" is the value specified by the **Iterator Store Key Connector** parameter.

This is how you can set a start datetime for the next synchronization:

```

var syncTime = system.newEntry();
syncTime.setAttribute("SYNC_TIME", new java.util.Date()); //current time
syncTime.setAttribute("SYNC_CHECK_DOCS", new java.lang.Boolean("false"));
system.setPersistentObject("dcd_sync", syncTime);

```

**Filtering entries:** No filtering of documents is performed in this version of the Connector. All database documents that have been created, modified or deleted are reported by the Connector.

If you need filtering you must do this yourself by scripting in the Connector hooks.

**Sorting:** The changed documents can be delivered sorted by the date they were last modified on. This is done by checking the checkbox "Deliver Sorted" in the configuration screen.

**Note:** Using sorting comes with a performance penalty, in terms of memory usage and CPU time. That is why you should consider carefully whether you really need sorting.

**Running from the Administration and Monitor Console (AMC):** When an AssemblyLine that contains the Domino Change Detection Connector is started from AMC it displays the Lotus Notes password prompt on the console of the IBM Tivoli Directory Integrator (TDI) Server. Since generally AMC and the TDI Server run on different machines, the AMC operator will not see this password prompt on the machine he or she works on. That is why the AMC operator might be tricked into thinking that the AssemblyLine is running properly, while at the same time it is waiting for the User ID password to be manually entered on the Server machine. Also, that is why when starting an AssemblyLine (that contains a Domino Change Detection Connector) from AMC, the AMC operator must see to it that the User ID password be manually entered on the IBM Tivoli Directory Integrator Server machine for the AssemblyLine to execute properly.

**Domino Server system time is used:** The Domino Change Detection Connector uses the timestamp of last modification for detecting changes in a Domino database. The Connector state includes timestamp values read by the Domino Server system clock. That is why changing the Domino Server system time while the Connector is running or between Connector runs might result in incorrect Connector operation – changes missed or repeated, incorrect change type reported, etc.

**Processing very large Domino databases (.nsf files):** The Connector could need a bigger amount of physical memory – for example, when working on very large databases containing 1,000,000 documents or more, especially when performing a full synchronization. This is caused by the Connector keeping all retrieved document UnIDs in memory for the duration of the synchronization session. For example, 512 MB of physical memory should be enough for processing a database that contains about 1,000,000 changed documents (provided that no other memory consuming processes are running). If this amount of memory is unavailable, then you can increase the memory available to IBM Tivoli Directory Integrator.

Also, be mindful of the "Deliver Sorted" parameter - enabling this could have a major performance impact.

**Checkpoint/Restart support:** The Domino Change Detection Connector supports the TDI Checkpoint/Restart functionality only when the **State Key Persistence** is set to "After Read". In this mode the Connector keeps track of the complete state of the synchronization process and is therefore able to restart the synchronization process if interrupted, that is, when run in this mode the Connector is capable of checkpoint/restart.

## Required Setup of the IBM Tivoli Directory Integrator

See the section, Supported session types by Connector and the sections below about the issue of required libraries, and possible library conflicts.

## Required Domino Setup

**Required Domino Server tasks:** The Connector requires that the following Domino Server tasks be started on the Domino Server:

- *HTTP Web Server*
- *DIOP Server*

If these Domino Server tasks are not started on the server the Connector will fail.

**Required user privileges:** The Domino Change Detection Connector creates two sessions to the Domino Server – a session through the local Notes client code using the local User ID file and a remote IOP session using an internet user account (the same Domino user can be used for establishing both sessions but this is not required). The accounts used for these sessions must have the following privileges:

### The account of the local User ID

The Domino user whose User ID file is deployed locally needs at least the "Reader" Access configured in the Access Control List (ACL) of the Domino database that is polled for changes. You can configure this from the "Files" tab of the Lotus Domino Administrator: right click on the database which will be polled for changes, select "Access Control -> Manage...". If you don't see the user name associated with this User ID file listed, click the "Add..." button and add this user name to the list. Select this user name in the list and make sure that the Access is set to "Reader" or higher (that is, "Reader", "Author", "Editor", "Designer" or "Manager") for this user.

### The internet account for the IOP session

The Connector needs the username and password of a Lotus Domino Internet user for creating the IOP session. The Internet user must have at least the "Reader" Access configured in the Access Control List (ACL) of the Domino database that is polled for changes.

You can configure this from the "Files" tab of the Lotus Domino Administrator: right click on the database which will be polled for changes, select "Access Control -> Manage...". If you don't see the Internet user listed, click the "Add..." button and add the Internet user to the list. Select the Internet user name in the list and make sure that the Access is set to "Reader" or higher (that is, "Reader", "Author", "Editor", "Designer" or "Manager") for this user.

## Configuration

The Domino Change Detection Connector provides the following parameters:

### Session Type

Specifies whether the Connector will create an IOP session or performs Local Client calls. This is a drop-down list; the default value is "IOP". Note that the IOP session connection type for this Connector is deprecated; future version of TDI will only support Local Client calls, at which time this parameter will be removed.

### Domino Server IP Address

The IP address of the Domino Server where the database that will be polled for changes resides.

### IOR String

The IOR string used to create the IOP session.

**HTTP Port**

The port on which the HTTP task of the Domino Server is running. The default value is 80.

**User Name**

The name of the user used for the Java IIOp session authentication as specified by the first value of the User name field of the user's Person document.

**Internet Password**

The password of the user used for the Java IIOp session authentication as specified in the "Internet password" field of the user's Person document.

**Database**

The filename of the Domino database which will be polled for changes, for example "names.nsf".

**Iterator State Key**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This should be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator's User Property Store.

The **Delete** button clears all synchronization state associated with the value of this parameter. When clicked, the **Delete** button deletes the key-value pair from the User Property Store as well as the Connector-specific table from the System Store.

**Start At**

The type of starting condition. Can be one of:

**Start Of Data**

Performs a full synchronization retrieving all documents from the database.

**End Of Data**

Retrieve future changes only (changes that are done after the connector is run once.)

**Specific date**

Retrieve changes that occurred at or after the value specified by the **Start Date** parameter.

The default value is "**Start Of Data**".

**Note:** This parameter is taken into account only when the persistent parameter specified by **Iterator State Key** is not found in the User Property Store.

**Start Date**

The Connector will retrieve documents which have been changed at or after this date/time. This parameter accepts the following date/time formats:

- **yyyy-MM-dd HH:mm:ss.SSS** — for example: 2002-05-23 16:39:07.628 (that is 4-digit year, 2-digit month, 2-digit day, 2-digit 24-hour hour, 2-digit minutes, 2-digit seconds and 3-digit milliseconds). Please note that the actual precision of Lotus Notes date/times is 10 milliseconds.
- **yyyy-MM-dd HH:mm:ss** — for example: 2002-05-23 16:39:07
- **yyyy-MM-dd** — for example: 2002-05-23

It is only taken into account when the persistent parameter specified by "**Iterator State Key**" is not found in the System Store and the "**Start At**" parameter is set to "**Specific Date**".

**State Key Persistence**

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and choices are:

**After Read**

Updates the System Store when you read an entry from the Domino change log, just before you continue with the rest of the AssemblyLine. This mode of operation was called "Assured once and only once delivery" in older versions of TDI.

### End of Cycle

Updates the System Store when all Connectors and other components in the AssemblyLine have been evaluated and executed.

### Manual

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the Domino Change Detection Connector's *saveStateKey()* method, at a suitable place at your discretion in your AssemblyLine.

### Timeout

Specifies the maximum number of seconds the Connector waits for the next changed document. If this parameter is 0, then the Connector waits forever. If the Connector has not retrieved the next changed document object within timeout seconds from the beginning of the waiting, then it returns a NULL Entry, indicating that there are no more Entries to return.

### Sleep Interval

Specifies the number of seconds the Connector sleeps between successive polls for changes.

### Use SSL

Enables encrypted communications with the Domino server, using client-side certificates. The parameter is relevant only for IIOP Sessions.

### Deliver Sorted

If checked, the changed documents are delivered sorted by the date they were last modified on; otherwise the changed documents are delivered in random order.

### Detailed Log

Check for additional log messages.

## Troubleshooting the Domino Change Detection Connector

- Problem:** When you run an AssemblyLine that uses the Domino Change Detection Connector, just after you enter the User ID password at the password prompt the AssemblyLine fails with the following exception: *NotesException: Could not get IOR from Domino Server: ...* where *<domino\_server\_ip>* is the IP address of the Domino Server you are trying to access, that is, the value of the **Domino Server IP address** Connector parameter.

**Solution:** This exception indicates that the HTTP Web Server task on the Domino Server is not running. Start the HTTP Web Server task on the Domino Server you are trying to access and then start your AssemblyLine again.
- Problem:** When you run an AssemblyLine that uses the Domino Change Detection Connector, just after you enter the User ID password at the password prompt the AssemblyLine fails with the following exception: *NotesException: Could not open Notes session: org.omg.CORBA.COMM\_FAILURE: java.net.ConnectException: Connection refused: connect Host: <domino\_server\_ip> Port: XXXXX vmcid: 0x0 minor code: 1 completed: No* where *<domino\_server\_ip>* is the IP address of the Domino Server you are trying to access, that is, the value of the **Domino Server IP address** Connector parameter.

**Solution:** This exception indicates that the DIIOP Server task on the Domino Server is not running. Start the DIIOP Server task on the Domino Server you are trying to access and then start your AssemblyLine again.
- Problem:** While the Domino Change Detection Connector is retrieving changes the following exception occurs: *Exception in thread "main" java.lang.OutOfMemoryError*

**Solution:** This exception indicates that the memory available to the IBM Tivoli Directory Integrator Java Virtual Machine (the JVM maximum heap size) is insufficient. In general the Java Virtual Machine does not use all the available memory. You can increase the memory available to the IBM Tivoli Directory Integrator JVM by doing the following:

## Windows platforms

Edit *ibmdisrv.bat* in the IBM Tivoli Directory Integrator install directory to adjust the existing `-Xms16m` option to `-Xms254m -Xmx1024m` in the next to last line of the file (i.e. the line that invokes java).

**Note:** `-Xms` is the initial heap size in bytes and `-Xmx` is the maximum heap size in bytes. You can set these values according to your needs.

This will have no effect if you are trying to run an AssemblyLine with a memory problem from the Config Editor (ibmditk), as the Config Editor starts a new instance of the JVM to run the AssemblyLine; with default parameters. In order to accommodate this situation, you need to do the following:

- a. Edit the `global.properties` or `solution.properties` file to alter the settings of `com.ibm.di.javacmd` to refer to a batch file. (for example, `com.ibm.di.javacmd=c:\Program Files\IBM\TDI\V6.1\myjava.bat`)
- b. Create a command file (the aforementioned `c:\Program Files\IBM\TDI\V6.1\myjava.bat`) containing the appropriate Java invocation command, like `"javaw" -Xms254m -Xmx1024M %*`

Now the CE will use the modified JVM invocation, with increased heap size.

## Unix/Linux platforms

Edit *ibmdisrv* in the IBM Tivoli Directory Integrator install directory to adjust the existing `-Xms16m` option to `-Xms254m -Xmx1024m` in the last line of the file (i.e. the line that invokes java).

**Note:** `-Xms` is the initial heap size in bytes and `-Xmx` is the maximum heap size in bytes. You can set these values according to your needs.

This will have no effect if you are trying to run an AssemblyLine with a memory problem from the Config Editor (ibmditk), as the Config Editor starts a new instance of the JVM to run the AssemblyLine; with default parameters. In order to accommodate this situation, you need to do the following:

- a. Edit the `global.properties` or `solution.properties` file to alter the settings of `com.ibm.di.javacmd` to refer to a batch file. (for example, `com.ibm.di.javacmd=/opt/IBM/TDI/V6.1/myjava.bat`)
- b. Create a command file (the aforementioned `/opt/IBM/TDI/V6.1/myjava.bat`) containing the appropriate Java invocation command, like `"java" -Xms254m -Xmx1024M $*`

Now the CE will use the modified JVM invocation, with increased heap size.

4. **Problem:** The Connector reports all database documents as *deleted* although they are not deleted.

**Solution:** The user of the local User ID file is not given the necessary privileges on the database polled for changes. Give the necessary user rights as described in the "Required user privileges" section.

5. **Problem:** When you run an AssemblyLine that uses the Domino Change Detection Connector, the following exception occurs: `java.lang.UnsatisfiedLinkError: <TDI_install_folder>\libs\domchdet.dll: Can't find dependent libraries` where `<TDI_install_folder>` is the folder where IBM Tivoli Directory Integrator is installed.

**Note:** If you run the Integrator Server from the command prompt, then before this exception message is printed, a popup dialog box appears saying "This application has failed to start because nNOTES.dll was not found. Re-installing the application may fix this problem."

**Solution:** This exception message as well as the popup dialog box are displayed because the Connector is unable to locate the Lotus Notes dynamic-link libraries. Most probably the path to the Lotus Notes directory specified in `ibmditk.bat` or in `ibmdisrv.bat` is either incorrect or not specified at all. That is why you should verify that the Lotus Notes directory specified in the PATH environment



variable in both `ibmditk.bat` and `ibmdisrv.bat` is correct. For more information please see the "Required Setup of the IBM Tivoli Directory Integrator" section.

**Compatibility:** Refer to the section on Supported session types by Connector on how this connector should be set up with the necessary libraries, and about incompatibilities with other Domino®/Lotus Notes® Connectors.



## Domino Users Connector

The Domino Users Connector provides access to Lotus® Domino user accounts and means for managing them. With it, you can do the following:

- Retrieve users documents and their items from the Name and Address Book
- Create and register Domino users
- Initiate Domino users deletion (through the Domino Administration Process) by posting administration requests to the Administration Requests Database
- Modify users by modifying their Person documents in the Name and Address Book
- Perform users' "disabling/enabling" by adding/removing users' names to/from a "Deny Access Group"
- Perform "lookup" of Domino users.

Currently, the Connector does not support the process of Users recertifying.

The Domino Server accessed can be on a remote server, or on the local machine.

It operates in Iterator, Lookup, AddOnly, Update and Delete modes, and enables the following operations to be performed:

### Iterator

Iterate over all (or a filtered subset of) Person documents from the Name and Address Book.

The Connector iterates through the Person documents of the 'Name and Address Book' database. All Person documents (matching the filter, if filter is set) are delivered as Entry objects, and all document items, except attachments, are transformed into Entry Attributes.

Along with the Attributes corresponding to the Person document items, the Entry returned by the Connector will contain some extra Attributes, created by the Connector itself. The table below describes these Attributes. Their names will be prefixed with "DER\_" to indicate that they have been derived by the Connector, and they are not "native" Domino Attributes):

Table 2. Derived Attributes

| Attribute Name | Type    | Value  |
|----------------|---------|--|
| DER_IsEnabled  | Boolean | <i>true</i> – if the user does not belong to a "Deny List only" group;<br><i>false</i> – if the user belongs to at least one group of type "Deny List only". |

### Lookup

Search for and retrieve Person documents that match some criteria.

In Lookup mode, the Connector will perform different type of searches, depending on the value of the "useFTSearch" parameter:

- "useFTSearch" = "true": The Connector will perform a full-text search in the "People" view.

**Note:** "Full-text search" will work both with full-text indexed and not full-text indexed databases; however, the search will be less efficient if the database is not full-text indexed.

It is also possible that the database full-text index will not be updated, in which case the search results would not match the actual database content.

- "useFTSearch" = "false": the Connector will perform a regular database search using Lotus formula. The element (Form = "Person") will be automatically added to the formula by the Connector, so the search will be limited to user documents only.

### AddOnly

Register new users in Domino Server and create their Person documents. When doing so, you

have the option to specify a mail template when registering users. If a template is not specified the Connector will continue to work as the TDI 6.0 version of the Connector (that is, use the default template).

#### **Update**

Modify users' Person documents; Enable/disable users; Register existing (internet) users, as well as "disabling/enabling" by adding/removing users' names to/from a "Deny Access Group".

**Delete** Post requests for user deletion in the Domino Server Administration Requests Database.

This Connector can be used in conjunction with the IBM Password Synchronization plug-ins. For more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.

**Note:** Domino Users Connector requires Lotus Notes to be release 6.0 or 6.5; and Lotus Domino Server version 6.0 and 6.5..

### **Deployment and connection to Domino server**

Refer to the section, Supported session types by Connector for more information about required libraries setup, and possible library conflicts.

#### **Deploying on a Domino Server machine**

When the Domino Users Connector is deployed on a machine where a Domino Server is installed you can use both Authentication mechanisms supported – Internet Password authentication and Notes ID File authentication.

#### **Deploying on a Notes client machine**

When the Domino Users Connector is deployed on a machine where a Notes client is installed you can only use Notes ID File authentication.

To authenticate the local server connection, Domino requires the user's short name and internet password (these are Connector's parameters).

### **Configuration**

The Connector needs the following parameters:

#### **Domino Server IP Address**

The IP Address of the Domino Server, which hosts the 'Name and Address Book' Database.

If this parameter is missing or empty, the local machine is used. This behavior ensures backward compatibility with pre-6.1 TDI configuration files.

#### **Name and Address Book Database**

The name of the Domino Directory database (previously known as the "Name and Address Book" database). Usually it is "names.nsf" (default)

#### **Authentication Mechanism**

Specifies the authentication mechanism used by the Connector.

When "Internet password" authentication is selected, the **userName** Connector parameter must set to the Domino user's Short Name and the **password** Connector parameter must be set to the Domino user's Internet password.

When "Notes ID File" authentication is selected, the **userName** Connector parameter is ignored, because the Domino user to be used is unambiguously identified by the currently configured default Notes ID file. When "Notes ID File" authentication is selected, the **password** Connector parameter must be set to the password of the currently configured default Notes ID file.

For more information about the two supported authentication mechanism, please see the "Authentication" section.

## Username

The user name used for log in or authentication to the Domino Server. Ignored if "Notes ID File" authentication is selected. See "Authentication" on page 48 for more details.

## Password

The password for the **Username**, or password associated with the Notes ID File if that type of authentication is used. See "Authentication" on page 48 for more details.

## Use full-text search

If checked, the Connector accesses user documents through the **People** view and full-text searches. If not checked, the Connector uses regular database searches. In this case the Connector automatically narrows the database search to user documents only, by accessing only documents for which **Form item** value is **Person**. This parameter affects the Iterator and Lookup modes only.

## Full-text filter

This value is taken into account only when **Use full-text search** is enabled. This parameter contains full-text query that filters the user documents returned by the Connector in Iterator mode. If null or empty string, no filtering is performed. Default value is " ".

## Formula filter

This value is taken into account only when **Use full-text search** is not enabled. This parameter contains a formula that filters the users returned by the Connector in Iterator mode. The Connector automatically adds the following to this formula:

```
"& Form = "Person""
```

which limits the search to user documents only. Default value is " ".

## Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Security

To have the IBM Tivoli Directory Integrator access the Domino Server, you might have to enable it through **Domino Administrator -> Configuration -> Current Server Document -> Security -> Java/COM Restrictions**. The user account you have configured the IBM Tivoli Directory Integrator to use must belong to a group listed under **Run restricted Java/JavaScript/COM** and **Run unrestricted Java/JavaScript/COM**.

**Configuring encryption between the Domino Server and a client:** When the Domino Users Connector is running on a Notes client machine, there is communication going on between the Notes client machine and the Domino Server machine.

Port encryption in Domino and/or Notes can be used to encrypt this communication. Two options are available:

### Encrypt Domino Server communication ports

This is easier to setup (the Server settings only are configured), but this affects the communication with all clients including regular users using Lotus Notes clients.

1. In Lotus Domino Administrator select **Configuration**.
2. Select **Server/Server Ports...** from the right-side panel.
3. For each communication port in use, select the port in the **Communication ports** list and check the **Encrypt network data** option.
4. Click **OK**.
5. Restart the Domino Server for changes to take effect.

### Encrypt Lotus Notes communication ports

This does not affect other Notes clients if encryption is not necessary for them.

1. In Lotus Notes go to **File->Preferences->User Preferences...**
2. Select **Ports** from the left navigation panel.

3. For each communication port in use, select the port in the **Communication ports** list and check the Encrypt network data option.
4. Click **OK**.
5. Restart Lotus Notes for changes to take effect.

**Authentication:** The Domino Users Connector impersonates as a Domino user in order to access the Domino Directory (Names and Address Book database).

The Domino Users Connector supports two authentication mechanisms – Internet Password authentication and Notes ID file based authentication.

#### **Internet Password Authentication**

This authentication mechanism uses the Domino user's Short Name and Internet password. The Domino user's Short Name and Internet password must be supplied as Connector configuration parameters **Username** and **Password**.

The Domino Users Connector uses this mechanism in order to create an Internet Session object for making local calls based on the Domino Directory. This authentication mechanism requires that a Domino Server is installed on the local machine.

#### **Notes ID File Authentication**

This authentication mechanism uses the currently configured default Notes ID file along with its password.

The currently configured default Notes ID file is a part of the Notes client configuration. Normally the Notes client stores the path to the currently configured default Notes ID file in the notes.ini file, so that when the next time Notes client starts it will use this Notes ID file by default.

The password of the Notes ID file must be supplied as a Connector configuration parameter **Password**.

The Domino Users Connector uses this authentication mechanism in order to create a Session object for making local calls based on the Notes user ID. A Domino server or Notes client must be installed locally.

This authentication mechanism can be used both on a Notes client machine and on a Domino Server machine. When this mechanism is used on a Domino Server machine the Server ID file is used. Normally Server ID files do not have passwords or have empty passwords; that is why you would normally leave the **Password** Connector configuration parameter blank. If, however, the Server ID file does have a password you should specify that password as the value for the **Password** Connector configuration parameter.

**Authorization:** The Domino Server uses the Access Control Lists of the Domino Directory (Names and Address Book database) to verify that the Domino user which the Connector uses has actually the right to access the required database, document or field.

If the Connector is used to change the FirstName or LastName or both of a Domino user, then the Access Control Lists of databases to which the user used to have access before the renaming occurred must be updated manually, so that the new user name would be recognized.

### **Using the Domino Connector**

**Iterator mode:** The Connector iterates through the Person documents of the **Name and Address Book** database. All Person documents (matching the filter, if filter is set) are delivered as Entry objects, and all document items, except attachments, are transformed into Entry attributes.

Along with the attributes corresponding to the Person document items, the Entry returned by the Connector contains some extra (derived) attributes for which values are calculated by the Connector. Here is the list of the derived attributes:

**DER\_IsEnabled**

(Boolean) Specifies whether the user is enabled/disabled:

- **true** - if the user does not belong to a **Deny List only** group
- **false** - if the user belongs to at least one **Deny List only** group

**Lookup mode:** In Lookup mode, the Connector performs searches for user documents, and the type of search depends on the value of the **Use full-text search** parameter:

- **Use full-text search = true:** The Connector performs a full-text search in the People view. Full-text searches work both with full-text indexed and not full-text indexed databases. However, the search is less efficient if the database is not full-text indexed. It is also possible that the database full-text index is not updated, in which case the search results do not match the actual database content.
- **Use full-text search = false:** The Connector performs a regular database search using Lotus formula. The element (Form = "Person") is automatically added to the formula by the Connector, so the search is limited to user documents only.

When simple link criteria are used, you can use both canonical (CN=UserName/O=Org) and abbreviated (UserName/Org) name values to specify the user's FullName. The Connector automatically processes and converts the value you specified, if necessary.

When advanced link criteria is used, you must be careful and specify the user's FullName in the correct format, which is:

- for full-text search: use abbreviated names (UserName/Org)
- for regular database search: use canonical names (CN=UserName/O=Org)

**AddOnly mode:** The AddOnly mode always adds a new Person document in the **Name and Address Book** database. The add process accepts whatever attributes are provided by the Attribute Mapping, however to have correct user processing by Domino, the attribute names must match the **Item** names Domino operates with. As the Connector operates with users only, it always sets the attributes **Type** and **Form** to the value of **Person**, thus overriding any values set to these attributes during the Attribute Mapping process. The **LastName** Domino user attribute is required for successful creation of a Person document. The HTTPPassword attribute is not required, but if present its value is automatically hashed by the Connector.

Depending on a fixed schema of attributes, the Connector can register the new user. The table below specifies these attributes and the Connector behavior according to their presence or absence in the **conn** Entry, and their values:

| Attribute name      | Type    | Required for registration? | Value   |
|---------------------|---------|----------------------------|---|
| REG_Perform         | Boolean | Yes                        | If set to true the Connector performs user registration. If this attribute is missing, or its value is false, the Connector does not perform user registration, regardless of the presence and the values of the other REG_ Attributes. |
| REG_IdFile          | String  | Yes                        | Contains the full path of the ID file to be registered. For example,<br>c:\newuserdata<br>\newuser.id   |
| REG_UserPw          | String  | No                         | The user's password.  |
| REG_CertifierIDFile | String  | Yes                        | The full file path to the certifier ID file.  |

| Attribute name           | Type               | Required for registration? | Value  |
|--------------------------|--------------------|----------------------------|--|
| REG_CertPassword         | String             | Yes                        | The password for the certifier ID file.<br><b>Note:</b> If the certifier password is wrong when registering users, a popup window is displayed. Ensure that the Certifier password is correctly specified.   |
| REG_Server               | String             | No                         | The name of the server containing the user's mail file. If this attribute is missing, the value is obtained from the Connector's Domino Session object.  |
| REG_CreateMailDb         | Boolean/String     | No                         | true - Creates a mail database false - Does not create a mail database; it is created during setup. If this attribute is missing, a default value of false is assumed. If this attribute is true, the MailFile attribute must be mapped to a valid path.                                       |
| REG_Expiration           | Date               | No                         | The expiration date to use when creating the ID file. If the attribute is missing, or its value is null, a default value of the current date + 2 years is used.  |
| REG_IDType               | Integer/String     | No                         | The type of ID file to create: 0 - create a flat ID 1 - create a hierarchical ID 2 - create an ID that depends on whether the certifier ID is flat or hierarchical. If the attribute is missing, a default value of 2 is used.   |
| REG_IsNorthAmerican      | Boolean/String     | No                         | true - the ID file is North American false - the ID file is not North American. If this attribute is missing, a default value of true is used.   |
| REG_OrgUnit              | String             | No                         | The organizational unit to use when creating the ID file. If this attribute is missing, a default value of " " is used.  |
| REG_RegistrationLog      | String             | No                         | The log file to use when creating the ID file. If this attribute is missing, a default value of " " is used.   |
| REG_StoreIDInAddressBook | Boolean/String     | No                         | true - stores the ID file in the server's Domino Directory false - does not store the ID file in the server's Domino Directory. If this attribute is missing, a default value of false is used.  |
| REG_RegistrationServer   | String             | No                         | The server to use when creating the ID file. This attribute is used only when the created ID is stored in the server Domino Directory, or when a mail database is created for the new user.  |
| REG_MinPasswordLength    | Integer/String     | No                         | The REG_MinPassword Length value defines the minimum password length required for subsequent changes to the password by the user. The password used when the user registers is not restricted by the REG_MinPassword Length value. If this attribute is missing, a default value of 0 is used. |
| REG_Forward              | String             | No                         | The forwarding domain for the user's mail file.  |
| REG_AltOrgUnit           | Vector of <String> | No                         | Alternate names for the organizational unit to use when creating ID file.  |



| Attribute name         | Type               | Required for registration? | Value  |
|------------------------|--------------------|----------------------------|--|
| REG_AltOrgUnit<br>Lang | Vector of <String> | No                         | Alternate language names for the organizational unit to use when creating ID file. |

The attributes for which the **Required for registration** field is set to **Yes** are required for successful user registration. Along with these REG\_ Attributes, the **LastName** Domino user attribute is also required for successful user registration.

If REG\_Perform is set to **true** and any of the other attributes required for registration are missing, the Connector throws an Exception with a message explaining the problem.

**Update mode:** In Update mode, the following happens:

1. A search for the Entry to be updated is performed in Domino.
2. If an Entry is not found, an AddOnly operation is performed as described in the AddOnly mode (including user registration if the necessary REG\_ Attributes are supplied).
3. If the Entry is found, a modify operation is performed.

When modifying a user, the Domino Users Connector always modifies its Person document in the **Name and Address Book** database with the attributes provided. The modify process accepts whatever Attributes are provided by the Attribute Mapping, however to have correct user processing by Domino, the Attribute names must match the **Item** names Domino operates with. See "List of Domino user attributes (or Person document items)" on page 54 for a (possibly not full) list of Domino user properties.

As the Connector operates with users only, it does not modify the attributes **Type** and **Form** (their value must be **Person**) regardless of the Attribute Mapping process. If the **HTTPPassword** attribute is specified, its value is automatically hashed by the Connector.

In the process of modifying users, the Domino Users Connector provides the options to disable and enable users. A user is disabled by adding his name into a specified **Deny List only** group (consult the Domino documentation for information on **Deny List only** groups. Go to <http://www.lotus.com/products/domdoc.nsf>, and click the **Lotus Domino Document Manager 3.5** link). A user is enabled by removing his name from all **Deny List only** groups.

The Connector performs user disabling or enabling depending on the presence in the **conn** Entry, and the values of the following Entry attributes:

#### ACC\_SetType

(Integer/String) If this attribute is missing, no actions are performed and the user keeps its current disable/enable status. If this Attribute is provided, its value is inspected:

- **0** - The Connector performs the operation **disable user** (the user's name is placed in the group specified by the **ACC\_DenyGroupName** attribute).
- **1** - The Connector performs the operation **enable user** (any other value results in Exception).

#### ACC\_DenyGroupName

(String) The name of the **Deny List only** group where the user's name is added when disabling the user. When the value of **ACC\_SetType** is **0**, the **ACC\_DenyGroupName** attribute is required. If it is missing or its value specifies a non-existing **Deny List only** group, an Exception is thrown. When the **ACC\_SetType** attribute is missing, or its value is **1**, the **ACC\_DenyGroupName** attribute is not required and its value is ignored.

The Connector can perform user registration on modify too. To determine whether or not to perform registration, the same rules apply as in the AddOnly mode. The same schema of attributes is used and all REG\_ Attributes have the same meaning.

If the REG\_Attributes determine that registration is performed, the following cases might happen:

- The user has not yet been registered (for example, this can be an internet or Web user that you want to register and enable to log on and work through a Notes client). The user is then registered, a new ID file is created, and so forth.
- The user has already been registered. In this case the user is re-registered, for example, the Domino registration values are reset with the new values provided. A new ID file is also created.

**Notes:**

1. When registering users on modify, turn off the **Compute Changes** Connector option. When turned on, the **Compute Changes** function might clear attributes required in certain variants of user registration, and this results in registration failure.
2. When registering users on modify, you must know beforehand what is the user's FullName after registration, and you must provide the attribute **FullName** in the **conn** Entry with this value (which is probably constructed by scripting). This is not very convenient and requires deep knowledge of the Domino registration process. Without setting the expected user's FullName beforehand, however, you risk registering a new user instead of the existing one.
3. When registering users on modify, you must provide the attribute **FirstName** in the **conn** Entry with the value of the FirstName of the user you need to register. If the **FirstName** attribute is not provided, you risk creating a new user.

**Delete mode:** For user deletion, the Connector uses the Domino Administration Process.

The Connector posts **Delete in Address Book** requests in the **Administration Requests** Database . Each request of type **Delete in Address Book**, when processed by the Domino Administration Process, triggers the whole chain of posting and processing administration requests and actions performed by the Administration Process to delete a user. The result of posting a **Delete in Address Book** administration request is the same as manually deleting a user through the Domino Administrator. In particular:

- The time of processing the administration requests depends on the Domino Server configuration.
- Depending on the type of deletion requested, the chain of administration requests can include requests that require Administrator's approval (for example, the **Approve File Deletion** request for deleting the user's mail file).

The Connector enables tuning of each single user deletion it initiates. The parameters that can be configured are:

**Delete mail file**

You can specify one of the following options:

- Don't delete mail file.
- Delete just the mail file specified in Person document.
- Delete mail file specified in Person document and all replicas.

**Add to group**

Specifies if the user's name must be placed in a group when deleting the user, and if **yes**, specifies the name of the group too. This option is usually used to add the user in a **Deny List only** group when deleting the user; thus the user is denied access to the servers.

The delete parameters described previous, have default values that can also be changed through APIs provided by the Domino Users Connector. Each time an instance of the Domino Users Connector is created (in particular on each AssemblyLine start), the parameters have the following default values:

**Delete mail file**

Don't delete mail file.

**Add to group**

On deletion, do not add the user's name in any group.

If the default values fit the type of deletion you want, then no special configuration for the deletion is needed. You must specify the correct link criteria in the Delete Connector.

You can however use the APIs provided by the Domino Users Connector, to change these default values at runtime (using scripting):

#### **int getDeleteMailFile()**

Returns the code of the default value for the Delete mail file parameter:

- **0** - Don't delete mail file.
- **1** - Delete just the mail file specified in Person document.
- **2** - Delete mail file specified in Person document and all replicas.

#### **void setDeleteMailFile (int deleteType)**

Sets the default value for the Delete mail file parameter. The **deleteType** method's parameter must contain the code of the desired value (the codes are as described for getDeleteMailFile()).

#### **String getDeleteGroupName()**

Returns the default value for the Add to group parameter:

- **NULL** - Means **Do not add the user's name in any group.**
- **Non-NULL value** - The name of the Group where the user's name is added.

#### **void setDeleteGroupName (String groupName)**

Sets the default value for the Add to group parameter:

- **NULL** - Specifies that the user's name must not be added in any group on deletion.
- **Non-NULL String value** - Specifies the name of the group where the user's name is added on deletion.

The default values for the delete parameters are used in all deletions performed by the Connector, until another change in their values is made, or the Connector instance (object) is destroyed.

The following are possible scenarios that use these methods:

- Script code in the **Before Delete** hook checks the values of the **work** and **conn** objects (and everything else it needs to check), and depending on the specific decision logic uses the **setDeleteMailFile** and **setDeleteGroupName** to tune each particular user deletion.
- If all users for deletion must be deleted using one pattern (and there is no need to tune each particular user deletion), script code in the AssemblyLine Prolog can use the **setDeleteMailFile** and **setDeleteGroupName** methods and set the desired values for the whole process.

Another method to manipulate the delete parameters, is to provide the following attributes in the **conn** Entry:

#### **DEL\_DeleteMailFile**

(Integer/String)

If this attribute is missing in the **conn** Entry, the default value for **Delete mail file** is used.

If this attribute is provided in the **conn** Entry, its value determines the value for the **Delete mail file** parameter for the current deletion only:

- **0** - Don't delete mail file.
- **1** - Delete just the mail file specified in Person document.
- **2** - Delete mail file specified in Person document and all replicas.

#### **DEL\_DeleteGroupName**

(String)

If this attribute is missing in the **conn** Entry, the default value for **Add to group** is used.

If this attribute is provided in the **conn** Entry, its value determines the value for the **Add to group** parameter for the current deletion only:

- NULL - Specifies that the user's name must not be added in any group.
- Non-NULL String value - Specifies the name of the group where the user's name is added.

The use of the **DEL\_DeleteMailFile** and **DEL\_DeleteGroupName** attributes in the **conn** Entry overrides the default values of the corresponding delete parameters for the current deletion only.

Setting the **DEL\_DeleteMailFile** and **DEL\_DeleteGroupName** attributes in the **conn** Entry can be done through scripting in the **Before Delete** hook. Adding attributes by scripting might not be very convenient, so you might prefer to use the default delete parameters values and the APIs that change them.

### **List of Domino user attributes (or Person document items)**

The following is a list (possibly not full) of Domino user document items, which are understood or processed by Domino when the server operates with users. For more information on these Items consult the Lotus Domino documentation. Go to <http://www.lotus.com/products/domdoc.nsf>, and click the **Lotus Domino Document Manager 3.5** link.

The same names must be used for Entry attribute names when performing Add, Modify, Delete or Lookup operations with the Connector.

- AltFullName
- AltFullNameLanguage
- AltFullNameSort
- Assistant
- AvailableForDirSync
- CalendarDomain
- CellPhoneNumber
- CcMailUserName
- Certificate
- CheckPassword
- Children
- City
- ClientType
- Comment
- CompanyName
- country
- Department
- DocumentAccess
- EmployeeID
- EncryptIncomingMail
- FirstName
- Form
- FullName
- HomeFAXPhoneNumber
- HTTPPassword
- InternetAddress
- JobTitle
- LastName

- Level0
- Level0\_1
- Level0\_2
- Level0\_3
- Level1
- Level1\_1
- Level1\_2
- Level1\_3
- Level2
- Level2\_1
- Level2\_2
- Level2\_3
- Level3
- Level3\_1
- Level3\_2
- Level3\_3
- Level4
- Level4\_1
- Level4\_2
- Level4\_3
- Level5
- Level5\_1
- Level5\_2
- Level5\_3
- Level6
- Level6\_1
- Level6\_2
- Level6\_3
- LocalAdmin
- Location
- MailAddress
- MailDomain
- MailFile
- MailServer
- MailSystem
- Manager
- MessageStorage
- MiddleInitial
- NetUserName
- NoteID
- OfficeCity
- OfficeCountry
- OfficeFAXPhoneNumber
- OfficeNumber
- OfficePhoneNumber

- OfficeState
- OfficeStreetAddress
- OfficeZIP
- Owner
- PasswordChangeDate
- PasswordChangeInterval
- PasswordGracePeriod
- PersonalID
- PhoneNumber
- PhoneNumber\_6
- SametimeServer
- ShortName
- Spouse
- State
- StreetAddress
- Suffix
- Title
- Type
- WebSite
- x400Address
- Zip

### **Domino Server 6.0 for AIX/Linux/Solaris**

For Domino Users Connector with Domino Server 6.0 for AIX/Linux/Solaris, you must update the `ibmditk` and `ibmdisrv` scripts. Add the following two lines in the script, after the `PATH` definition and before the startup line:

```
LD_LIBRARY_PATH=Domino_binary_folder
export LD_LIBRARY_PATH
```

where *Domino\_binary\_folder* is the folder containing Domino native libraries, for example, `/opt/lotus/notes/latest/sunspa` for Solaris, and `/opt/lotus/notes/latest/linux` for Linux.

Start IBM Tivoli Directory Integrator with the Domino user (do not use **root**). The Domino user is called **notes** unless it is changed during the installation of the Domino Server.

### **Examples**

Go to the `root_directory/examples/dominoUsersConnector` directory of your IBM Tivoli Directory Integrator installation.

### **See also**

“Lotus Notes Connector” on page 57.

## Lotus Notes Connector

The Lotus Notes Connector provides access to Lotus Domino databases.

The Lotus Notes Connector reads, writes and deletes records in any Notes database, and is therefore not limited to the Domino directory. Managing users in Lotus Notes requires modifying certificates, ACLs and mailboxes. This must be done manually or using the Config Editor. Users can be provisioned in and out of Notes by applying staging databases and integrating with Config Editor through Notes scripting.

**Note:** Lotus Notes Connector requires Lotus Notes to be release 5.0.8 or higher.

### Known limitations

For Notes Connector using Local Client or Local Server modes only: You might not be able to use the IBM Tivoli Directory Integrator Config Editor to connect to your Notes database. Sometimes, the Notes Connector prompts the user for a password even though the Notes Connector provides it to the Notes APIs. The prompt is written to standard-output, and input from the user is read from standard-input. This prompting is performed by the Notes API and is outside the control of IBM Tivoli Directory Integrator.

When you run the IBM Tivoli Directory Integrator Server, both standard input and output are connected to the console which enables the user to see the prompt and enter a password. The Notes Connector regains control and continues execution. This means the Connector works as expected.

When you run the IBM Tivoli Directory Integrator Config Editor, the standard input and output are disconnected from the console so the user cannot see or type anything in response. A connect operation can hang indefinitely waiting for user input.

When the **Session Type** is **LocalClient**, you can start your Notes or Designer client and permit other applications to use its connection by setting a flag in the **File->Tools->UserID** panel. The checkbox is labeled **Don't prompt for a password from other Notes-based programs. (Share this user ID password with these Notes add-ins)**. In this case, the Notes Connector (that is, the Notes API) ignores the provided password and reuses the current session established by the Notes or Designer client. The Notes or Designer client must be running to enable IBM Tivoli Directory Integrator to reuse its session.

**Note:** You can switch to using DIIOP mode to configure your AssemblyLines and switch back to Local Client or Local Server mode when you run the AssemblyLine through IBM Tivoli Directory Integrator Server.

### Session types

The following session types are supported (also refer to Supported session types by Connector for more information regarding libraries, setups and incompatibilities with other Domino Connectors):

**IIOP** This session type uses a TCP connection to the Domino server. The Lotus Notes Connector uses HTTP and IIOP to access the Domino server, so make sure these services are started and accessible from the host where you are running the Lotus Notes Connector.

#### LocalClient

This session type uses a local installation of Lotus Notes or Designer. The Lotus Notes Connector uses the ID file in use by the local client.

With this session type, the **Username** parameter (dominoLogin) is ignored. The **Password** (dominoPassword) must match the password in the ID file used or the local Notes client prompts for a password.

**Note:** This can be difficult, for example, when you run an AssemblyLine with standard input or output detached from the console. Always try to run an AssemblyLine in a command line window to detect whether the local client is prompting for the password. Testing shows

that the local client ignores the correct **Password** parameter and always prompts for a password. One way of making sure the prompt is avoided is to do the following:

1. Start the Notes or Designer client.
2. Go to the **File->Tools->UserID** menu.
3. Check **Don't prompt for a password for other Notes programs**.

### **LocalServer**

Same as for **LocalClient** but uses the local Domino server installation. One difference is that you can specify a valid **Username** and matching **Password**.

## **Connecting with IIOP**

The Connector can use IIOP to communicate with a Domino server. To establish an IIOP session with a Domino server, the Connector needs the IOR string that locates the IIOP process on the server.

When you configure the Notes Connector, specify a hostname and, optionally, a port number where the server is located. This *hostname:port* string is in reality the address to the Domino server's http service from which the Connector retrieves the IOR string. The IOR string is then used to create the IIOP session with the server's IIOP service (diiop). The need for the http service is only for the discovery of the IOR string. This operation is very simple. The Connector requests a document called **/diiop\_ior.txt** from the domino http server that is expected to contain the IOR string. You can replace the *hostname:port* specification with this string and bypass the first step and also the dependency of the http server. The *diiop\_ior.txt* file is typically located in the *data/domino/html* directory in your Domino server installation directory. Check the Web configuration in the Lotus Administrator for the exact location.

To verify the first step, go to the following URL: [http://hostname:port/diiop\\_ior.txt](http://hostname:port/diiop_ior.txt) where *hostname* is the hostname, and *port* is the port number of your domino server. You receive a document that says IOR: *numbers*. If you get a response similar to this, the first step is verified. If this fails, you must check both the HTTP configuration on the server that it enables anonymous access, and verify that the process is running.

## **Configuration**

The Connector needs the following parameters:

### **Hostname**

The IP hostname or address of the Domino server. You can also specify the IOR:<xxx> string to circumvent automatic discovery of this via HTTP. See the section about the IOR string for more information.

### **HTTP port**

This parameter is used by the Connector to get the IOR string from the Domino HTTP task so as to create an IIOP session.

### **Username**

The username used for IIOP sessions and Local Server sessions. Ignored if you use Session type **LocalClient**.

### **Password**

Internet password for IIOP sessions and Local Server sessions. Notes ID file password for Local Client sessions.

### **Session Type**

Can be one of **IIOP**, **LocalClient** or **LocalServer**. See "Session types" on page 57.

### **Use SSL**

Checking this flag causes the Connector to request an encrypted IIOP connection. This flag has meaning when the session type is IIOP only. One of the requirements for using SSL is that the *TrustedCerts.class* file that is generated every time the DIIOP process starts must be in the classpath. You must copy the *TrustedCerts.class* to a local path included in the CLASSPATH or have the *\Lotus\Domino\Data\Domino\Java* of your Domino installation in the classpath.



**Server** The name of the server where **Database** is found. Leave blank to use the server you are connecting to (**Host Name**).

**Database**

The name of the database to use.

**Document Selection**

The selection used when iterating the data source. You must use valid Lotus Notes select statements. To select entries from the name and address book use the following select statement:

```
Select Form="Person"
```

**Always use Formula Search**

This flag is used when View is not set and the database accessed is full-text indexed. If you check this flag, the Connector uses Formula statements regardless of whether the database is indexed or not. When a view is specified, full-text searches are always used because View does not support Formula search statements.

**Database View**

The database view to use.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Security**

To have IBM Tivoli Directory Integrator access your Domino server, you must enable it through **Domino Administrator -> Security -> IIOP restriction**. The user account you configured for the IBM Tivoli Directory Integrator to use must belong to a group listed under **Run restricted Java/Javascript** and **Run unrestricted Java/Javascript**.

The Domino Web server must be configured to enable anonymous access. If not, the current version of the Notes Connector cannot connect to the Domino IIOP server.

**Note:** If you want to encrypt the **HTTPassword** field of a Notes Address Book, add the following code to your AssemblyLine:

```
var pwd = "MyPassword";  
var v = dom.connector.getDominoSession().evaluate  
("@Password(\"\" + pwd + "\"")" );  
ret.value = v.elementAt(0);
```

This code uses Domino's password encryption routines to encrypt the variable *pwd*. It can be used anywhere that you want to encrypt a string using the **@Password** function that Domino provides. A good place to use this code is in the **Output Map** for the **HTTPassword** attribute.



---

## ITIM DSMLv2 Connector

This Connector is used in solutions which require communication with IBM Tivoli Identity Manager (ITIM).

The ITIM server provides a communication interface which uses a ITIM-proprietary version of DSMLv2. This ITIM-proprietary version of DSMLv2 doesn't fully comply with the DSMLv2 specification. Hence the Connector name – *ITIM DSMLv2 Connector*.

This Connector is used for both:

- retrieving provisioning data, and
- feeding provisioning data

using the ITIM-proprietary DSMLv2 communication interface.

The version of ITIM supported is 4.5 and higher.

The Directory Services Markup Language v1.0 (DSMLv1) enables the representation of directory structural information as an XML document. DSMLv2 goes further, providing a method for expressing directory queries and updates (and the results of these operations) as XML documents.

**Note:** This Connector is *pecially designed* for use with ITIM; for generic use, use the DSMLv2Soap Connector and/or the DSMLv2SoapServer Connector instead.

The ITIM DSMLv2 Connector which connects to a IBM Tivoli Identity Manager Server repository using DSML over HTTP.

The Connector connects to the DSMLv2 ITIM event handler (introduced in ITIM 4.5) that allows the import of data into ITIM with ITIM acting as a DSMLv2 server. Therefore, only ITIM Server 4.5 and above is supported. The ITIM DSMLv2 Connector uses the ITIM DSML JNDI driver "dsm12.jar", to connect to and interact with the ITIM Server. Deployment of the DSMLv2 Connector uses JNDI queries to interact with the ITIM repository.

The Connector supports the **AddOnly**, **Delete**, **Iterator**, **Lookup** and **Update** modes.

## Using the Connector with ITIM Server

When connecting to a ITIM Server the following URL should be specified in the ITIM DSMLv2 Connector: `http://<ITIM_Server_host:ITIM_Server_port>/enrole/dsm12_event_handler`; for example, "http://192.168.113.12:9080/enrole/dsm12\_event\_handler".

The following limitations apply to ITIM DSMLv2 Connector modes when interacting with ITIM Server:

- Iterator mode – will only work if the JNDI filter specified matches exactly one Entry; if the filter matches more than one Entry, no Entries will be returned.
- Lookup, Update and Delete – will only work correctly if the link criteria specified result in finding exactly one Entry; if the link criteria match more than one Entry, the Connector will act as if the link criteria matched no Entries.

When interacting with ITIM Server, all JNDI queries and filters, used either from the GUI or in scripting (in Advance Search Criteria, for example) must be enclosed in brackets, for example "(uid=user1)".

## HTTPS (SSL) Support

In order to use a secure HTTPS connection to the DSMLv2 Server, the provider URL specified must begin with "https://" and the server's certificate must be included in TDI's trust store.

## Configuration

The ITIM DSMLv2 Connector needs the following parameters:

### Provider URL

The URL for the connection.

### Referrals

Specifies how referrals encountered by the LDAP server are to be processed. The possible values are:

- **follow** - Follow referrals automatically.
- **ignore** - Ignore referrals
- **throw** - Throw a ReferralException when a referral is encountered. You need to handle this in an error Hook.

### Authentication Method

The authentication method.

### Login username

The principal name (for example, username).

### Login password

The credentials (for example, password).

### Name parameter

Specify which parameter in the AssemblyLine entry is used for naming the entry. This is used during add, modify and delete operations and returned during read or search operations. If not specified, "\$dn" is used.

### Provider Params

A list of extra provider parameters you want to pass to the provider. Specify each "parameter:value" on a separate line.

### Search Base

The search base to be used when iterating the directory. Specify a distinguished name. Some directories allow you to specify a blank string which defaults to whatever the server is configured to do. Other directory services require this to be a valid distinguished name in the directory.

### Search Filter

The search filter to be used when iterating the directory.

### Search Scope

The search scope to be used when iterating the data source. Possible values are:

- subtree - search all levels from search base and below
- onelevel - search only immediate children of search base

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## See also

"ITIM Agent Connector" on page 100

---

## DSMLv2 SOAP Connector

The DSMLv2 SOAP Connector implements the DSMLv2 standard. The Connector is able to:

- Execute DSMLv2 requests against a DSML Server.
- Provide the option to use DSML SOAP binding.
- Internally instantiate, configure and use the HTTP Parser to create HTTP requests and parse HTTP responses.
- Internally instantiate, configure and use the DSMLv2 Parser to create DSMLv2 request messages and parse DSMLv2 response messages.

## Supported Connector Modes

The Connector mode determines the type of DSML operation the Connector requests. The DSMLv2 SOAP Connector supports the following modes:

### AddOnly

The DSMLv2 SOAP Connector sends DSMLv2 addRequest and receives a DSMLv2 addResponse message.

### Iterator

The DSMLv2 SOAP Connector sends a DSMLv2 searchRequest operation with a Search Base, Search Filter and Search Scope taken from the current Connector configuration. The DSML server returns a DSMLv2 searchResponse message with multiple searchResultEntry elements. The Connector cycles through the DSML searchResultEntry elements and delivers each one in a separate AssemblyLine iteration.

### Lookup

The DSMLv2 SOAP Connector sends a DSMLv2 searchRequest with a Search Filter constructed from the Connector's Link Criteria. The DSML server returns a DSMLv2 searchResponse message that is returned as the Entry found. If there are multiple searchResultEntry elements in the searchResponse message, you must process them in an On Multiple Entries hook.

**Delete** The Connector creates and sends a DSML deleteRequest as per the Link Criteria. The DSML server returns a deleteResponse message.

### Update

If the \$dn Attribute in the work Entry is equal to the \$dn Attribute of the Entry to be updated, the Connector sends a modifyRequest DSMLv2 request and receives a modifyResponse response; otherwise a modDnRequest request is sent to the DSML server and a modDnResponse response is received.

**Delta** In Delta mode, it is the AssemblyLine that, depending on the Entry tagging, decides which Connector method to invoke and what DSMLv2 request will be sent. Delta tagging at the Attribute level is handled by the DSMLv2 Parser and delta information is incorporated into the resulting DSMLv2 request.

### CallReply

In CallReply mode, the Connector provides the work Entry to the DSMLv2 Parser and sends the DSMLv2 message produced by the DSMLv2 Parser. The response from the DSMLv2 Server is passed directly to the DSMLv2 Parser, and the Entry produced is returned by the Connector. You must assign the correct request type, because the Connector will not automatically set any DSMLv2 element. In particular, the CallReply mode can be used to send DSMLv2 extended operations. See "Extended Operations" for more information.

## Extended Operations

In CallReply mode, the DSMLv2 SOAP Connector can send DSMLv2 extended operations. Extended operations are identified by their Operation Identifier (OIDs). For example, the OID of the extended operation for retrieving a part of the log file of the IBM Tivoli Directory Server is 1.3.18.0.2.12.22.

Extended operations can also have a value property, which is a data structure containing input data for the corresponding operation. The value property of the extended operation must be Basic Encoding Rules (BER) encoded and then base-64 encoded in the DSMLv2 message. The user of the DSMLv2 SOAP Connector is responsible only for BER encoding the value property. The Connector will automatically base-64 encode the data when creating the DSMLv2 message.

Two classes are used for BER encoding and decoding: `BEREncoder` and `BERDecoder`, located in the `com.ibm.asn1` package.

The following example illustrates sending a DSMLv2 extended operation request and the processing of the response:

1. Place the following script code in Output Map for attribute `dsml.extended.requestvalue`:

```
enc = new Packages.com.ibm.asn1.BEREncoder();
serverFile = 1; //slapdErrors log file

nFirstLine = new java.lang.Integer(7200);
nLastLine = new java.lang.Integer(7220);

seq_nr = enc.encodeSequence();
enc.encodeEnumeration(serverFile);

enc.encodeInteger(nFirstLine);
enc.encodeInteger(nLastLine);

enc.endOf(seq_nr);
var myByte = enc.toByteArray();

ret.value = myByte;
```

2. Place the following script code in the After CallReply hook of the Connector:

```
var ba = conn.getAttribute("dsml.response").getValue(0);
bd = new Packages.com.ibm.asn1.BERDecoder(ba);

main.logmsg("SLAPD log file:");
main.logmsg(new java.lang.String(bd.decodeOctetString()));
```

## Configuration

The DSMLv2 SOAP Connector uses the following parameters:

### DSMLv2 Server URL

Specifies the URL of the DSMLv2 Server.

### Authentication Method

Specifies the type of HTTP authentication. If the type of HTTP authentication is set to `Anonymous`, then no authentication is performed. If HTTP basic authentication is specified, HTTP basic authentication is used with user name and password as specified by the `username` and `password` parameters.

### Username

The user name used for HTTP basic authentication.

### Password

The password used for HTTP basic authentication.

### Binary Attributes

Specifies a comma-delimited list of attributes that will be treated by the Connector as binary attributes. This parameter has the following default list of attributes that you can change:

- photo
- personalSignature
- audio

- jpegPhoto
- javaSerializedData
- thumbnailPhoto
- thumbnailLogo
- userPassword
- userCertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair
- x500UniqueIdentifier
- objectGUID
- objectSid

**Search Base**

Specifies the starting point for searches when iterating.

**Search Filter**

Specifies the LDAP filter used when iterating.

**Search Scope**

The search scope to be used when iterating. Possible values are:

- subtree
- onelevel

The default is subtree.

**Soap Binding**

When this parameter is enabled, the Connector sends and receives SOAP DSML messages. Otherwise, the DSML messages are not wrapped in SOAP.

**Detailed Log**

Turns on debug messages. This parameter is common to all TDI components.





---

## DSMLv2 SOAP Server Connector

The DSMLv2 SOAP Server Connector listens for DSMLv2 requests over HTTP. Once it receives the request, the Connector parses the request and sends the parsed request to the AssemblyLine workflow for processing. The result is sent back to the client over HTTP.

The DSMLv2 SOAP Server Connector is able to:

- Execute DSMLv2 requests against a DSML Server.
- Provide the option to use DSML SOAP binding.
- Internally instantiate, configure and use the HTTP Parser to create HTTP requests and parse HTTP responses.
- Internally instantiate, configure and use the DSMLv2 Parser to create DSMLv2 request messages and parse DSMLv2 response messages.
- Process each event in a separate thread, allowing the Connector to process several DSMLv2 events in parallel.

The DSMLv2 SOAP Connector supports Server mode.

**Note:** The DSMLv2 SOAP Server Connector is not designed as a replacement of the “DSMLv2 EventHandler” on page 245. The Connector provides a generic functionality for processing DSMLv2 requests.

### Extended operations

DSMLv2 SOAP Server Connector supports extended operations. The value property of the extended operation is automatically base-64 decoded from the DSMLv2 message. You must then properly Basic Encoding Rules (BER) decode this value. You must also BER encode the responseValue property represented by the dsm1.response Entry Attribute. The Connector will automatically base-64 encode the data when creating and sending the DSMLv2 response.

You can use the following two helper classes to BER encode and decode data:

- com.ibm.asn1.BEREncoder
- com.ibm.asn1.BERDecoder

**Note:** The schema of the extended operations cannot be automatically determined by the Connector. There is no metadata that describes the structure of an extended operation request.

The following example illustrates an extended operation request to return a part of the IBM Tivoli Directory Server log:

```
var name = work.getString("dsm1.extended.requestname");
var ba = work.getAttribute("dsm1.extended.requestvalue").getValue(0);

decoder = new Packages.com.ibm.asn1.BERDecoder(ba);
iSequence = decoder.decodeSequence();
fileNumber = decoder.decodeEnumeration();
firstLine = decoder.decodeIntegerAsInt();
lastLine = decoder.decodeIntegerAsInt();

main.logmsg("Operation: " + name);
main.logmsg("File: " + fileNumber);
main.logmsg("First line: " + firstLine);
main.logmsg("Last line: " + lastLine);

// send the response, assuming this sample string is the log file content
var str = new java.lang.String("Apr 13 16:18:18 2005 Entry cn=chavdar kovachev,o=ibm,c=us already exists.");
enc = new Packages.com.ibm.asn1.BEREncoder();
```

```
enc.encodeOctetString(str.getBytes());
myByte = enc.toByteArray();

work.setAttribute("dsm1.response", myByte);
work.setAttribute("dsm1.responseName", "1.3.18.0.2.12.23");
work.setAttribute("dsm1.resultdescr", "success");
```

## Configuration

The DSMLv2 SOAP Server Connector uses the following parameters:

### Dsm1 Port

Specifies the TCP port on which the DSMLv2 SOAP Server Connector is listening.

### Connection Backlog

Specifies the maximum queue length for incoming connections. If a connection request arrives when the queue is full, the connection will be refused.

### HTTP Basic Authentication

Determines if clients must provide HTTP basic authentication.

### Auth Realm

Specifies the authentication realm sent to the client when requesting HTTP Basic authentication

### Binary Attributes

Specifies a comma-delimited list of attributes that will be treated by the Connector as binary attributes.

This parameter has the following default list of attributes that you can change:

- photo
- personalSignature
- audio
- jpegPhoto
- javaSerializedData
- thumbnailPhoto
- thumbnailLogo
- userPassword
- userCertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair
- x500UniqueIdentifier
- objectGUID
- objectSid

### Use SSL

If checked, Secure Sockets Layer (SSL) will be used while initializing the connector.

### Require Client Authentication

If checked, the connector will require client authentication using SSL.

### Chunked Transfer Encoding

If checked, the HTTP body of the response message is transferred as a series of chunks.

### Soap Binding

If checked, the Connector sends and receives SOAP DSML messages. Otherwise, the DSML messages are not wrapped in SOAP.

**Detailed Log**

Turns on debug messages. This parameter is common to all TDI components.



---

## Exchange Changelog Connector

The Exchange Changelog Connector is a specialized instance of the LDAP Connector. The Exchange Connector contains logic to poll Exchange for changed objects using the uSNChanged mechanism.

The Exchange Changelog Connector operates in Iterator mode.

### Notes:

1. Microsoft dropped the extended support for Exchange 5.5 at the end of 2005. As TDI 6.1 does not support NT4, the Exchange Changelog Connector is *deprecated* along with the Exchange Changelog EventHandler in TDI 6.1.1.
2. The Exchange Changelog Connector connects to Microsoft Exchange Server 5.5; . Microsoft Exchange is usually used with Windows NT4. Users of Windows 2000 Server with Exchange 2000 and above would normally use Active Directory As a result the Exchange Changelog Connector is only applicable in Windows NT4 environment.
3. The Exchange 5.5 Service Pack 4 must be installed on the Exchange Server.

## Behavior

When started, the Exchange Changelog Connector reads from the IBM Tivoli Directory Integrator User Property Store the USN values stored from the most recent Exchange Connector's session. The Exchange Connector first retrieves the newly added Exchange objects, then the modified and deleted Exchange objects. After an Exchange object is retrieved, it is parsed and its attributes and attribute values are copied to a new Entry object. This Entry object is then returned by the Exchange Connector. When there are no more changed objects to retrieve, the Exchange Connector cycles, waiting for a new change to happen. The **Sleep Interval** parameter specifies the number of seconds the Exchange Connector sleeps between successive polls when waiting for new changes. The Exchange Connector loops until either a new change is retrieved or the timeout expires. If the timeout expires, the Exchange Connector returns a **null** Entry, indicating that there are no more Entries to return. If a changed object is retrieved, it is processed, and the new Entry is returned by the Exchange Connector.

The Exchange Changelog Connector delivers changed Exchange objects as they are, with all their current attributes. It does not determine which object attributes have changed, nor how many times an object has been modified. All intermediate changes to an object are irrevocably lost. Exchange does not have a changelog, it only stamps an object when it is changed. Each object reported by the Exchange Connector represents the cumulative effect of all changes performed to that object. The Exchange Connector, however, recognizes the type of object change that must be performed on the replicated data source, and reports whether the object has to be added, modified or deleted in the replicated data source.

**Note:** You can retrieve only objects and attributes that you have permission to read. The Exchange Connector does not retrieve an object or an attribute which you don't have permission to read, even if it exists in Exchange. In such a case the Exchange Connector acts as if the object or the attribute does not exist in Exchange.

## Using the Exchange Changelog Connector

The Exchange Changelog Connector adds the **changeType** attribute to every Entry returned. The possible values of the **changeType** attribute are **add**, **modify** and **delete**. These are used to represent new, changed and deleted objects respectively.

When an object is deleted in the Exchange Server, it is marked as **tombstone** and its **"Is-Deleted"** attribute is set to **true**. The object, however, is not moved to other container (like in the Active Directory Connector), and keeps its **distinguishedName** attribute. Exchange objects cannot be moved. As a result, the **distinguishedName** attribute never changes in Exchange and can be used safely for object identifier when synchronizing.

**Note:** Deleted objects in Exchange live for a configurable period of time (30 days by default), after which they are completely removed. To avoid missing deletions, perform incremental synchronizations more frequently.

It is possible for an object to be reported as modified, even though the object's contents have not changed since it was reported as a new object. This happens when the object has been created before the current Exchange Connector session has started and is later modified after the current Exchange Connector session has started but before the Exchange Connector has actually retrieved the object. In such a case the Exchange Connector retrieves the object's modified contents and reports it as a new object. After a short period of time (during the same session) the Exchange Connector reports the same object as modified and retrieves the same changed and already reported object's contents. Do not be concerned about this behavior since it neither hurts the synchronization process, nor has it any significant performance overhead.

It is also possible for an already deleted object to be reported as a new object and later reported as a deleted object during the same Exchange Connector session. This happens when the object has been created before the current Exchange Connector session has started and is later deleted after the current Exchange Connector session has started, but before the Exchange Connector has actually retrieved it. In this case the Exchange Connector retrieves the object's deleted state and reports it as a new object. After a short period of time (during the same session) the Connector reports the same object as deleted. The addition of an already deleted object can be recognized by checking for the "**Is-Deleted**" attribute. If the object is present and has a value of **true**, the object is already deleted.

The Exchange Changelog Connector can be interrupted any time during the synchronization process. It saves the state of the synchronization process in the User Property Store of the IBM Tivoli Directory Integrator (after each Entry retrieval) and the next time the Connector is started it successfully continues the synchronization from the point the Exchange Changelog Connector was interrupted.

The Exchange Changelog Connector supports the IBM Tivoli Directory Integrator 6.1.1 Checkpoint/Restart functionality.

## The Is-Deleted attribute in Exchange

By default, Exchange does not expose the **Is-Deleted** object attribute through LDAP. However, the **Is-Deleted** attribute can be used in LDAP search queries when it is not returned as part of the returned Exchange object. That is why the Exchange Connector properly detects the type of change even if the **Is-Deleted** attribute is not visible through LDAP. If the **Is-Deleted** attribute is visible through LDAP, then the Exchange Connector can retrieve changes quicker if you set the "**Is-Deleted**" **Attribute Visible** parameter to **TRUE**. The Connector uses the returned **Is-Deleted** attribute and completes the work faster.

**Note:** If the server does expose the **Is-Deleted** attribute, but "**Is-Deleted**" **Attribute Visible** is set to **false**, then the Connector still works properly, but you can accelerate the Exchange Connector by setting "**Is-Deleted**" **Attribute Visible** to **true**. If the server does not expose the **Is-Deleted** attribute, but "**Is-Deleted**" **Attribute Visible** is set to **true**, then the Connector cannot distinguish between modify and delete and reports modify for both modify and delete operations.

To expose the **Is-Deleted** attribute you must obtain Exchange server administrator privileges and do the following:

1. Start the Exchange Administration program **admin.exe** in RAW mode (**admin /r**).
2. Select **View->Raw Directory** from the menu.
3. Select **Schema** from the window on the left.
4. Double-click **Is-Deleted** from the window on the right.
5. A message box is displayed, informing you that only raw properties are displayed. This message box asks if you want to view these raw properties. Click **Yes**.

6. Select the **Heuristics** property. You can see the current property value on the right. You can also edit the property value.
7. To decide what value to set the Heuristics property to, please refer to the following. The heuristic property is a bit mask, which is interpreted as follows:

**Bit 0**

- **0:** Replicate between sites
- **1:** Do not replicate between sites

**Bit 1**

- **0:** Attribute is not visible through LDAP
- **1:** Attribute is visible to anonymous and authenticated LDAP clients

**Bit 2**

- **0:** Attribute is not accessible by authenticated clients
- **1:** Attribute is accessible to authenticated clients but not anonymous clients

**Bit 3**

- **0:** Attribute is not an operational attribute
- **1:** Attribute is an operational attribute

**Bit 4**

- **0:** Attribute is not visible in Config Editor (Attributes page of DS Site Configuration object)
- **1:** Attribute is visible in Config Editor (Attributes page of DS Site Configuration object)

By taking note of heuristics, you can determine the visibility of particular attributes. For example, a heuristic value of **3** means the attribute is not replicated between sites and is visible by anonymous LDAP clients. A heuristic value of **11** means the attribute is an operational attribute and is visible to authenticated LDAP clients.

As can be seen from the table, bit **1** of the heuristics value determines whether an object is visible through LDAP. That is why you need to set bit **1** to make the attribute visible through LDAP.

Another important property of an Exchange object or an Exchange object attribute is the Description property. It determines the LDAP name of the attribute or object.

**Note:** Changing the LDAP name might cause interoperability problems.

## Accessing the USN synchronization values in the User Property Store

The state of synchronization at any time is represented by 4 USN numbers:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

These values are packed and stored in the User Property Store. Do not change these values manually. You might want to archive the numbers corresponding to a certain stage of synchronization and later use these numbers to replay synchronization from that stage.

The following script code can be used in the IBM Tivoli Directory Integrator to get USN values stored in the User Property Store:

```
// Retrieve USN values from User Property Store
var usn = system.getPersistentObject("exchange_sync");
var startUsn = usn.getString("START_USN");
var endUsn = usn.getString("END_USN");
```

```

var currentUsnCreated = usn.getString("CURRENT_USN_CREATED");
var currentUsnChanged = usn.getString("CURRENT_USN_CHANGED");

main.logmsg("START_USN: " + startUsn);
main.logmsg("END_USN: " + endUsn);
main.logmsg("CURRENT_USN_CREATED: " + currentUsnCreated);
main.logmsg("CURRENT_USN_CHANGED: " + currentUsnChanged);

```

"exchange\_sync" is the name of a parameter already stored in the User Property Store. The **Iterator State Key** parameter specifies this value. The above example just dumps the values to the screen, but you may do whatever you want with them - for example save them in a file and backup this file.

The next script code example shows how the USN values can be stored in the User Property Store:

```

// Store USN values in the User Property Store
var usn = system.newEntry();
usn.setAttribute("START_USN", startUsn);
usn.setAttribute("END_USN", endUsn);
usn.setAttribute("CURRENT_USN_CREATED", currentUsnCreated);
usn.setAttribute("CURRENT_USN_CHANGED", currentUsnChanged);
system.setPersistentObject("exchange_sync", usn);

```

This code assumes that the variables *startUsn*, *endUsn*, *currentUsnCreated* and *currentUsnChanged* contain the USN numbers as strings. This example saves the USN values under the "exchange\_sync" parameter, so exchange\_sync must be specified in the **Iterator State Key** parameter to continue synchronization from the desired point.

## Accessing the runtime Connector's USN synchronization values

The Exchange Changelog Connector provides the following public methods for access to its current USN values:

### **public Entry getUsnValues ();**

Returns an Entry object with the following attributes:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

The value of each of the attributes is of type `java.lang.Integer` and represents the corresponding Connector's USN value.

### **public void setUsnValues (Entry usnEntry);**

Sets the Exchange Connector's current USN synchronization values to the values specified in the **usnEntry** parameter. The structure of the **usnEntry** parameter must be the same as the structure of the Entry returned by `getUsnValues()`. The values of the **usnEntry** attributes must be either **java.lang.Integer** or the String representations of the corresponding numbers.

**Note:** Be careful when changing the USN values at runtime. Specifying inconsistent values can result in improper synchronization.

## Configuration

The Connector needs the following parameters:

### **LDAP URL**

The LDAP URL of the Exchange server you want to access. The LDAP URL has the form `ldap://hostname:port` or `ldap://server_IP_address:port`. For example, `ldap://localhost:389`

**Note:** The default LDAP port number is 389. When using SSL, the default LDAP port number is 636.



**Login username**

The distinguished name used for authentication to the service. For example, **cn=administrator,ou=domain\_name,o=organization\_name**.

**Note:** If you use Anonymous authentication, you must leave this parameter blank.

**Login password**

The credentials (password).

**Note:** If you use Anonymous authentication, you must leave this parameter blank.

**Authentication Method**

The authentication method to be used. Possible values are:

- Anonymous (use no authentication)
- Simple (use weak authentication (cleartext password))

**Use SSL**

Specifies whether to use Secure Sockets Layer for LDAP communication with Exchange Server.

**LDAP Search Base**

The specified Exchange sub-tree which is polled for changes. For example, **cn=recipients,ou=domain\_name,o=organization\_name**.

**USN Filename**

Specifies the name of the text file where the most recent Connector session USN values are stored. If the file does not exist or is not in the correct format, the Connector performs a full synchronization with Exchange. The file must not be read-only, as the Connector writes the updated USN values each time it retrieves an Entry.

**Note:** The use of a separate USN file by means of this parameter is deprecated. Use the **Iterator State Key** parameter instead.

If you change the search base or the server or both, you might want to change or edit the USN file as well, because the stored USN values might be invalid in regard to the new search base or server.

**Iterator State Key**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

**Start at**

Specifies a start USN number from which synchronization must start. **EOD** means report only changes that happen after the Connector has started.

**"Is-Deleted" Attribute visible**

Specifies whether the Exchange server exposes the **Is-Deleted** object attribute through LDAP.

**Note:** If the server does expose the **Is-Deleted** attribute, but **"Is-Deleted" Attribute visible** is set to **false**, then the Connector still works properly. You can accelerate the Connector by setting **"Is-Deleted" Attribute visible** to **true**. If the server does not expose the **Is-Deleted** attribute, but **"Is-Deleted" Attribute visible** is set to **true**, then the Connector cannot tell the difference between a modified object and a deleted object and reports all deletions as modify change operations.

**Timeout**

Specifies the number of seconds the Connector searches for a new change. Regardless of the value of this parameter, the Connector does not timeout until it has scanned every change that has happened before the current Connector session has started.

If this parameter is **0**, then the Connector waits indefinitely for the next change.

When the Connector times out, it returns an empty (**null**) Entry, thus indicating that there are no more Entries to return.

**Sleep Interval**

Specifies the number of seconds the Connector sleeps between successive polls for changes.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Comment**

Your comments here.

## Migration

For IBM Tivoli Directory Integrator 6.1.1, the Exchange Changelog Connector stores the USN synchronization values into the User Property Store of the IBM Tivoli Directory Integrator. Older versions (pre-6.0) of the Exchange Changelog Connector store the USN values in a text file.

Do the following to migrate a pre-6.0 IBM Tivoli Directory Integrator configuration:

1. Open the pre-6.0 configuration and set a value for the **Iterator State Store** parameter.
2. Run the AssemblyLine. The Exchange Connector reads the start USN values from the text file, but stores the updated USN values both in the text file and in the User Property Store.
3. Stop the AssemblyLine.
4. Clear the value of the **USN Filename** parameter and save the configuration. The Connector reads and stores the USN synchronization values in the User Property Store and no text file is used.

## See Also

“LDAP Connector” on page 133

“Active Directory Changelog (v.2) Connector” on page 13,

“Netscape/iPlanet/Sun Directory Changelog Connector” on page 161,

“IBM Directory Server Changelog Connector” on page 97.

“z/OS Changelog Connector” on page 233.

---

## File system Connector

The file system Connector is a transport Connector that requires a Parser to operate. The file system Connector reads and writes files available on the system it runs on. Concurrent usage of a file can be controlled by means of a locking mechanism.

**Note:** This Connector can only be used in Iterator or AddOnly mode, or for the equivalent operations in Passive state.

### Configuration

The Connector needs the following parameters:

#### File Path

The name of the file to read or write.

#### Timeout (in seconds)

When this parameter is specified as a positive number, the Connector waits for available data when reading from a file. Specify **0** (zero) to wait forever, or any other number which specifies the number of seconds to wait before signalling end of file. Setting this parameter to **0** (zero) causes the Connector to simulate the UNIX-style **tail -f** command.

If you have requested a lock on the file (using the **Lock File** parameter), the Timeout parameter instead specifies how long to wait to acquire the lock. An unspecified or negative number means wait forever.

#### Append on Output

If set, the Connector appends instead of overwriting when the file is opened for writing.

#### Lock file

When writing, acquire an exclusive lock on the file being written. When reading, acquire a shared lock.

The lock is acquired when the Connector is initialized, and released when the Connector is closed.

If one Connector (A) has acquired an exclusive lock on a file, and another Connector (B) tries to open it, then Connector B will either wait for the lock to be released, or an error will be thrown. If Connector B has checked the exclusive Lock parameter, it will wait; if Connector B has not checked the exclusive Lock parameter, an error will be thrown.

The locking mechanism is Operating System dependent. Note that file locking can cause deadlocks, especially if more than one file is locked per AssemblyLine.

For more information, see [http://java.sun.com/j2se/1.5.0/docs/api/java/nio/channels/FileChannel.html#lock\(\)](http://java.sun.com/j2se/1.5.0/docs/api/java/nio/channels/FileChannel.html#lock())

#### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Parser** In the Parser tab, you can configure the name of a Parser to access the contents of the file by selecting a Parser in the "Inherit from:" button.

### See also

"URL Connector" on page 227.



---

## FTP Client Connector

The FTP Client Connector is a transport Connector that requires a Parser to operate. The Connector reads or writes a data stream that can either be a file or a directory listing. Think of the FTP Client Connector as a remote read/write facility, not something you use to transfer files.

This Connector supports FTP Passive Mode, as per RFC959. Passive Mode reverses who initiates the data connection in a file transfer. Normally the server initiates a data connection to the client (after a command from the client), whereas passive mode enables the client to initiate the data connection. This makes it easier to transfer files when the client is behind a firewall.

### Notes:

1. Iterator mode supports the operations **get** and **list**; AddOnly supports **put**.
2. This Connector is not intended for transferring binary files.
3. The FTP Client in AddOnly mode with Save Connector Restart Info does not support Checkpoint/Restart.

## Configuration

The Connector needs the following parameters:

### FTP Hostname

The hostname on which the FTP Server resides that the Connector will connect to.

### FTP Port

The FTP TCP port (defaults to **21**).

### Login User

The login username.

### Login Password

The login password.

### Operation

The intended operation. Specify **get** to read a file (Iterator), **put** to write a file (Add Only), or **list** to do a directory listing (Iterator).

### Remote Path

Initial remote directory (for list) or file (for get/put) to access.

### Transfer Mode

ASCII or Binary. ASCII is the only supported mode.

### Passive Mode

When this checkbox is enabled, specifies that the FTP Client Connector will connect to the FTP Server in passive mode instead of active mode. This parameter is ignored on an IPv6 connection, since IPv6 *always* uses passive mode.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

From the Parser pane, you select the mandatory Parser. For example, Line Reader is a useful parser for list, or if you simply want to copy one file. The select dialog is activated by pressing the bottom-right **Inherit From:** button.

## See also

- “The FTP object” on page 437,
- “URL Connector” on page 227,
- “Old HTTP Client Connector” on page 87,
- “Old HTTP Server Connector” on page 95.

---

## GLA Connector

### Introduction

The GLA Connector processes log files and transforms them to Common Base Event (CBE) objects, which are then fed into the AssemblyLine.

It uses Generic Log Adapter (GLA) technology, part of IBM's Autonomic Computing Toolkit, to process log files and transform their contents into Common Base Event format. The Autonomic Computing Toolkit website contains (in addition to general information and documentation) a variety of downloadable software, including the Eclipse plug-in to edit GLA configuration files.

### Adapter configuration file

An adapter configuration file, prepared externally using the Adapter Configuration Editor Eclipse plug-in is used in conjunction with the GLA Connector. It provides the tooling to create the specific parser rules that are used by the GLA Connector at runtime to create Common Base Event objects, that is, the configuration file contains information about the log file which will be processed. From this file all the CBE objects will be later created. The logic for parsing the objects is also implemented in the adapter configuration file. In the Eclipse GLA plug-in there are several examples of such configuration files, made to process some well known application log files. You can also create your own configuration files using the Eclipse's user interface.

In both cases, either using an already created configuration file or creating a new configuration file, you should note that a specially made outputter called *TDIOutputter* needs to be configured. This should be done because when the CBE objects are created, the *TDIOutputter* sends these CBE objects to the GLA Connector (which can then send them into the AssemblyLine using the ordinary mapping mechanism ).

### Using more than one outputter in the configuration file

It is not possible to use more than one *TDIOutputter*. If two or more *TDIOutputters* are configured in the adapter configuration file an Exception will be thrown when the GLA Connector tries to get the correlation ID from the *TDIOutputter*. When there is more than one *TDIOutputter* configured, the GLA Connector which uses the configuration file does not know which of the multiple *TDIOutputters* to use—it is not possible to get the CBE Objects from the correct *TDIOutputter*.

However, it is possible to define more than one outputter as long as it is not a *TDIOutputter*. For example, you could combine the *TDIOutputter* with a *FileOutputter*. This will cause all CBE objects to be sent (and saved) both to a file and to the GLA Connector.

## Configuration

To configure the GLA Connector you must have a valid adapter configuration file. The path to the file must be set in the Connector **Config File Path** parameter. The configuration file is being checked for validity and if this is not a valid adapter configuration file an Exception will be thrown.

### Config File Path

Determines where the adapter configuration file is located. The configuration file contains the entire information about the log file and how it will be processed.

### Debug

Checking this parameter causes more information to be logged.

## Configuring the TDIOutputter

In order to configure the adapter file to use the *TDIOutputter* you use Eclipse's GLA user interface (the Eclipse GLA plug-in). Below a description of how to configure the outputter using the Eclipse user interface:

1. Open the adapter configuration file for editing. Now the Eclipse plug-in is showing the contents of the configuration file.

2. Go to Adapter -> Configuration -> Context Instance.
3. Right click on Context Instance.
4. Choose Add -> Logging Agent Outputter. Now you are able to see and configure the outputter.
5. For the outputter type choose undeclared.
6. Type a description of your choosing in the Description field.
7. Right click on the Outputter and choose Add -> Property.
8. Name the property "*tdi\_correlation\_id*".
9. For the value of this property use an arbitrary and **unique** value which will become the correlation ID of the GLA Connector using this configuration file.
10. If no value is filled the TDIOutputter will use a default value and will register any Connector which attempts to start its adapter configuration file.
11. Go to Adapter -> Contexts -> Basic Context Implementation and right click over it.
12. Choose add -> Logging Agent Outputter.
13. Fill the name and description fields.
14. In the Executable Class field enter "*com.ibm.di.connector.gla.TDIOutputter*".
15. Make sure the role is set to outputter.
16. In the Role version field add a number (for example: 1.0.0).
17. For the unique ID click browse and choose the outputter you just made in steps 2 – 7.
18. Now you have configured the outputter and you are ready to use this adapter configuration file with the GLA Connector.

## Using the Connector

To configure the GLA Connector you must have a valid adapter configuration file. The path to the file must be set in the Connector **Config File Path** parameter.

When the GLA Connector starts, a GLA instance is started in a separate thread inside the Connector. Starting the adapter in a separate thread makes it possible to start iterating through the entries before GLA has completed processing the entire log file. When the Connector receives CBE objects it stores them into a queue, which orders the elements in FIFO (first-in-first-out) manner. When there are no elements in the queue and the Connector wants to take an element from it, it will not return null value but will wait until an element is available (that is, it blocks). On the other side of the queue when it is full and an element needs to be added to it, it will block until there is available space in the queue.

Conditions like end-of-data, GLA adapter errors etc. are handled by special messages in the queue, enabling the Connector to work in the manner expected of a TDI Connector.

When iterating, CBE objects are read one by one from the queue, and delivered to the GLA Connector. The CBE object itself is stored into an Attribute called "*rawCBEObject*" of the work Entry. The CBE attributes are also set in the work Entry.

In order to be able to handle the situation when more than one Connector instance is running simultaneously a mechanism to send the correct CBE objects to the correct GLA Connector is required. This is achieved by using a unique correlation ID parameter in the TDIOutputter configuration. Before a GLA Connector starts the adapter configuration file it gets the correlation ID from the TDIOutputter configuration (the Connector actually parses the adapter configuration file). Then it registers it in an internal TDIOutputter table. When the TDIOutputter is ready to send the generated CBE object it gets its correlation ID and takes the GLA Connector which is registered with this ID in the table.

## Schema

The unprocessed, raw CBE object read from the TDIoutputter queue object is available in the following attribute, ready to be mapped into the *work* entry:

Table 3.

| Attribute Name | Description   |
|----------------|---|
| \$rawCBE       | This attribute holds a single CBE object which is a result of the processed application log file. The number of the CBE objects depends on the configuration of the parser in the adapter configuration file. |

The remaining attributes follow the specification as outlined in the output map schema definition in the documentation for the “CBE Generator Function Component” on page 347.

## See Also

The example demonstrating the processing of a DB2 log file, in the <TDI \_install\_directory>/examples/glaconnector directory,

“RAC Connector” on page 183,

“CBE Generator Function Component” on page 347.



---

## HTTP Client Connector

The HTTP Client Connector enables greater control on HTTP sessions than the URL Connector provides. With the HTTP Connector you can set HTTP headers and body using predefined attributes. Also, any request to a server that returns data is available for the user as attributes.

This Connector supports secure connections using the SSL protocol when so requested by the server, for example when accessing a server using the 'https://' prefix in an URL. If client-side certificates are required by the server, you will need to add these to the TDI truststore, and configure the truststore in `global.properties` or `solution.properties`. More information about this can be found in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*, in the section named "Client SSL configuration of TDI components".

**Note:** The HTTP Client Connector does not support the Advanced Link Criteria (see "Advanced link criteria" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

### Modes

The HTTP client Connector can be used in four different AssemblyLine modes. These are:

#### Iterator

Each call to the Connector requests the same URL configured for the Connector. This causes the Connector to run forever requesting the same page unless you include a Parser in the Connector's configuration. If you include a Parser, the Parser notifies when the last entry has been read from the connection and the Connector eventually causes an AssemblyLine to stop.

#### Lookup

In this mode the Connector requests a page every time the Lookup function is called. In your search criteria you can specify the page or URL to request, or include any number of parameters all of which are appended to the base URL as request parameters.

#### AddOnly

In this mode the Connector request is performed much like the Iterator mode.

#### Call/Reply

In this mode the Connector has two attribute maps, Input and Output. When the AssemblyLine invokes the Connector, an Output map operation is performed, followed by an Input map operation.

### Lookup Mode

In Lookup mode you can dynamically change the request URL by setting the search criteria as follows:

- If you have only one criteria and the attribute is named **url**, then the value specified in the criteria is used as the request URL.

```
url equals $url
```

- If you have more than one criteria or the only criteria is anything but **url**, then all attribute names and values are appended to the URL given by the Connector configuration as the request URL.

```
Base URL: http://www.example_page_only.com/lookup.cgi
```

```
Search Criteria:
```

```
name equals john  
mail equals doe.com
```

```
Resulting URL: http://www.example_page_only.com/lookup.cgi?name=john&mail=doe.com
```

- The Lookup function ignores the operand. So if you specify **contains** instead of **equals** the Connector still constructs the URL as if equals where used.

## Special attributes

When using the Connector in Iterator or Lookup mode the following set of attributes or properties is returned in the Connector ("*conn*") entry:

### **http.responseCode**

The HTTP response code as an Integer object.

200 OK → 200

### **http.responseMsg**

The HTTP response message as a String object.

200 OK → OK

### **http.content-type**

The content type for the returned `http.body` (if any).

### **http.content-encoding**

The encoding of the returned `http.body` (if any).

### **http.content-length**

The number of bytes in `http.body`.

### **http.body**

This object is an instance/subclass of `java.io.InputStream` class that can be used to read bytes of the returned body.

```
var body = conn.getObject ("http.body");
var ch;
```

```
while ( (ch = body.read()) != -1 ) {
    task.logmsg ("Next character: " + ch);
}
```

Consult the Javadocs for the `InputStream` classes and their methods.

### **http.body.response**

When the Connector operates in `AddOnly` mode, responses from the server `http.body` part will be made available in this Attribute; and the `http.body` Attribute as it was on the outbound call will be unmodified. If on the outbound call you did not specify a value in the `http.body` Attribute, then on return from the server the `http.body` Attribute will be identical to the `http.body.response` Attribute.

### **http.text-body**

If the `http.content-type` starts with the sequence `text/`, the Connector assumes the body is textual data and reads the `http.body` stream object into this attribute.

When using the Connector in `AddOnly` mode the Connector transmits any attribute named **http.** as a header. Thus, to set the content type for a request name the attribute **http.content-type** and provide the value as usual. One special attribute is **http.body** that can contain a string or any `java.io.InputStream` or `java.io.Reader` subclass.

For all modes the Connector always sets the **http.responseCode** and **http.responseMsg** attributes. In `AddOnly` mode this is special because the **conn** object being passed to the Connector is the object being populated with these attributes. To access these you must obtain the value in the Connector's **After Add** hook.

## Configuration

The Connector has the following parameters:

### **HTTP URL**

The HTTP page to request.

**Note:** If you use an `https://` address, you might need to import a certificate as well.

### Request Method

The HTTP method to use when requesting the page. See <http://www.w3.org/Protocols/HTTP/Methods.html> for more information

### Username

If set the HTTP Authorization header is set using this parameter along with the **Password** parameter.

### Password

Used if **Username** is specified.

**Proxy** If specified, connect to a proxy server rather than directly to the host specified in the URL. The format is *proxyhost:port* (for example, *proxy:8080*), where *proxy* is the name of the *proxyhost*, and 8080 is the *port* number to use.

### File to HTTP Body

The full path of the file. The file contents are copied as HTTP body in the HTTP message. This overrides any possible Parser processing.

### Content Type

If set, this will be used as the *http.content-type* for the file sent as specified by the **File to HTTP Body** parameter, or other *HTTP Body Attribute* that may be present in the Entry (see the HTTP Attributes described above).

### File from Response HTTP Body

The full path of the file. The body of the response HTTP message is copied to the file.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

You select a Parser from the Parser pane; select the parser by clicking the bottom-right **Inherit From:** button. If specified, this Parser is used to generate the **http.body** content when sending data. The parser gets an entry with those attributes where the name does not begin with **http**. Also, this Parser (if specified) gets the **http.body** for additional parsing when receiving data. However, do not specify `system:/Parsers/ibmdi.HTTP`, because a message body does not contain another message.

## Examples

In your attribute map you can use the following assignment to post the contents of a file to the HTTP server:

```
// Attribute assignment for "http.body"
ret.value = new java.io.FileInputStream ("myfile.txt");

// Attribute assignment for "http.content-type"
ret.value = "text/plain";
```

The Connector computes the **http.content-length** attribute for you. There is no need to specify this attribute.

## See also

“URL Connector” on page 227,  
“HTTP Server Connector” on page 91,  
“HTTP Parser” on page 297.



---

## Old HTTP Client Connector

**Note:** This Connector is kept for legacy purposes only. If you are setting up a new Connector, please use the HTTP Client Connector instead.

The Old HTTP Client Connector enables greater control on HTTP sessions than the URL Connector provides. With the HTTP Connector you can set HTTP headers and body using predefined attributes. Also, any request to a server that returns data is available for the user as attributes.

**Note:** The Old HTTP Client Connector does not support the Advanced Link Criteria (see "Advanced link criteria" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

### Modes

The Old HTTP Client Connector can be used in three different AssemblyLine modes. These are:

#### Iterator

Each call to the Connector requests the same URL configured for the Connector. This causes the Connector to run forever requesting the same page unless you include a Parser in the Connector's configuration. If you include a Parser, the Parser notifies when the last entry has been read from the connection and the Connector eventually causes an AssemblyLine to stop.

#### Lookup

In this mode the Connector requests a page every time the Lookup function is called. In your search criteria you can specify the page or URL to request, and include any number of parameters all of which are appended to the base URL as request parameters.

#### AddOnly

In this mode the Connector request is performed much like the Iterator mode.

### Lookup Mode

In Lookup mode you can dynamically change the request URL by setting the search criteria as follows:

- If you have one and only one criteria and the attribute is named **url** then the value specified in the criteria is used as the request URL.  
url equals \$url
- If you have more than one or the only criteria is anything but url, then all attribute names and values are appended to the URL given by the Connector configuration as the request URL.

Base URL: `http://www.example_name.com/lookup.cgi`

Search Criteria:

```
name equals john  
mail equals doe.com
```

Resulting URL: `http://www.example_name.com/lookup.cgi?name=john&mail=doe.com`The Lookup function ignores the operand. So if you specify *contains* instead of *equals* the Connector still constructs the URL as if equals where used.

### Special attributes

When using the Connector in Iterator or Lookup mode the following set of attributes or properties is returned in the Connector entry:

#### **http.responseCode**

The HTTP response code as an Integer object.

200 OK —> 200

#### **http.responseMsg**

The HTTP response message as a String object.

200 OK → OK

#### **http.content-type**

The content type for the returned `http.body` (if any).

#### **http.content-encoding**

The encoding of the returned `http.body` (if any).

#### **http.content-length**

The number of bytes in `http.body`.

#### **http.body**

This object is an instance/subclass of `java.io.InputStream` class that can be used to read bytes of the returned body.

```
var body = conn.getObject ("http.body");
var ch;

while ( (ch = body.read()) != -1 ) {
    task.logmsg ("Next character: " + ch);
}
```

Consult the Javadocs for the `InputStream` classes and their methods.

#### **http.text-body**

If the `http.content-type` starts with the sequence `text/`, the Connector assumes the body is textual data and reads the `http.body` stream object into this attribute.

When using the Connector in `AddOnly` mode the Connector transmits any attribute named **http**. as a header. Thus, to set the content type for a request, name the attribute **http.content-type** and provide the value as usual. One special attribute is **http.body** that can contain a string or any `java.io.InputStream` or `java.io.Reader` subclass.

For all modes the Connector always sets the **http.responseCode** and **http.responseMsg** attributes. In `AddOnly` mode this is a bit special since the **conn** object being passed to the Connector is the object being populated with these attributes. To access these you must obtain the value in the Connector's **After Add** hook.

## **Configuration**

The Connector has the following parameters:

#### **HTTP URL**

The HTTP page to request.

#### **Request Method**

The HTTP method to use when requesting the page. See <http://www.w3.org/Protocols/HTTP/Methods.html> for more information.

#### **Username**

If set, the HTTP Authorization header uses this parameter along with the **Password** parameter.

#### **Password**

Used if **Username** is specified.

#### **Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Parser** If specified, this Parser is used to generate the posted data for an **Add** operation.

## **Examples**

In your attribute map you can use the following assignment to post the contents of a file to the HTTP server:

```
// Attribute assignment for "http.body"  
ret.value = new java.io.FileInputStream ("myfile.txt");  
  
// Attribute assignment for "http.content-type"  
ret.value = "text/plain";
```

The Connector computes the **http.content-length** attribute for you. There is no need to specify this attribute.

## See also

“URL Connector” on page 227,  
“Old HTTP Server Connector” on page 95,  
“HTTP Client Connector” on page 83.





---

## HTTP Server Connector

IBM Tivoli Directory Integrator provides a HTTP server Connector that listens for incoming HTTP connections and acts like a HTTP server. Once it receives the request, it parses the request and sends the parsed request to the AssemblyLine workflow to process it. The result is sent back to the HTTP client. By default, the returned result has a content-type of "text/html".

If a Parser is specified then the Connectors process **post** requests and parse the contents using the specified Parser. **get** requests do not use the Parser. If a **post** request is received and no Parser is specified the contents of the **post** data is returned as an attribute (**postdata**) in the returned entry.

The HTTP Server Connector uses `ibmdi.HTTP` as internal Parser if no Parser is specified.

The HTTP Server Connector supports Server mode only.

The Connector parses URL requests and populates an entry in the following manner:

```
http://localhost:8888/path?p1=v1&p2=v2
```

```
http.method : 'GET'  
http.Host   : 'localhost:8888'  
http.base   : '/path'  
http.qs.p1  : 'v1'  
http.qs.p2  : 'v2'  
http://localhost:8888/?p1=v1&p2=v2
```

```
http.method : 'GET'  
http.Host   : 'localhost:8888'  
http.base   : '/'  
http.qs.p1  : 'v1'  
http.qs.p2  : 'v2'
```

If a **post** request is used then it is expected that the requestor is sending data on the connection as well. Depending on the value for the **Parser** parameter the Connector does the following:

### Parser present

Instantiates the Parser with the HTTP input stream. Connector delegates `getNext` to the Parser's `getEntry` and returns whatever the Parser returns.

### Parser not present

Puts contents of post data in a Connector attribute called **http.body**.

The session with the HTTP client is closed when the Connector receives a `getNext` request from the AssemblyLine and there is no more data to fetch. For example, if the Parser has returned a null value, or on the second call to `getNext` if no Parser is present.

## Connector structure and workflow

The HTTP Server Connector receives HTTP requests from HTTP clients and sends HTTP responses back. As mentioned above, the default content-type header is set to "text/html"; you can override that by setting the Entry attribute `http.content-type` to the appropriate value before the Connector returns the result to the client.

After the AssemblyLine initializes the HTTP Server Connector, it calls the `getNextClient()` method of the Connector. This method blocks until a client request arrives. When a request is received, the Connector creates a new instance of itself, which is handed over to the AssemblyLine that spawns a new AssemblyLine thread for that Connector instance. This design feature provides the ability to process each Event in a separate thread, which allows the HTTP Server Connector to process several HTTP events in parallel. The AssemblyLine then calls the `getNextEntry()` method on this new Connector instance in the new thread. Each Entry returned by the `getNextEntry()` call represents an individual HTTP request from

the HTTP client. The Connector's `replyEntry(Entry conn)` method is called for each Entry returned from `getNextEntry()` to send to the client the corresponding HTTP response.

## Connector Client Authentication

The parameter HTTP Basic Authentication governs whether client authentication will be mandated for HTTP clients accessing this connector over the network.

There are two different ways to implement HTTP Basic Authentication with the HTTP Server Connector:

### 1. Using an Authentication Connector

This is a mechanism for backward compatibility with the deprecated HTTP EventHandler. A connector parameter **Auth Connector** specifies a TDI Connector that will be used in Lookup Mode, with the username and password for the HTTP Basic Authentication data specified as the Link Criteria:

- If the lookup returns an Entry, the authentication is considered successful and the HTTP Server Connector proceeds with processing the client's request.
- If the lookup cannot find an Entry, the client is not authenticated and the request will not be processed.

### 2. Script authentication

This mechanism requires a certain amount of coding, but provides more power and lets you implement authentication through your own scripting. It can only be used when the **Auth Connector** parameter is NULL or empty.

The Connector will make available to you the username and password values in the "After Accepting connection" Hook through the `getUserName()` and `getPassword()` public Connector methods. It is now your responsibility to implement the authentication mechanism. You should call the Connector's `rejectClientAuthentication()` method from the AssemblyLine hook if authentication is not successful. Consider the following example authentication script code:

```
var httpServerConn = conn.getAttribute("connectorInterface").getValue(0);
var username = httpServerConn.getUserName();
var password = httpServerConn.getPassword();

//perform verification here
successful = true;

if (!successful) {
    httpServerConn.rejectClientAuthentication();
}
```

## Chunked Transfer Encoding

When the parameter **Chunked Transfer Encoding** is enabled, the Connector will write the HTTP body as series of chunks.

When chunked encoding is used, the user is responsible for calling the Connector's `putEntry(entry)` method for each chunk – the value of the "http.body" Attribute of the Entry provided will be sent as an HTTP chunk. The `replyEntry(entry)` Connector's method is automatically called by the AssemblyLine at the end of the iteration – it will write the last chunk of data (if the "http.body" Attribute is present) and close the chunk sequence.

When a Parser is specified to the HTTP Server Connector, it will be the stream returned by the Parser that will be sent as a HTTP chunk on each `putEntry(entry)` or `replyEntry(entry)` call.

## Configuration

The Connector needs the following parameters:

### TCP Port

The TCP port to listen for incoming requests (the default port is 80).

### **Connection Backlog**

This represents the maximum queue length for incoming connection indications (a request to connect). If a connection indication arrives when the queue is full, the connection is refused.

### **Content Type**

The default HTTP content type to use for outbound data. This value is overridden by the "http.content-type" Attribute of the work object. The default is text/html.

### **TCP Data as Properties**

If the check box is checked (default), the TCP connection properties are accessed through the getProperty() method of the work Entry object. If unchecked, the TCP connection properties appear as Entry Attributes.

### **HTTP Headers as Properties**

If the check box is checked (default), all HTTP headers are accessible using the getProperty() method of the work Entry object. If unchecked, all HTTP headers appear as Entry Attributes.

### **HTTP Basic Authentication**

If enabled (by default it is not), clients will be challenged for HTTP Basic authentication.

### **Auth Realm**

The authentication realm sent to the client when requesting HTTP Basic authentication. The default is "IBM Tivoli Directory Integrator".

### **Auth Connector**

This drop-down list specifies an Authenticator Connector. If a Connector is specified it must exist in the Connector library and be configured for Lookup mode.

When this parameter is specified, the HTTP Server Connector will issue authentication requests to any client (e.g., a Web browser) that tries to access this service and does not provide authentication data. When the client provides the username/password the HTTP Server Connector will call the Authenticator Connector's lookup method providing the username and password attributes. Hence, the authentication Connector must be configured using a Link Criteria where the \$username and \$password attributes are used. A typical link criteria would be:

```
username equals $username  
password equals $password
```

If the search fails, the HTTP Server Connector denies the request and sends an authentication request back to the client. If the search succeeds, the HTTP Server Connector processes the request.

The entry returned by the authenticator Connector can be accessed through the "auth.entry" Property of the event Entry.

For more details on client authentication, and for an alternative method to using an Auth Connector, see "Connector Client Authentication" on page 92.

### **Use SSL**

If enabled (by default it is not), then the Connector will require clients to use SSL; non-SSL connection requests will fail.

When SSL is used, the Connector will use the default TDI Server SSL settings – certificates, keystore and truststore.

### **Require Client Authentication**

If enabled (by default it is not), the Connector mandates client authentication when using SSL. This means that the Connector will require clients to supply client-side SSL certificates that can be matched to the configured TDI trust store. This parameter is only taken into account if the previous parameter (Use SSL) is enabled as well.

### Chunked Transfer Encoding

If checked, the HTTP body of the message is transferred as a series of chunks; see “Chunked Transfer Encoding” on page 92.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Note:** You can select a Parser from the **Parser** configuration pane; click on the *Inherit from:* button in the bottom right corner when the Parser pane is active.

## Connector Schema

Listed below are all the Attributes supported by the HTTP Server Connector.

### Input Attributes

- http.\* - Any HTTP header.
- http.Authorization - The type of http authorization.
- http.base - HTTP base parameter.
- http.body - The body of HTTP request.
- http.content-length - The number of bytes in http.body.
- http.content-type - The type of HTTP content, for example text/plain, text/xml, etc.
- http.method - HTTP method type. Valid values are: GET/POST/PUT
- http.qs.\* - Query string parameter.
- http.remote-pass - The remote user password.
- http.remote-user - The remote username.
- auth.entry - The entry returned by the authenticator Connector.
- tcp.inputstream - Socket input stream.
- tcp.outputstream - Socket output stream.
- tcp.remoteIP - Remote IP address.
- tcp.remotePort - Remote port.
- tcp.remoteHost - Remote host name.
- tcp.localIP - Local IP address.
- tcp.localPort - Local port.
- tcp.localHost - Local host name.
- tcp.socket - Raw socket object.

### Output Attributes

- http.body - The body of HTTP response.
- http.content-type - The type of HTTP content.
- http.redirect - Redirect client to specified location.
- http.status - Status code of returned operation.

### See also

“URL Connector” on page 227,

“HTTP Client Connector” on page 83,

“HTTP Parser” on page 297.

---

## Old HTTP Server Connector

**Note:** This Connector is kept for legacy purposes only. If you are creating a new Connector, please use HTTP Server Connector instead.

The Old HTTP Server Connector listens for incoming HTTP connections and returns the **get** parameters as an entry. If a Parser is specified then the Connectors process **post** requests and parse the contents using the specified Parser. **get** requests do not use the Parser. If a **post** request is received and no Parser is specified, the contents of the **post** data are returned as an attribute (**postdata**) in the returned entry.

The Connector parses URL requests and populates an entry in the following manner:

```
http://host/path?p1=v1&p2=v2
```

```
entry.path = "/path"  
entry.p1="v1"  
entry.p2="v2"
```

```
http://host?p1=v1&p2=v2
```

```
entry.path="/"   
entry.p1="v1"   
entry.p2="v2"
```

If a **POST** request is used then it is expected that the requestor is sending data on the connection as well. Depending on the value for the **Parser** parameter the Connector does the following:

### Parser present

Instantiates the Parser with the HTTP input stream. Connector delegates getNext to the Parser's getEntry and returns whatever the Parser returns.

### Parser not present

Puts contents of post data in an attribute called **postdata**.

```
entry.postdata = "postdata"
```

The session with the HTTP client is closed when the Connector receives a getNext request from the AssemblyLine and there is no more data to retrieve. For example, if the Parser has returned a null value, or on the second call to getNext no Parser is present. If you call getNext (for example, iterate) after having received a null from the Connector.

## Configuration

The Connector needs the following parameters:

### TCP Port

The TCP port to listen to (the default port is 80).

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Parser** The name of a Parser to handle the contents of **post** requests.

## See also

"URL Connector" on page 227,

"HTTP Server Connector" on page 91.



---

## IBM Directory Server Changelog Connector

The IBM Directory Server Changelog Connector is a specialized instance of the LDAP Connector. The IBM Directory Server Changelog Connector contains logic to iterate the Changelog. It returns various attributes, including the **changes** attribute. The Connector returns **changes** as something that looks like a standard attribute, but it is in fact of the Entry class.

The Connector can be used in batch-oriented runs where it starts at a specific change number and stops after the last **Changelog** entry. It can also be run in continuous mode where you specify the timer values for periodically checking for the next **Changelog** entry.

The Connector reads Changelog entries and automatically increases the Changelog counter by one for each iteration. When the Connector tries to read a non-existing Changelog entry, the Connector goes to sleep for a period of time (**Sleep Interval**). If the total time the Connector is waiting for a new entry exceeds the **Timeout** value, then the Connector returns to the caller with a **null** value (end of iteration).

This connector also exposes a “**Use Notifications**” option which specifies whether the Connector will use a polling or a notification mechanism to retrieve new IDS changes. If set to “false” the Connector will operate as in TDI 6.0 and will poll for new changes. If this parameter is set to “true” then after processing all existing changes the Connector will block and wait for an unsolicited event notification from the IBM Directory Server. The Connector will not sleep and timeout when the notification mechanism is used.

This connector also supports Delta Tagging, at the Entry level, the Attribute level and the Attribute Value level. It is the LDIF Parser that provides Delta support at the Attribute and Attribute Value levels.

## Configuration

The Connector needs the following parameters:

### LDAP URL

The LDAP URL for the connection (`ldap://host:port`).

### Login username

The LDAP distinguished name used for authentication to the server. Leave blank for anonymous access.

### Login password

The credentials (password).

### Authentication Method

The authentication method. Possible values are:

- CRAM-MD5 (use the CRAM-MD5 (RFC-2195) SASL mechanism).
- none (use no authentication (**anonymous**)).
- simple (use weak authentication (cleartext password)).
- If not specified, default (simple) is used. If **Login username** and **Login password** are blank, then **anonymous** is used.

### Use SSL

If Use SSL is **true** (that is, checked), the Connector uses SSL to connect to the LDAP server. Note that the port number might need to be changed accordingly.

### ChangeLog Base

The search base where the Changelog is kept. The standard DN for this is **cn=changelog**.

### Extra Provider Parameters

Allows you to pass a number of extra parameters to the JNDI layer. It is specified as name:value pairs, one pair per line.

### Iterator State Key

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

### Start at changenumber

Specifies the starting changenumber. Each Changelog entry is named **changenumber=intvalue** and the Connector starts at the number specified by this parameter and automatically increases by one. The special value **EOD** means start at the end of the Changelog.

### State Key Persistence

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and choices are:

#### After read

Updates the System Store when you read an entry from the directory server's change log, before you continue with the rest of the AssemblyLine.

#### End of cycle

Updates the System Store with the change log number when all Connectors and other components in the AssemblyLine have been evaluated and executed.

#### Manual

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the IBM Directory Server Changelog Connector's *saveStateKey()* method, somewhere in your AssemblyLine.

### Use Notifications

Specifies whether to use notification when waiting for new changes in IBM Directory Server. If enabled, the Connector will not sleep or timeout, but instead wait for a Notification event from the IBM Directory Server.

### Batch retrieval

Specifies how searches are performed in IDS changelog. When unchecked, the Connector will perform incremental lookups (backward compatible mode). When checked, and the server supports "Sort Control", searches will be performed with query '*changenumber>=some\_value*', corresponding to the last retrieval you made; this works in conjunction with the next parameter, **Page Size**. By default, this option is unchecked.

### Page Size

Specifies the size of the pages IDS will return entries on (default value is 500). It is used only when **Batch retrieval** is set to true, i.e, checked.

### Timeout

Specifies the number of seconds the Connector waits for the next Changelog entry. The default is 0, which means wait forever.

### Sleep Interval

Specifies the number of seconds the Connector sleeps between each poll. The default is 60.

### Detailed Log

If this field is checked, additional log messages are generated.

## See also

"LDAP Connector" on page 133,

"Active Directory Changelog (v.2) Connector" on page 13,

"Exchange Changelog Connector" on page 71

"Netscape/iPlanet/Sun Directory Changelog Connector" on page 161,

"z/OS Changelog Connector" on page 233.





---

## ITIM Agent Connector

The ITIM Agent Connector uses the IBM Tivoli Identity Manager's JNDI driver to connect to ITIM Agents (the JNDI driver uses the DAML protocol). Thus the ITIM Agent Connector is able to connect to all ITIM Agents that support the DAML protocol.

The Connector itself does not understand the particular schema of the ITIM Agent it is connected to – it provides the basic functionality to create, read, update and delete JNDI entries.

The ITIM Agent Connector supports the Iterator, Lookup, AddOnly, Update and Delete modes.

This Connector uses the client library `enroleagent.jar` from the ITIM 4.6 release.

## Setting up SSL for the ITIM Agent Connector

Since the `enroleagent.jar` client library uses JSSE (Java based keystore/truststore) for SSL authentication, you are now required to mention the SSL-related certificate details in the `global.properties/solution.properties`; previous versions of the ITIM Agent Connector required you to specify the certificate name in the "CA Certificate File" parameter. You need to first import the ITIM Agent's certificate into the TDI truststore.

For example, with the following command you import the `servercertificate.der` file into `tim.jks`.

```
keytool -import -file servercertificate.der -keystore tim.jks
```

After you import the certificate, you need to mention this truststore in the "server authentication" section of the `global.properties /solution.properties` file.

```
## server authentication
```

```
javax.net.ssl.trustStore=E:\IBMDirectoryIntegrator\tim.jks  
{protect}-javax.net.ssl.trustStorePassword=<jks_keystore_password>  
javax.net.ssl.trustStoreType=jks
```

**Note:** The "CA Certificate File" property of the ITIM Agent Connector is no longer present, since now the certificates mentioned in the JKS trust store in `global.properties` or `solution.properties` are being used.

## Configuration

The Connector needs the following parameters:

### Agent URL

The URL used to connect to the ITIM Agent, in the form "https://<agent\_ip\_address>:<port>", for example "https://localhost:45580"

### UserName

The username specified in the configuration of the ITIM Agent – used by the Connector to authenticate to the ITIM Agent.

### Password

The password specified in the configuration of the ITIM Agent – used by the Connector to authenticate to the ITIM Agent.

### Connection Retry Count

Specifies how many times to retry a failed connection (including initial connection attempt). If no value is specified the ITIM JNDI driver uses a default value of 3.

### Search Filter

Filter expression to use in Iterator mode. If no value is specified a default filter of "(objectclass=\*)" is used to return all Entries.

## Detailed Log

Checking this parameter generates extra log messages.

## Known Issues

The Connector has been briefly tested with a few ITIM Agents. Some lookup issues have been detected that result from constraints of the underlying Agents implementation:

Sometimes simple JNDI searches might not return the expected results. For example, if you are using the Windows 2000 Agent, the JNDI search for the Guest user account "(eruid=Guest)" might return more than one Entries; or when you are using the Red Hat Linux Agent the search for the "root" group "(erLinuxGroupName=root)" returns an empty result set.

A work-around for these cases is to use an extended search filter where the object class is specified: "((&(eruid=)(objectclass=<classname>))". So for the Windows 2000 Agent the search would look like "((&(eruid=Guest)(objectclass=erW2KAccount))" and for the Red Hat Linux Agent the search filter should be "((&(eruid=root)(objectclass=erLinuxGroup))".

This work-around does not work for all lookup issues, for example the search for the Windows "Administrators" group (Windows 2000 Agent) – "(erW2KGroupName=Administrators)" returns an empty result set. The extended search filter "((&(eruid=Administrators)(objectclass=erW2KGroup))" returns an empty result set too.

When you encounter a lookup problem:

1. 1. Make sure you are using the latest version of the Agent.
2. 2. Try the work-around described above.
3. 3. If the work-around doesn't work, examine the schema of the Agent for other attributes that can be used for Entry identification.

Here are a few examples for how other attributes from the Agent schema can be used for Entry identification:

- In the search for the Windows "Administrators" group mentioned above, instead of "erW2KGroupName" attribute, the attribute "erW2KGroupCommonName" could be used. The filter "(erW2KGroupCommonName=Administrators)" works fine and you will get the "Administrators" group Entry.
- For the LDAP-X Agent, searches for LDAP users ("erXLdapAccount" class) with the default "eruid" attribute might fail – in this case you can use the "cn" attribute for Entry identification.

## See also

"ITIM DSMLv2 Connector" on page 61



---

## JDBC Connector

The JDBC Connector provides database access to a variety of systems. To reach a system using JDBC you need a JDBC driver from the system provider. This provider is typically delivered with the product in a jar or zip file. These files must be in your path or copied to the jars/ directory of your TDI installation; otherwise you may get cryptic messages like "Unable to load T2 native library", indicating that the driver was not found on the classpath.

You will also need to find out which of the classes in this jar or zip file implements the JDBC driver; this information goes into the **JDBC Driver** parameter.

The JDBC Connector also provides multi-line input fields for the SELECT, INSERT, UPDATE and DELETE statements. When configured, the JDBC connector will use the value for any of these instead of its own auto-generated statement. The value is a template expanded by the parameter substitution module that yields a complete SQL statement. The template has access to the connector configuration as well as the *searchcriteria* and *conn* objects. The *work* object is not available for substitution, since the connector does not know what *work* contains. Additional provider parameters are also supported in the connector configuration.

The JDBC Connector supports the following modes: AddOnly, Update, Delete, Lookup, Iterator, Delta.

This Connector in principle can handle secure connections using the SSL protocol; but it may require driver-specific configuration steps in order to set up the SSL support. Refer to the manufacturer's driver documentation for details.

### Connector structure and workflow

The JDBC connector makes a connection to the specified data sources during the connector initialization. While making a connection to the specified data source extra provider parameters are checked for, and set if they are specified. The auto-commit flag setting is also handled and set during connection initialization.

The JDBC connector builds SQL statements internally using a predefined mapping table. The connector flow behaves the same way as other connectors in AddOnly, Update, Delete, Iterator and Lookup modes.

In addition, this Connector supports Delta mode; the delta functionality for the JDBC connector is handled by the ALComponent (a generic building block common to all Connectors). The ALComponent will do a lookup and apply the delta Entry to a target Entry before doing an update, and then decide what the correct database operation must be. The Connector will then use the SQL statements for add, modify or delete, corresponding to what the operation is.

### Understanding JDBC Drivers

In order for the JDBC Connector to access a relational database, it needs to access a *driver*, a set of subroutines or methods contained in a Java classlibrary. This library must be present in the *classpath* of TDI, otherwise TDI will not be able to load the library when initializing the Connector, and hence be unable to talk to the Relational Database (RDBMS). A good way to install a JDBC driver library such that TDI can use it is to copy it into the <TDI\_HOME>/jars directory.

There are 4 fundamental ways of accessing an RDBMS through JDBC (these are often referred to as driver types):

1. Drivers that implement the JDBC API as a mapping to another data access API, such as Open Database Connectivity (ODBC). Drivers of this type are generally dependent on a native library, which limits their portability. The JDBC-ODBC Bridge driver is an example of a Type 1 driver; this driver is generally part of the JVM, so it does not need to be specified separately on the TDI classpath.

To configure ODBC, see “Specifying ODBC database paths” on page 107.

**Note:** The JDBC-ODBC bridge may be present in any of the different platform-dependent JVM's that IBM ships with the product. However, IBM supports the JDBC-ODBC bridge on Windows platforms only. In addition, performance is likely to be sub-optimal compared to a dedicated, native (“Type 4”) driver. Commercial ODBC/JDBC bridges are available. If you need an JDBC-ODBC bridge, consider purchasing a commercially available bridge; see also the JDBC-ODBC bridge drivers discussion at <http://java.sun.com/products/jdbc/drivers.html>.

2. Drivers that are written partly in the Java programming language and partly in native code. The drivers use a native client library specific to the data source to which they connect. Again, because of the native code, their portability is limited.
3. Drivers that use a pure Java client and communicate with a middleware server using a database-independent protocol. The middleware server then communicates the client’s requests to the data source.
4. Drivers that are pure Java and implement the network protocol for a specific data source. The client connects directly to the data source.

With the exception of the JDBC-ODBC bridge on Windows, we only use Type 4 drivers with IBM Tivoli Directory Integrator. We will discuss other types as well—in the context of each of the supported databases—for a better understanding.

JDBC Type 3 and Type 4 drivers use a network protocol to communicate to their back-ends. This usually implies a TCP/IP connection; this will either be a straight TCP/IP socket, but if the driver supports it, it can be a Secure Socket Layer (SSL) connection.

## Connecting to DB2

The IBM driver for JDBC and SQLJ bundled with TDI was obtained from <http://www-306.ibm.com/software/data/db2/java>. It is JDBC 1.2, JDBC 2.0, JDBC 2.1 and JDBC 3.0 compliant.

Information about the JDBC driver for IBM DB2® is available online; a starting point and example for configuration purposes is the section on “Connecting to database servers in JDBC applications” in the DB2 Developer documentation. This driver may or may not suit your purpose.

### Driver Licensing

This driver does not need further licensing for Cloudscape and other DB2 database systems (that is, the appropriate license files, `db2jcc_license_c.jar` and `db2jcc_license_cu.jar` are already included), except DB2 for z/Series and iSeries. In order for the driver to be able to communicate with the latter two systems you would need to obtain the DB2 Connect product, and copy its license file, `db2jcc_license_cisuz.jar`, to the `jars/3rdparty/IBM` directory.

Based on the JDBC driver architecture DB2 JDBC drivers are divided into four types.

#### 1. DB2 JDBC Type 1

This is an DB2 ODBC (not JDBC) driver, that you connect to using a JDBC-ODBC bridge driver. This driver is essentially not used anymore.

A JDBC Type 1 driver can be used by JDBC 1.2 JDBC 2.0, and JDBC 2.1.

To configure ODBC, see “Specifying ODBC database paths” on page 107.

#### 2. DB2 JDBC Type 2

The DB2JDBC Type 2 driver is quite popular and is often referred to as the *app* driver. The *app* driver name comes from the notion that this driver will perform a native connect through a local DB2 client to a remote database, and from its package name (`COM.ibm.db2.jdbc.app.*`).

In other words, you have to have a DB2 client installed on the machine where the application that is making the JDBC calls runs. The JDBC Type 2 driver is a combination of Java and native code, and will therefore usually yield better performance than a Java-only Type 3 or Type 4 implementation.

This driver's implementation uses a Java layer that is bound to the native platform C libraries. Programmers using the J2EE programming model will gravitate to the Type 2 driver as it provides top performance and complete function. It is also certified for use on J2EE servers.

The implementation class name for this type of driver is *com.ibm.db2.jdbc.app.DB2Driver*.

The JDBC Type 2 drivers can be used to support JDBC 1.2, JDBC 2.0, and JDBC 2.1.

### 3. DB2 JDBC Type 3

The JDBC Type 3 driver is a pure Java implementation that must talk to middleware that provides a DB2 JDBC Applet Server. This driver was designed to enable Java applets to access DB2 data sources. An application using this driver can talk to another machine where a DB2 client has been installed.

The JDBC Type 3 driver is often referred to as the net driver, appropriately named after its package name (COM.ibm.db2.jdbc.net.\*).

The implementation class name for this type of driver is *com.ibm.db2.jdbc.net.DB2Driver*.

The JDBC Type 3 driver can be used with JDBC 1.2, JDBC 2.0, and JDBC 2.1.

### 4. DB2 JDBC Type 4

The JDBC Type 4 driver is also a pure Java implementation. An application using a JDBC Type 4 driver does not need to interface with a DB2 client for connectivity because this driver comes with Distributed Relational Database Architecture™ Application Requester (DRDA® AR) functionality built into the driver.

The implementation class name for this type of driver is *com.ibm.db2.jcc.DB2Driver*.

The latest version of this driver (9.1) supports SSL connections; this requires setting a property in the **Extra Provider Parameters** field. For more information see <http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.apdv.java.doc/doc/rjvdsprp.htm>. Note that the target database must be set up such that it accepts incoming SSL connections.

If you are running DB2 on a z/OS platform, and the database is not configured correctly with the required stored procedure for retrieving the schema, you might encounter some problems using the JDBC Connector. If the JDBC Connector's query schema throws an exception, or the Add/Update action on JDBC tables fails for BLOB data types, contact your database administrator and request that the required stored procedure for retrieving the schema be installed. For more information about accessing DB2 from Java, see also Overview of Java Development in DB2 UDB for Linux, UNIX, and Windows.

## Connecting to Informix Dynamic Server

If you install the Informix Client SDK, you will also install Informix ODBC drivers which allow you to use a JDBC-ODBC bridge driver. This driver is not recommended for production use. To configure ODBC, see "Specifying ODBC database paths" on page 107.

However, we recommend you use the Informix JDBC driver, version 3.0. It is a pure-Java (Type 4) driver, which provides enhanced support for distributed transactions and is optimized to work with IBM WebSphere® Application Server.

It consists of a set of interfaces and classes written in the Java programming language. Included in the driver is Embedded SQL/J which supports embedded SQL in Java.

The implementation class for this driver is *com.informix.jdbc.IfxDriver*.

## Connecting to Oracle

Based on the JDBC driver architecture the following types of drivers are available from Oracle.

### 1. Oracle JDBC Type 1

This is an Oracle ODBC (not JDBC) driver, that you connect to using a JDBC-ODBC bridge driver. Oracle does supply an ODBC driver, but does not supply a bridge driver. Instead, you can use the

default JDBC-ODBC bridge that is part of the JVM, or get one of the JDBC-ODBC bridge drivers from <http://java.sun.com/products/jdbc/drivers.html>. This configuration works fine, but a JDBC Type 2 or Type 4 driver will offer more features and will be faster.

To configure ODBC, see “Specifying ODBC database paths” on page 107.

## 2. Oracle JDBC Type 2

There are two flavors of the Type 2 driver.

- JDBC OCI client-side driver

This driver uses Java native methods to call entrypoints in an underlying C library. That C library, called OCI (Oracle Call Interface), interacts with an Oracle database. The JDBC OCI driver requires an Oracle client installation of the same version as the driver. The use of native methods makes the JDBC OCI driver platform specific. Oracle supports Solaris, Windows, and many other platforms. This means that the Oracle JDBC OCI driver is not appropriate for Java applets, because it depends on a C library. Starting from Version 10.1.0, the JDBC OCI driver is available for installation with the OCI Instant Client feature, which does not require a complete Oracle client-installation. Please refer to the Oracle Call Interface for more information.

- JDBC Server-Side Internal driver

This driver uses Java native methods to call entrypoints in an underlying C library. That C library is part of the Oracle server process and communicates directly with the internal SQL engine inside Oracle. The driver accesses the SQL engine by using internal function calls and thus avoiding any network traffic. This allows your Java code to run on the server to access the underlying database in the fastest possible manner. It can only be used to access the same database.

## 3. Oracle JDBC Type 4

Again, there are two flavors of the Type 4 driver.

- JDBC Thin client-side driver

This driver uses Java to connect directly to Oracle. It implements Oracle’s SQL\*Net Net8 and TTC adapters using its own TCP/IP based Java socket implementation. The JDBC Thin client-side driver does not require Oracle client software to be installed, but does require the server to be configured with a TCP/IP listener. Because it is written entirely in Java, this driver is platform-independent. The JDBC Thin client-side driver can be downloaded into any browser as part of a Java application. (Note that if running in a client browser, that browser must allow the applet to open a Java socket connection back to the server.)

This is the most commonly-used driver. In general, unless you need OCI-specific features, such as support for non-TCP/IP networks, use the JDBC Thin driver.

The implementation class for this driver currently is *oracle.jdbc.driver.OracleDriver*.

- JDBC Thin server-side driver

This driver uses Java to connect directly to Oracle. This driver is used internally within the Oracle database, and it offers the same functionality as the JDBC Thin client-side driver, but runs inside an Oracle database and is used to access remote databases. Because it is written entirely in Java, this driver is platform-independent. There is no difference in your code between using the Thin driver from a client application or from inside a server.

For more information about accessing Oracle from Java, see also [Java, JDBC & Database Web Services](#), and the [Oracle JDBC FAQ](#).

## Connecting to SQL Server

The Microsoft SQL Server 2005 driver for JDBC supports the JDBC 1.22, JDBC 2.0 and JDBC 3.0 specification. It is a Type 4 driver.

The implementation class for this driver is *com.microsoft.sqlserver.jdbc.SQLServerConnection*. It is contained in the driver file *sqljdbc.jar*, typically obtained from the MS SQL Server 2005 installation, at `<Microsoft SQL Server 2005-Install-Dir>\sqljdbc_1.1.1501.101_enu\sqljdbc_1.1\enu\sqljdbc.jar`.

You can also use other third party drivers for connecting to Microsoft SQL Server.



The jTDS JDBC 3.0 driver distributed under the GNU LGPL is a good choice. This is a Type 4 driver and supports Microsoft SQL Server 6.5, 7, 2000, and 2005. jTDS is 100% JDBC 3.0 compatible, supporting forward-only and scrollable/updateable ResultSets, concurrent (completely independent) Statements and implementing all the DatabaseMetaData and ResultSetMetaData methods. It can be downloaded freely from <http://jtds.sourceforge.net>. More information about this driver is available from the Web site.

## Connecting to Sybase Adaptive Server

The jConnect for JDBC driver by Sybase provides high performance native access (Type 4) to the complete family of Sybase products including Adaptive Server Enterprise, Adaptive Server Anywhere, Adaptive Server IQ, and Replication Server.

jConnect for JDBC is an implementation of the Java JDBC standard; it supports JDBC 1.22 and JDBC2.0, plus limited compliance with JDBC 3.0. It provides Java developers with native database access in multi-tier and heterogeneous environments. You can download jConnect for JDBC quickly, without previous client installation, for use with thin-client Java applications - like IBM Tivoli Directory Integrator.

The implementation class name for this driver is *com.sybase.jdbc3.jdbc.SybDriver*.

You can also use other third party drivers for connecting to Sybase.

The jTDS JDBC 3.0 driver distributed under the GNU LGPL is a good choice. This is a Type 4 driver and supports Sybase 10, 11, 12 and 15. jTDS is 100% JDBC 3.0 compatible, supporting forward-only and scrollable/updateable ResultSets, concurrent (completely independent) Statements and implementing all the DatabaseMetaData and ResultSetMetaData methods. It can be downloaded freely from <http://jtds.sourceforge.net>. More information about this driver is available from the Web site.

## Specifying ODBC database paths

When you use ODBC connectivity using the JDBC-ODBC bridge (supported on Windows systems only) you can specify a database or file path the ODBC driver must use, if the ODBC driver permits. This type of configuration avoids having to define a data source name for each database or file path your Connector uses.

### jdbcDriver

`sun.jdbc.odbc.JdbcOdbcDriver`

### jdbcSource

`jdbc:odbc:driver name;DBQ=path`

The syntax of this parameter is dependent on the following:

#### MS Access is installed

Open the ODBC data source control panel, and select the **User DSN** tab. In this table you see the driver names you can use in the JDBC Source parameter. For example, if you want to access an MS Access database (C:\Documents and Settings\\My Documents\mydb.mdb), provide the following value for the JDBC source:

`jdbc:odbc:MS Access Database;dbq=C:\Documents and Settings\\My Documents\mydb.mdb`

#### MS Access is not installed

If MS Access is not installed, and you are on a Windows system, use the following:

`jdbc:odbc:Driver={MS Access Driver  
 (*.mdb)};dbq=C:\Documents and Settings\\My Documents\mydb.mdb`

Alternatively, use the Windows System DSN utility, available under Administrative Tools > Data Sources (ODBC). Once you define a System DSN, use a jdbcSource parameter like the following:

`jdbc:odbc:myDSNNameHere`

Check the Driver list that you get in the utility. Your JDBC URL must exactly match the wording found in this list.

## Configuration

The Connector needs the following parameters:

### JDBC URL

See documentation for your JDBC provider. Typical URL's for common RDBMS systems are:

*Table 4. JDBC URL examples*

| RDBMS   | Example connection URL  |
|---|---|
| IBM DB2 (using the DRDA driver)                                 | "jdbc:db2://hostname:port/dbname"   |
| Informix® Dynamic Server 10.0                                   | "jdbc:informix-sqli://hostname:port/dbname:informixserver=<Informix Server Name>"                                   |
| Oracle (using the "thin driver")                                | "jdbc:oracle:thin:@hostname:1521:SID", using "host:port:sid" syntax, TNSListener accepting connections on port 1521 |
| Microsoft SQL Server (using Microsoft's driver)                 | "jdbc:sqlserver://hostname:1433;datasource=dbname;", SQL Server listening for connections on port 1433              |
| Sybase 15 (also older versions from v. 10), using jConnect 6.05 | "jdbc:sybase:Tds:hostname:port/"  |

### JDBC Driver

The JDBC driver implementation class name. The default value of `sun.jdbc.odbc.JdbcOdbcDriver` addresses the JDBC-ODBC bridge, which is not recommended for production use. For databases for which another type of driver is available, typical driver implementation class names are:

*Table 5. Driver implementation class names*

| RDBMS                                      | Driver implementation class name                          |
|--|---|
| IBM DB2, type 2 or 4                       | <code>com.ibm.db2.jcc.DB2Driver</code>                    |
| Oracle, type 4                             | <code>oracle.jdbc.driver.OracleDriver</code>              |
| Informix Dynamic Server 10.0               | <code>com.informix.jdbc.IfxDriver</code>                  |
| Microsoft SQL Server, type 4               | <code>com.microsoft.sqlserver.jdbc.SQLServerDriver</code> |
| Sybase 15 (also older versions from v. 10) | <code>com.sybase.jdbc3.jdbc.SybDriver</code>              |

Also see "Understanding JDBC Drivers" on page 103.

### Username

Signon to the database using this username; only the tables accessible to this user will be shown.

### Password

The password used in the signon for the user.

### Schema

The schema from the table of the database that you want to use. If left blank, the value of the `jdbcLogin` (that is, the **Username** parameter) is used.

**Note:** Throughout the TDI documentation, you will find the term Schema used to mean the data definition of the object you are accessing. However, in the RDBMS world, the term Schema has a different meaning, namely the overall collection of data definitions, tables and objects grouped under one identifier (username). For this particular parameter in this particular Connector, we use it in the RDBMS sense.

### Table Name

The table or view to operate on. This is only used when the Connector operates in Lookup or

Update mode. If the **SQL Select** parameter is not specified, then the Iterator mode Connector also uses this parameter to construct a default SELECT statement.

#### Select...

Click this button to bring up a list of available table names that you can select from to enter into the **Table Name** field. This only works if the underlying database supports this; for example, Microsoft Access using ODBC does not.

#### Return null values

If this parameter is set to **true**, then NULL values are returned as empty attributes (for example, empty value set). If set to **false**, then the attribute is not part of the entry returned.

#### Commit

Controls when database transactions are committed. Options are:

- **After every database operation** (default)
- **After every database operation (Including Selects)**
- **On Connector close**
- **Manual**

**Manual** means user must call the *commit()* method of the JDBC Connector—or *rollback()*, as appropriate.

**Note:** The option **After every database operation (Including Selects)** has been provided for those databases which lock database tables in transactions even when they only have been Selected for read operations (notably DB2).

#### SQL Select

The select statement to execute when selecting entries for iteration, that is, Iterator mode. If you leave this blank, the default construct (SELECT \* FROM TABLE) is used.

#### SQL Lookup

The custom SQL statement to use for lookups (used in Lookup and Delete modes).

#### SQL Insert

The custom SQL statement to use when inserting into the database, using AddOnly mode.

#### SQL Update

The custom SQL statement to use when updating the database, using Update mode.

#### SQL Delete

The custom SQL statement to use when using Delete mode.

#### Alter Session Statements

This parameter is a multi-line field where you can specify ALTER SESSION commands. The following is an example of an ALTER SESSION command:

```
"SET NLS_FORMAT 'YYYY-MM-DD'"
```

#### Extra Provider Parameters

Additional JDBC provider parameters (name:value - one for each line). With this you can specify additional parameters supported by the JDBC provider. You should check your driver documentation for the supported parameters and then use them. For example, specific to DB2:

```
securityMechanism:KERBEROS_SECURITY  
loginTimeout:20  
readOnly:true
```

#### Date Format

A format string used to parse dates when they are supplied as strings. You can select from a list of pre-defined format strings, or supply your own.

#### Use Prepared Statements

This value of this check box determines whether to use PreparedStatement or Statement. If this is

selected the PreparedStatement will be used by the JDBC connector else Statement will be used. The default is checked, that is, "true", meaning try to pre-compile SQL statements, fall back to normal.

### Connector Flags

A list of flags to enable specific behavior.

*{ignoreFieldErrors}*

If getting field values causes an error, this flag causes the Connector to return the Java exception object as the value instead of throwing the exception (that is, calling the Connectors \*Fail EventHandlers).

### Detailed Log

If this field is checked, additional log messages are generated.

### Link Criteria configuration

Link criteria specified in the Connector's configuration for Lookup, Delete, Update and Delta modes are used to specify the WHERE clause in the SQL queries used to interact with the database.

The TDI operand **Equal** is translated to the equal sign ( = ) in the SQL query, while the **Contains**, **Start With** and **End With** operators are mapped to the **like** operator.

## Customizing select, insert, update and delete statements

### Overview

The JDBC connector has the ability to expand a SQL template before executing any of its SQL operations. There are five operations where the templates can be used. These operations are:

*Table 6. SQL Operations*

| Operation | Description  | Mode(s)                |
|-----------|--|------------------------|
| SELECT    | Used in Iterator mode (no search criteria).                                  | Iterator               |
| INSERT    | Used when adding an entry to the data source.                                | Update, AddOnly        |
| UPDATE    | Used when modifying an existing entry in the data source.                    | Update                 |
| DELETE    | Used when deleting an existing entry in the data source.                     | Delete                 |
| LOOKUP    | A SELECT statement with a WHERE clause. Used when searching the data source. | Lookup, Delete, Update |

If the template for a given operation is not defined (e.g., null or empty), the JDBC connector will use its own internal template.

When there is a template defined for an operation, the template must generate a complete and valid SQL statement. The template can reference the standard parameter substitution objects (e.g. mc, config, work, Connector), as well as the JDBC schema for the table configured for the connector and a few other convenience objects.

### Metadata Object

The information about JDBC field types is provided as an Entry object named metadata. Each attribute in the metadata Entry object corresponds to a field name and the value will be that field's corresponding type. For example, a table with the following definition:

```
CREATE TABLE SAMPLE (
  name varchar(255),
  age numeric(10),
)
```

could be referenced in the following manner, during parameter substitution:

```

{javascript<<EOF
    metadata = params.get("metadata");
    if (metadata.getAttribute("name").equals("varchar"))
    return "some sql statement";
    else
    return "some other sql statement";
EOF
}

```

## Link Object (Link Criteria)

The LinkCriteria values are available in the *link* object. The link object is an array of link criteria items. Each item has fields that define the link criteria according to configuration. If the configured link criteria is defined as *cn equals john doe* then the template could access this information with the following substitution expressions:

```

link[0].name ▶ "cn"
link[0].match ▶ "="
link[0].value ▶ "john doe"
link[0].negate ▶ false

```

A complete template for a SELECT operation could look like this:

```
SELECT * FROM {config.jdbcTable} WHERE {link[0].name} = '{link[0].value}'
```

## Convenience Objects

Generating the WHERE clause or the list of column names is not easy without resorting to JavaScript code. As a convenience, the JDBC Connector makes available the column names that would have been used in an UPDATE and INSERT statement as columns; this does not apply to SELECT and LOOKUP statements. This value is a comma-delimited list of column names. The textual WHERE clause is available as “whereClause” to simplify operations. Below is an example of how to use both:

```
SELECT {columns} from {config.jdbcTable} WHERE {whereClause}
```

e.g., *SELECT a,b,c from TABLE-A WHERE a > 1 AND b = 2*

Table 7. Information available for different statements

| Object      | SELECT | LOOKUP | INSERT | DELETE | UPDATE |
|-------------|--------|--------|--------|--------|--------|
| config      | yes    | yes    | yes    | yes    | yes    |
| Connector   | yes    | yes    | yes    | yes    | yes    |
| metadata    | no     | maybe  | maybe  | yes    | yes    |
| conn        | no     | no     | yes    | yes    | yes    |
| columns     | no     | no     | yes    | yes    | yes    |
| link        | no     | yes    | no     | yes    | yes    |
| whereClause | no     | yes    | no     | yes    | yes    |

## Additional JDBC Connector functions

Apart from the standard functions exposed by all Connectors, this Connector also exposes several other functions you can use in your scripts. You could call them using the special variable *thisConnector*, e.g. *thisConnector.commit()*; — when called from any scripting location in the Connector.

### commit()

Commits any pending database operations.

### execSQL (string)

Starts an arbitrary SQL command. Returns the error string if it fails.

### execSQLSelect (string)

Starts SQL SELECT command. Returns the error string if it fails.

### **getNextSQLSelectEntry ()**

Having started `execSQLSelect` you can use this method to get the next entry from the result set.

The Connector's **Table Name** parameter must be empty for this to work correctly.

### **rollback()**

Backs out any database operations performed since the last `commit()` (irrespective of whether the commit was done manually, or as a result of autocommit operations).

The above functions do not interfere with the normal flow of entries and attribute mappings for the Connector.

## **Timestamps**

If you want to store a timestamp value containing both a date and a time, you must make sure you provide an object of type `java.sql.Timestamp`, as you can with this Attribute Mapping:

```
ret.value = java.sql.Timestamp(java.util.Date().getTime());
```

The `java.sql.Timestamp` type can also come in handy if for some reason storing DATE fields in tables causes trouble, for example the Oracle error **ORA-01830: date format picture ends before converting entire input string**. Normally, if you try to store date/time values which are in the form of strings, the **Date Format** parameter comes into play to convert the string into the DATE type the underlying database expects, and if there is a mismatch between this parameter and your date/time value formatted as a string, problems will ensue.

To troubleshoot your problem:

- What is your Data Pattern configuration?
- Find out how TDI sees this field (check in the schema tab of the Connector). A fair guess is that your JDBC driver will convert the Oracle Data type into a `java.sql.TimeStamp` or `java.sql.Date` type (and note that there are differences between `java.util.Date` and `java.sql.Date`, in terms of precision amongst others). For example, in the case of a `java.sql.Timestamp` type, try specifying the construct mentioned above, that is

```
ret.value = java.sql.Timestamp(java.util.Date().getTime());
```

and see if this helps. If it does, then you will be able to use

```
ret.value = java.sql.Timestamp(system.parseDate(work.getString("yourDate"),  
"yyyyMMddHHmmssz").getTime());
```

- If none of the above helps, turn the Connector into detailed log mode and see whether the Connector is able to get the schema from the database. If not, the Connector does not use prepared statements which makes it less efficient and more error-prone - so you'll have to make sure that the Connector's **schema** configuration parameter is set correctly.

## **Calling Stored Procedures**

The JDBC Connector's "connection" property gives you access to the JDBC Connection object created when the connector has successfully initialized.

In other words, if your JDBC connector is named DBconn in your AL,

```
var con = DBconn.connector.connection;
```

will give you access to the JDBC Connection object (an instance of `java.sql.Connection`).

**Note:** When called from anywhere inside the connector itself, you can also use the `thisConnector` variable.

Here is a code example illustrating how you can invoke a stored procedure on that database:

```

// Stored procedure call
command = "{call DBName.dbo.spProcedureName(?,?)}";

try {
    cstmt = con.prepareStatement(command);

    // Assign IN parameters (use positional placement)
    cstmt.setString(1, "Christian");
    cstmt.setString(2, "Chateauvieux");

    cstmt.execute();

    cstmt.close();
    // TDI will close the connection, but you might want to force a close now.
    DBConn.close();
}

catch(e) {
    main.logmsg(e);
}

```

## SQL Databases: column names with special characters

If you have columns with special characters in their names and use the AddOnly or Update modes:

1. Go to the attribute map of the Update or AddOnly Connector
2. Rename the Connector attribute (not the work attribute!) from **name-with-dash** to **"name-with-dash"** (add quotes).

The necessity of using this functionality might be dependent on the JDBC driver you are using, but standard MS Access 2000 has this problem.

## Using prepared statements

This section describes how the Connector creates SQL queries. You can skip this section unless you are curious about the internals.

For a database, the Connector uses prepared statements or dynamic query depending on the situation:

- If the Connector gets the schema definition from the database, it uses prepared statements.
- Otherwise, the Connector creates a dynamic SQL query.

### Taking advantage of PreparedStatements

The JDBC connector uses *PreparedStatement* to efficiently execute an SQL statement on a connected RDBMS server. However, there may be cases when the JDBC driver may not support *PreparedStatement*. As a fall back mechanism a config parameter is available in the JDBC connector's configuration. The config parameter is a Boolean flag called `usePreparedStatement` (configured via a checkbox called **Use Prepared Statements** in the connector config screen) which indicates whether the JDBC connector should use *PreparedStatement*. If this is set (the default) the connector will use *PreparedStatement* and will fall back to normal *Statement* (`java.sql.Statement`) in case of an exception. If this is not set, normal *Statement* will be used by the JDBC connector while executing SQL queries. This checkbox gives an option to a TDI solution developer to handle situations when there are problems due to use of *PreparedStatement*.

The `findEntry`, `putEntry`, `deleteEntry` and the `modEntry` methods of the JDBC connector checks for the value of `usePreparedStatement` flag to determine whether to use *PreparedStatement* or *Statement*.

If a connector config does not have this flag (as in an older version of the config), the value of this param will be "true" by default. This ensures that there are no migration issues or impact.

## On Multiple Entries

See Appendix B, “AssemblyLine and Connector mode flowcharts,” on page 443 for more information about what happens when a Connector has a link criteria returning multiple entries.

For the JDBC Connector in Delete or Update mode, if you have used the `setCurrent()` method of the Connector and not added extra logic, all entries matching the link-criteria are deleted or updated.



---

## JMS Connector

### Introduction

The JMS Connector's functions and features are:

- Enables communication of native Entry objects to be passed using a Java Message Service product.
- Supports JMS message headers and properties.
- Supports sending different types of data on the JMS bus (text message, object message, bytes message).
- Allows users to write their own Java code (JMS initiator class) to connect to different JMS systems.
- Allows users to write JavaScript to connect to different JMS systems.
- Support for plugging in other message queues than IBM MQ.
- Supports auto acknowledge and manual acknowledge through the acknowledge() method.

The JMS Connector provides access to JMS based systems such as IBM MQ Server or the bundled MQE. A partly-preconfigured version of this Connector exists under the name "**IBM MQ Connector**", where the JMS Server Type is hidden, and pre-set to "IBMMQ".

Refer to Specific topics to see what you might need to do to your IBM Tivoli Directory Integrator installation to make the JMS Connector work.

The Connector enables communication of both native Entry objects and XML text to be passed using a Java Message Server product.

The JMS Connector supports JMS message properties. Each message received by the JMS Connector populates the `conn` object with properties from the JMS message (see the `getProperty()` and `setProperty()` methods of the entry class to access these). `conn` object properties are prefixed with `jms.` followed by the JMS message property name. The property holds the value from the JMS message. When sending a message the user can set properties which are then passed on to the JMS message sent. The JMS Connector scans the `conn` object for properties that starts with `jms.` and set the corresponding JMS message property from the `conn` property.

- JMS: correlationID=12 —> `conn.jms.correlationID=12`
- `conn:jms.inReplyTo=12` —> JMS:inReplyTo=12

The `conn` object is only available in a few hooks. See "Conn object" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.

### JMS message flow

Everything sent and received by the JMS Connector is a JMS message. The JMS Connector converts the IBM Tivoli Directory Integrator Entry object into a JMS message and vice versa. Each JMS message contains predefined JMS headers, user defined properties and some kind of body that is either text, a byte array or a serialized Java object.

There exists a method as part of the JMS Connector which can greatly facilitate communication with the JMS bus: `acknowledge()`. The method `acknowledge()` is used to explicitly acknowledge all the JMS session's consumed messages when **Auto Acknowledge** is unchecked. By invoking `acknowledge()` of the Connector, the Connector acknowledges all messages consumed by the session to which the message was delivered. Calls to `acknowledge` are ignored when **Auto Acknowledge** is checked.

When deploying the JMS Connector in conjunction with the Checkpoint/Restart functionality available with IBM Tivoli Directory Integrator, careful thought must be given to the acknowledgement of received messages (see "Checkpoint/Restart — Saving and storing AssemblyLine state information" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*). As described, the best approach is to not use **Auto Acknowledge** in the JMS Connector, but rather insert a Script Connector right after the JMS Connector in the

AssemblyLine, invoking the `acknowledge()` method of the JMS Connector. This ensures that the window between the relevant message information in the Checkpoint/Restart store being saved, and the JMS queue notification is as small as possible. If a failure occurs in this window, the message is received once more.

Conversely, relying on **Auto Acknowledge** creates a window that exists from the point at which the message is retrieved from the queue (and acknowledged), until the message contents mapped into the entry is secured in the Checkpoint/Restart store. If a failure occurs in this window, the message is lost, which can be a greater problem.

**Note:** There could be a problem when configuring the JMS Connector in the Config Editor when **Auto Acknowledge** is on, because as long as this is the case, when going through the process of schema discovery using either **Schema->Connect->GetNext** or Quick Discover from Input Map the message will be grabbed and consumed (that is, gone from the input queue). This may be an unintended side-effect. To avoid this, turn **Auto Acknowledge** off before Schema detection — but remember to switch it back on again afterwards, if this is the desired behavior

## WebSphere MQ and JMS/non-JMS consumers of messages

When the JMS Connector sends messages to WebSphere MQ it is capable of sending these messages in two different modes depending on the client which will read these messages:

- the messages are intended to be read by non-JMS clients (the default)
- the messages are intended to be read by JMS clients

By default the Connector sends the messages so that they are intended to be read by non-JMS clients. The major difference between these two modes is that when the messages are intended to be read by non-JMS clients, the JMS properties are ignored. Thus a subsequent lookup on these properties will not find a match.

In order to switch to the "intended to be read by JMS clients" mode, the "Specific Driver Attributes" parameter value must contain the following line (apart from any other attributes specified):  
`mq_nonjms=false`

## JMS message types

The JMS environment that enables you to send different types of data on the JMS bus. This Connector recognizes three of those types. The three types are referred to as Text Message, Bytes Message and Object Message. The most open-minded strategy is to use Text Message (for example, `jms.usetextmessages=true`) so that applications other than IBM Tivoli Directory Integrator can read messages generated by the JMS Connector.

When you communicate with other IBM Tivoli Directory Integrator servers over a JMS bus the BytesMessage provides a very simple way to send an entire Entry object to the recipient. This is also particularly useful when the entry object contains special Java objects that are not easy to represent as text. Most Java objects provide a `toString()` method that returns the string representation of it but the opposite is very rare. Also, the `toString()` method does not always return very useful information. For example, the following is a string representation of a byte array:

```
"[B@<memory-address>"
```

## Text message

A text message carries a body of text. The format of the text itself is undefined so it can be virtually anything. When you send or receive messages of this type the Connector does one of two things depending on whether you have specified a Parser:

- When you specify a Parser the Connector calls the Parser to interpret the text message and return these attributes along with any headers and properties. When sending a message the provided **conn** object is passed to the Parser to generate the text body part. This makes it easy to send data in various formats

onto a JMS bus (for example, use the LDIF Parser, XML Parser, and so forth). You can even use the Simple Object Access Protocol (SOAP) Parser to send SOAP requests over the JMS bus.

- If you don't have a Parser defined, the text body is returned in an attribute called message. When sending a message the Connector uses the provided message attribute to set the JMS text body part.

```
var str = work.getString ("message");
task.logmsg ("Received the following text: " + str );
```

If you expect to receive text messages in various formats (XML, LDIF, CSV ...) you must leave the Parser parameter blank and make the guess yourself as to what format the text message is. When you know the format you can use the `system.parseObject(parserName, data)` syntax to do the parsing for you:

```
var str = work.getString ("message");
// code to determine format
if ( isLDIF )
    e = system.parseObject( "ibmdi.LDIF", str );
else if ( isCSV )
    e = system.parseObject ( "ibmdi.CSV", str );
else
    e = system.parseObject ( "ibmdi.XML", str );
}
// Dump parsed entry to logfile
task.dumpEntry ( e );
```

The **Use Textmessage** flag determines whether the Connector must use this method when sending a message.

## Object message

An object message is a message containing a serialized Java object. A serialized Java object is a Java object that has been converted into a byte stream in a specific format which makes it possible for the receiver to resurrect the object at the other end. Testing shows that this is fine as long as the Java class libraries are available to the JMS server in both ends. Typically, a `java.lang.String` object causes no problems but other Java objects might. For this reason, the JMS Connector does not generate object messages but is able to receive them. When you receive an object message the Connector returns two attributes:

### java.object

This attribute holds the java object and you must access the object using the `getObject` method in your **workor conn** entry.

### java.objectClass

This attribute is a convenience attribute and holds the class name (String) of the Java object

```
var obj = work.getObject ("java.object");
obj.anyMethodDefinedForTheObject ();
```

You only receive these messages.

## Bytes message

A bytes message is a message carrying an arbitrary array of bytes. The JMS Connector generates this type of message when the **Use Textmessage** flag is **false**. The Connector takes the provided entry and serializes it into a byte array and send the message as a bytes message. When receiving a bytes message, the Connector first attempts to deserialize the byte array into an Entry object. If that fails, the byte array is returned in the message attribute. You must access the byte array using the `getObject` method in your **work** or **conn** entry.

```
var ba = work.getObject ("message");
for ( i = 0; i < ba.length; i++)
    task.logmsg ( "Next byte: " + ba [ i ] );
```

This type of message is generated only if **Use Textmessage** is **false** (not checked).

## Iterator mode

A message selector is a String that contains an expression. The syntax of the expression is based on a subset of the SQL92 conditional expression syntax. The message selector in the following example selects any message that has a NewsType property that is set to the value 'Sports' or 'Opinion':

```
NewsType = 'Sports' OR NewsType = 'Opinion'
```

## Lookup mode

The Connector supports Lookup mode where the user can search for matching messages in a JMS Queue (Topic (Pub/Sub) is not supported by Lookup mode).

The Link Criteria specifies the JMS headers and properties for selecting matching messages on a queue.

For the advanced link criteria you must conform to the Message Selection specification as described in the JMS specification (<http://java.sun.com/products/jms>). The JMS Connector reuses the SQL filter specification (JMS message selection is a subset of SQL92) to build the message selection string. Turn on debug mode to view the generated message filter string.

There are basically two ways to perform a Lookup:

- Do a non-destructive search in a Queue (using **QueueBrowser**) which returns matching messages without removing the messages from the JMS queue.
- Removes all matching entries from the JMS queue.

Decide which to use by setting the **Lookup Removes** flag in the Connector configuration. For Topic connections the **Lookup Removes** flag does not apply as messages on topics are always removed when a subscriber receives it. However, the Lookup mode heeds the **Durable Subscriber** flag in which case the JMS server holds any messages sent on a topic when you are disconnected.

The JMS Connector works in the same way as other Connectors in that you can specify a maximum number of entries to return in your AssemblyLine settings. To ensure you retrieve a single message only during Lookup, specify **Max duplicate entries returned = 1** in the AssemblyLine settings. Setting **Max duplicate entries returned** to 1 enables you to retrieve one matching entry at a time regardless of the number of matching messages in the JMS queue.

Since the JMS bus is asynchronous the JMS Connector provides parameters to determine when the Lookup must stop looking for messages. There are two parameters that tells the Connector how many times it queries the JMS queue and for how long it waits for new messages during the query. Specifying **10** for the retry count and **1000** for the timeout causes the Connector to query the JMS queue ten times each waiting 1 second for new messages. If no messages are received during this interval the Connector returns. If during a query the Connector receives a message, it continues to check for additional messages (this time without any timeout) until the queue returns no more messages or until the received message count reaches the **Max duplicate entries returned** limit defined by the AssemblyLine. The effect of this is that a Lookup operation only retrieves those messages that are available at the moment.

## Add Only mode

In this mode, on each AssemblyLine iteration the JMS Connector sends an entry to the JMS server. If a Topic is used the message is published and if a Queue is used the message is queued.

## Call/Reply mode

In this mode the Connector has two attribute maps, both **Input** and **Output**. When the AssemblyLine invokes the Connector, an Output map operation is performed, followed by an Input map operation. There is a method in the JMS Connector called `queryReply()` which uses the class `QueueRequestor`. The `QueueRequestor` constructor is given a non-transacted `QueueSession` and a destination Queue. It creates a `TemporaryQueue` for the responses and provides a `request()` method that sends the request message and waits for its reply.

## JMS headers and properties

A JMS message consists of headers, properties and the body. Headers are accessed differently than properties and were not available in previous versions. In this version you can specify how to deal with headers and properties.

### JMS headers

JMS headers are predefined named values that are present in all messages (although the value might be null). The following is a list of JMS header names this Connector supports:

#### JMSCorrelationID

(String) This header is set by the application for use by other applications.

#### JMSDeliveryMode

(Integer) This header is set by the JMS provider and denotes the delivery mode.

#### JMSExpires

(Long) A value of zero means that the message does not expire. Any other value denotes the expiration time for when the message is removed from the queue.

#### JMSMessageID

(String) The unique message ID. Note that this is not a required field and can be null.

Since the JMS provider might not use your provided message ID, the Connector sets a special property called `$jms.messageid` after sending a message. This is to insure that the message ID always is available to the user. To retrieve this value use `conn.getProperty("$jms.messageid")` in your **After Add** hook.

#### JMSPriority

(Integer) The priority of the message.

#### JMSTimestamp

(Long) The time the message was sent.

#### JMSType

(String) The type of message.

#### JMSReplyTo

(Destination) The queue/topic the sender expects replies to. When receiving a message this value holds the provider specific Destination interface object and is typically an internal Queue or Topic object. When sending a message you must either reuse the incoming Destination object or set the value to a valid topic/queue name. If the value is **NULL** (for example, an attribute with no values) or the string `"%this%"` the Connector uses its own queue/topic as the value. The difference between this method and explicitly setting the queue/topic name is that you need not update the attribute assignment if you change your Connector configuration's queue/topic name.

There is one restriction in the current version which enables you to only request a reply to the same type of connection as you are currently connected to. This means that you cannot publish a message on a topic and request the reply to a queue and vice versa.

It is not mandatory to respond to this header so the receiver of the message can completely ignore this field without any form of punishment.

These headers are all set by the provider and might be acted upon by the JMS driver for outgoing messages. In the configuration screen you can specify that you want all headers returned as attributes or specify a list of those of interest. All headers are named using a prefix of **jms..** Also note that JMS header names always start with the string **JMS**. This means that you must never use property names starting with **jms.JMS** as they can be interpreted as headers.

## JMS properties

In previous versions of this Connector all JMS properties were copied between the Entry object and the JMS Message. In this release you can refine this behavior by telling the Connector to return all user defined properties as attributes or specify a list of properties of interest. All properties are prefixed with **jms.** to separate them from other attributes. If you leave the list of properties blank and uncheck the **JMS Properties As Attributes** flag, you get the same behavior as for previous versions. Both JMS headers and JMS properties can be set by the user. If you use the backwards compatible mode you must set the entry properties in the **Before Add** hook as in:

```
conn.setProperty ( "jms.MyProperty", "Some Value" );
```

If you either check the **JMS Properties As Attributes** flag or specify a list of properties, you must provide the JMS properties as attributes. One way to do that is to add attributes using the **jms.** prefix in your attribute map. For example, if you add **jms.MyProperty** attribute map it results in a JMS property named **MyProperty**.

## Configuration

The Connector name is JMS Pub/Sub Connector, and it needs the following parameters:

### Broker

The URL for the JMS server. When working with IPv6 addresses, this parameter must contain both the IPv6 JMS Server address as well as the JMS Server port.

**Note:** The JMS Connector will support the IPv6 protocol if the JMS Server you connect to supports IPv6. IBM MQSeries® 5.3 does not.

### Server Channel

The name of the channel configured for the MQ server.

### Use SSL Connection

Enables use of parameters and configuration settings required for SSL connection.

### SSL Server Channel

The name of channel configured for using SSL to access the MQ server.

### Queue Manager

The name of Queue Manager defined for MQ server or INITIAL\_CONTEXT\_FACTORY for non-IBM MQ.

### SSL CipherSuite

Cipher Suite name which corresponds to cipher selected in configuring MQ server channel. This parameter only applies when the JMS Connector is used with IBM WebSphere MQ Server. This parameter is left in the configuration for backward compatibility.

### User Name

User name for authenticating access to the JMS.

### Password

Password for authenticating access to the JMS.

### Connection Type

Specify whether you are connecting to a **Queue** or **Topic** (Topic is sometimes called **Pub/Sub** for Publish/Subscribe).

### Topic/Queue

The topic/queue with which messages are exchanged.

### Durable Topic Subscriber

Only relevant for **Connection Type Topic** (Pub/Sub). If **true**, this causes the Connector to create a durable subscriber. This means that the server stores messages for a topic for later retrieval when the Connector is offline.

**Client ID**

The client ID to use for Topic connections (mandatory for durable).

**Message Selection Filter**

Specifies a message filter for selection of messages from a Topic/Queue. Used in Iterator mode only.

**GetNext Timeout**

Time (in milliseconds) to wait for a new entry in Iterator mode. **-1 == forever**

**JMS Server Type**

Select the JMS server type.

**Specific Driver Attributes**

These take the form of *name=value* driver attributes. For example:

```
QUEUE_FACTORY_NAME=primaryQCF, or  
TOPIC_FACTORY_NAME=primaryTCF
```

**JMS Driver Script**

This parameter contains Javascript code to be used for initialization of the JMS provider-specific objects. The contents of this parameter are passed to the configured JMS Driver using the "jsscript" Hashtable key name. This parameter is intended to be used by the JMS Script Driver, which executes the contents of this parameter as Javascript. This "jsscript" name is used as a key in the Hashtable passed to the JMS Script Driver. If the MQE or the MQ driver is configured to be used with the JMS Connector, then the contents of this parameter will be ignored. If a 3rd party JMS Driver different from the JMS Script Driver is configured the contents of this parameter will most likely be ignored.

For more details on the structure of this parameter's Javascript code as well as on the environment in which it executes, please see the section labeled "JMS Script driver" in the section about the System Queue in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide* and the "System Queue Connector" on page 171.

**Auto Acknowledge**

If **true**, each message is automatically acknowledged by this Connector. If **false**, you must manually acknowledge the receipt of a JMS message (by means of the Connector's `acknowledge()` method). If **off**, use the JMS CLIENT\_ACKNOWLEDGE mode.

**Use Textmessage**

If **true**, the Connector produces a Textmessage and sends the Entry object either by using the specified Parser to generate the text body or using the predefined message attribute as the text body.

**JMS Headers as attributes**

If **true**, all JMS headers are returned as attributes (prefixed by **jms.**) in Iterator and Lookup modes. For AddOnly mode, any attribute starting with **jms.JMS** is treated as JMS header. This causes these attributes to be set as JMS headers and removed from the Entry object before sending the message.

**Note:** only a few headers can be set, and setting them does not mean the JMS provider ever uses them.

**Specific JMS Headers**

Same as **JMS Headers as attributes**, but only the listed JMS headers are treated as headers. Specify one header per line.

**JMS Properties as attributes**

If **true**, all JMS properties are returned as attributes (prefixed by **jms.**) in Iterator and Lookup modes. For AddOnly mode, any attribute starting with **jms.** is treated as a JMS property. This causes these attributes to be set as JMS properties.

### Specific JMS Properties

Same as **JMS Properties as attributes** , but only the listed JMS properties are treated as properties. Specify one property per line.

### Lookup Removes

If **true**, each message found during Lookup is removed from the queue.

**Note:** You can set the **Max duplicate entries returned** parameter in your AssemblyLine Configuration settings to prevent Lookup from returning more than one entry.  
If **false**, messages are returned as usual, but they are not removed from the queue.

### Lookup Retries

The number of times Lookup searches the queue for matching messages.

### Lookup Timeout

Time (in milliseconds) the Connector waits for new messages during a Lookup query. This parameter is used when **Lookup Removes** is set to **true** only.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

A Parser can be selected from the **Parser...** pane; once in this pane, choose a parser by clicking the bottom-right Inheritance button. If a Parser is specified, a JMS Text message is parsed using this Parser. This Parser works with messages that are received by the JMS Connector, and is used to generate a text message when JMS Connector sends a message.

## Examples

Go to the *root\_directory/examples/jms* directory of your IBM Tivoli Directory Integrator installation.

TDI 6.1.1 comes with an example of a JMS script driver for Sonic MQ. This sample demonstrates how the TDI JMS components (JMS Connector, System Queue) can use the SonicMQ server as a JMS provider.

## External System Configuration

The configuration of external JMS systems which this Connector accesses is not specific to this Connector. Any external JMS system which this Connector accesses must be configured as it would be configured for any other JMS client.

### IBM WebSphere MQ

WebSphere MQ: When IBM WebSphere MQ is used as a JMS provider the following *jar* files have to be taken from the WebSphere MQ installation, and placed under the "`<tdi_root_folder>\jars\3rdparty\IBM>`" folder:

- `com.ibm.mqjms.jar` (this will replace an existing file)
- `com.ibm.mq.jar`
- `jms.jar`
- `connector.jar`

In order to enable a Secure Socket Layer (SSL) session, you must first configure a channel on your MQ server. Detailed instructions on how to perform these tasks are included in a Technical Journal Article, "Configuring SSL Connections between JMS Clients and the WebSphere MQ JMS Provider", [http://www7b.software.ibm.com/wsdd/techjournal/0211\\_yusuf/yusuf.html](http://www7b.software.ibm.com/wsdd/techjournal/0211_yusuf/yusuf.html), Dr Kareem Yusef, November 2002. This article also provides detailed instructions on obtaining and managing certificates required to run an SSL test. The version of IBM WebSphere MQ should be at least v5.3 service level 5.3.0.4 (i.e, fix pack CSD04 installed prior to attempting SSL configurations. In the TDI Properties store, specify the `trustStore` and `keyStore` settings prior to starting IBM Tivoli Directory Integrator. For example:



```
javax.net.ssl.trustStore=d:\\jdk141\\jre\\lib\\security\\cacerts
javax.net.ssl.trustStorePassword=
javax.net.ssl.trustStoreType=
```

```
javax.net.ssl.keyStore=C:\\Program Files\\IBM\\WebSphere MQ\\Java\\bin\\jmskeystore
javax.net.ssl.keyStorePassword=changeit
javax.net.ssl.keyStoreType=jks
```

### **IBM WebSphere MQ Everyplace**

When the bundled IBM WebSphere MQ Everyplace is used as a JMS provider, no additional *jar* file copying is needed after TDI is installed.



---

## JMX Connector

The JMX Connector uses the JMX 1.2 and JMX Remote API 1.0 specifications. It only uses standard JMX features.

The JMX Connector can listen to, and report, either local or remote JMX notifications, depending on how it is configured.

When the `AssemblyLine` starts the JMX Connector is initialized. On initialization, the Connector determines whether it will report local or remote notifications based on the Connector parameters (the Connector cannot report both local and remote notifications in a single run). Then, the Connector gets either a local or a remote reference to the respective MBean Server and registers for the desired JMX notifications specified in a Connector parameter.

In the `getNextEntry()` method, the Connector blocks the `AssemblyLine` while waiting for notifications. When a notification is received, the `getNextEntry()` method of the Connector returns an `Entry` (which contains the notification details) to the `AssemblyLine`.

Notifications that are received between successive `getNextEntry()` calls are buffered, so that no notifications are lost. If there are buffered notifications when the `getNextEntry()` is called, then the Connector returns the first buffered notification immediately without blocking the `AssemblyLine`.

This Connector operates in Iterator mode only.

## Connector Schema

The JMX Connector makes the following Attributes available (Input Attribute Map):

### **event.originator**

The JMX Connector object of type `com.ibm.di.connector.JMXConnector`

### **event.type**

The notification type of type `java.lang.String`

### **event.rawNotification**

The raw JMX Notification instance received by the JMX Connector (`javax.management.Notification`). If the component that broadcasts this notification has extended `javax.management.Notification` and has put some additional data in the subclass, this extra information can be retrieved through this property.

### **event.timestamp**

The notification timestamp of type `java.lang.Long`. It represents the moment when the notification was created.

### **event.sequenceNumber**

The notification sequence number (`java.lang.Long`). It represents the notification sequence number within the source object. It's a serial number identifying a particular instance of notification in the context of the notification source. The notification model does not assume that notifications will be received in the same order that they are sent. The sequence number can be used to sort received notifications.

### **event.message**

The message of the notification (`java.lang.String`).

### **event.mbean.objectName**

The object name of the registered and unregistered MBean (`javax.management.ObjectName`). This property is only available if the `event.type` is `JMX.mbean.registered` or `JMX.mbean.unregistered`. `ObjectName` represents an MBean Name (as well as a wildcard for MBean Names). The entire combination of the domain plus all keys and values must be unique. (That is equivalent to saying that the entire MBean Name must be unique).

**event.mbean.name**

The string representation of the MBean object name (`java.lang.String`). This property is only available if the `event.type` is `JMX.mbean.registered` or `JMX.mbean.unregisterd`.

**event.userData**

The JMX notification user data (`java.lang.Object`).

**event.source**

The MBean object name on which the notification initially occurred (`javax.management.ObjectName`).

## Configuration

**Mode** This parameter determines whether the JMX Connector will listen for local or remote JMX notifications. The Connector registers for and listens to remote JMX notifications according to the JMX Remote API 1.0 specification.

The available values (drop-down list) for this parameter are *remote* and *local*.

The value “local” means that the Connector will only listen for notifications issued by MBeans registered with an MBeanServer in the local Java Virtual Machine.

The value “remote” means that the Connector will connect to a remote JMX system based on the JMX Remote API 1.0 specification, and register for notifications issued by MBeans registered with an MBean server in the Java Virtual Machine of that remote system.

**Remote JMX URL**

This parameter is only taken into account if the “mode” parameter is set to “remote”. This is the JMX URL used to connect to the remote JMX system. More precisely, this URL is specified by the remote MBean Server on its startup and is used by remote clients to connect to it.

An example value for this parameter would be: “service:jmx:rmi://localhost/jndi/rmi://localhost:1099/jmxconnector”

The default value is “service:jmx:rmi://localhost/jndi/jmx”

**Listen to all MBeans**

Specifies whether the Connector will register with all available MBeans (checked) or only with the ones specified in the **MBeans to listen to** Connector parameter (unchecked). This parameter is checked by default.

**MBeans to listen to**

Specifies a list of MBean object names, each typed on a separate line. This list specifies the MBeans with which the Connector will register for notifications. If no MBean object names are specified (that is, the list is empty) notifications issued by any MBean will be reported. If at least one MBean name is specified, then only notifications issued from the MBeans specified will be reported.

**Notification types**

The type of a JMX notification, not to be confused with its Java class, is the characterization of a generic notification object. The type is assigned by the broadcaster object and conveys the semantic meaning of a particular notification. The type is given as a String field of the Notification object. This string is interpreted as any number of dot-separated components, allowing an arbitrary, user-defined structure in the naming of notification types.

Specifies the types of JMX notifications which the JMX Connector will listen to. Notifications whose types are not specified will not be reported by the Connector. Each notification type must be typed on a separate line.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

The JMX Connector is capable of using the SSL protocol on the connection. If the remote JMX system accepts only SSL connections, the JMX Connector will automatically establish an SSL connection provided that a trust store is configured properly. This means that appropriate values have to be set for the `javax.net.ssl.trustStore`, `javax.net.ssl.trustStorePassword` and `javax.net.ssl.trustStoreType` properties in `global.properties` or `solution.properties`.



---

## JNDI Connector

The JNDI Connector provides access to a variety of JNDI services. To reach a specific system, you must install the JNDI driver for that system. The driver is typically distributed as one or more jar or zip files. Place these file in a place where the Java runtime can reach them, for example, in the <TDI\_install>/lib/ext directory.

This Connector supports Delta Tagging at the Attribute level. This means that provided a previous Connector in the AssemblyLine has provided Delta information at the Attribute level, the JNDI Connector will be able to use it in order to make the changes needed in the target JNDI directory.

When using the JNDI Connector for querying an LDAP Server, a *SizeLimitExceededException* may occur if the number of entries satisfying the search criteria is greater than the maximum limit set by the LDAP Server. To work around this situation, either increase the LDAP Server's maximum result limit, or set the `java.naming.batchsize` provider parameter to some value smaller than the maximum limit of the server. For more information on the `java.naming.batchsize` parameter refer to: <http://java.sun.com/products/jndi/tutorial/ldap/search/batch.html>

## Configuration

The Connector needs the following parameters:

### JNDI Driver

The class name (the JNDI Naming factory) for the JNDI driver.

### Provider URL

The URL for the connection, e.g. `ldap://host` for the LDAP driver.

### Authentication Method

The type of JNDI authentication to be used; choose from the drop-down list. Choices are:

- **Anonymous** (use no authentication)
- **Simple** (use weak authentication (cleartext password))
- **CRAM-MD5** (use CRAM-MD5 (RFC-2195))
- **SASL** (use SASL)

### Login username

The principal name (for example, `username`).

### Login password

The credentials (for example, `password`).

### Use SSL

Uses secure sockets layer for communication with LDAP server.

### Name parameter

Specify which parameter in the AssemblyLine entry is used for naming the entry. This is used during add, modify and delete operations and returned during read or search operations. If not specified, `$DN` is used.

### Search Base

The search base used when iterating the directory. Specify a distinguished name. Some directories enable you to specify a blank string which defaults to whatever the server is configured to do. Other directory services require this to be a valid distinguished name in the directory.

### Search Filter

The search filter to be used when iterating the directory.

### Search Scope

The search scope to be used when iterating the data source. Possible values are:

**subtree**

Return entries on all levels from search base and below.

**onelevel**

Only return entries that are immediately below searchbase.

**Referrals**

Specifies how referrals encountered by the LDAP server are to be processed. The possible values are:

- **follow** – Follow referrals automatically.
- **ignore** – Ignore referrals.
- **throw** – Throw a ReferralException when a referral is encountered. You need to handle this in an error Hook.

**Provider Params**

A list of extra provider parameters you want to pass to the provider. Specify each *parameter:value* on a separate line. For example:

```
java.naming.batchsize=100
```

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

## Setting the Modify operation

The JNDI connector has a way to set a **modify operation** value when the connector is in Modify mode. You can also use the simple connector interface to directly add, remove or replace attribute values and attributes instead of setting **modify operation**.

There is no Config Editor provided to set the **modify operation**. You must manually add the operation value to each attribute in the work entry of the JNDI connector in Modify mode using the following interface:

**di.com.ibm.di.entry.Attribute.setOper(char operation) operation****di.com.ibm.di.entry.Attribute.ATTRIBUTE\_DELETE**

This constant deletes the specified attribute values from the attribute.

The resulting attribute has the set difference of its prior value set and the specified value set. If no values are specified, it deletes the entire attribute. If the attribute does not exist, or if some or all members of the specified value set do not exist, this absence might be ignored and the operation succeeds, or an Exception might be thrown to indicate the absence. Removal of the last value might remove the attribute if the attribute is required to have at least one value.

**di.com.ibm.di.entry.Attribute.ATTRIBUTE\_REPLACE**

This constant replaces an attribute with specified values.

If the attribute already exists, this constant replaces all existing values with new specified values. If the attribute does not exist, this constant creates it. If no value is specified, this constant deletes all the values of the attribute. Removal of the last value might remove the attribute if the attribute is required to have at least one value. This is the default modify operation.

**di.com.ibm.di.entry.Attribute.ATTRIBUTE\_ADD**

This constant adds an attribute with the specified values.

If the attribute does not exist, this constant creates the attribute. The resulting attribute has a union of the specified value set and the prior value set.



## Calling the Modify Interface

### Adding a value to an attribute:

```
public void addAttributeValue(String moddn, String modattr, String modval)
```

throws Exception where:

- *moddn* is the DN to which you want to add the attribute value
- *modattr* is the name of the attribute to which you want to add a value
- *modval* is the value you want to add to *modattr*

For example, if you want to add "cn=bob" to the **members** attribute of "cn=mygroup" you use the method as such:

```
thisConnector.connector.addAttributeValue("cn=mygroup","members","cn=bob");
```

An Exception is thrown when the underlying modify operation fails.

### Replacing the attribute value:

```
public void replaceAttributeValue(String moddn, String modattr, String modval)
```

throws Exception where:

- *moddn* is the DN to which you want to add the attribute value
- *modattr* is the name of the attribute to which you wish to add a value
- *modval* is the value you want to add to *modattr*

For example, if you want to replace the **members** attribute of "cn=mygroup" with "cn=bob" only, you use the method as such:

```
thisConnector.connector.replaceAttributeValue("cn=mygroup","members","cn=bob");
```

An Exception is thrown when the underlying modify operation fails.

### Removing attribute:

```
public void removeAttribute(String moddn, String modattr)
```

throws Exception where:

- *moddn* is the DN from which you want to remove all attribute values
- *modattr* is the attribute name for which you want to remove all values

For example, if you want to remove the **members** attribute of "cn=mygroup" you use the method as such:

```
thisConnector.connector.removeAttribute("cn=mygroup","members");
```

An Exception is thrown when the underlying modify operation fails.

### Removing a certain attribute value from an attribute:

```
public void removeAttributeValue(String moddn, String modattr, String modval)
```

throws Exception where:

- *moddn* is the DN from which you want to remove the attribute value
- *modattr* is the attribute name that you want to change
- *modval* is the value you want to remove from given attribute

An Exception is thrown when the underlying modify operation fails.

## modify operation

**modify operation** can be set per Modify request. It causes **modify operation** for all attributes in the modify request entry to be set to the proper modify operation value. Property values and matching modify operation values:

| Property value (String) | modify operation value                              |
|-------------------------|---|
| delete                  | di.com.ibm.di.entry.Attribute.<br>ATTRIBUTE_DELETE  |
| add                     | di.com.ibm.di.entry.Attribute.<br>ATTRIBUTE_ADD     |
| replace                 | di.com.ibm.di.entry.Attribute.<br>ATTRIBUTE_REPLACE |

This property can be set at any time while the Connector is running by setting the property **modOperation** from the scripts:

```
conn.setProperty("modOperation","delete");
```

**Note:** This property does not affect the behavior of the any interfaces defined above. However, it does overwrite the existing **modify operation** set by `di.com.ibm.di.entry.Attribute.setOper(char operation)`

## See also

“LDAP Connector” on page 133,  
“MQe Initialization” on page 173.

---

## LDAP Connector

The LDAP Connector provides access to a variety of LDAP-based systems. The Connector supports both LDAP version 2 and 3. It is built layered on top of JNDI connectivity.

This Connector can be used in conjunction with the IBM Password Synchronization plug-ins. For more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.

Note that, unlike most Connectors, while inserting an object into an LDAP directory, you must specify the object class attribute, the **\$dn** attribute as well as other attributes. The following code example, if inserted in the Prolog, defines an **objectClass** attribute that you can use later.

```
// This variable used to set the object class attribute
var objectClass = system.newAttribute ("objectclass");
objectClass.addValue ("top");
objectClass.addValue ("person");
objectClass.addValue ("inetorgperson");
objectClass.addValue ("organizationalPerson");
```

Then your LDAP Connectors can have an attribute called **objectclass** with the following assignment:

```
ret.value = objectClass
```

To see what kind of attributes the **person** class has, see [java.sun.com/products/jndi/tutorial/ldap/schema/object.html](http://java.sun.com/products/jndi/tutorial/ldap/schema/object.html)

You see that you must supply an **sn** and **cn** attribute in your Update or Add Connector.

In the LDAP Connector, you also need the **\$dn** attribute that corresponds to the distinguished name. When building **\$dn** in the Attribute Map, assuming an attribute in the work object called **iuid**, you typically have code like the following:

```
var tuid = work.getString("iuid");
ret.value = "uid= " + tuid + ",ou=people,o=example_name.com";
```

### Notes:

1. The two special attributes, **\$dn** and **objectclass** usually are not included in Modification in Update mode unless you want to move entries in addition to updating them.
2. If you cannot connect to your directory, make sure the **Use SSL** flag in the Configuration is set according to what the directory expects.
3. When doing a Lookup, you can use **\$dn** as the Connector attribute, to look up using the distinguished name. Do not specify a Simple Link Criteria using both **\$dn** and other attributes; in this case a simple lookup will be done with the DN using an Equals comparison.
4. Certain servers have a size limit parameter to stop you from selecting all their data. This can be a nuisance as your Iterator only returns the first *n* entries. Some servers, for example, Netscape/iPlanet, enable you to exceed the size limit if you are authenticated as a manager.
5. Those servers that return their whole directory in one go (for example, non-paged search) typically cause memory problems on the client side. See "Handling memory problems in the LDAP Connector" on page 137.
6. When **Connector Flags** contains the value **deleteEmptyStrings**, then for each attribute, the LDAP Connector removes empty string values. This possibly leaves the attribute with no values (for example, empty value set). If an attribute has an empty value set then a modify operation deletes the attribute from the entry in the directory. An add operation never includes an empty attribute since this is not permitted. Otherwise, modify entry replaces the attribute values.
7. When **Connector Flags** does not contain **deleteEmptyStrings**, then empty strings are passed as permitted values to the directory server. Most servers interpret a REPLACE request with an empty

string the same as removing the attribute altogether. If you want to control this behavior, you can call a function in your **Before Update** hook to modify the entry as in:

```
removeBlanks (work);  
function removeBlanks (entry) {  
  var list = entry.getAttributeNames();  
  for (i = 0; i < list.length; i++) {  
    if (entry.getString(list[i]) == "") {  
      entry.removeAttribute (list[i]);  
    }  
  }  
}
```

## Configuration

The Connector needs the following parameters:

### LDAP URL

The LDAP URL for the connection (`ldap://host:port`).

### Login username

The distinguished name used for authentication to the server.

### Login password

The credentials (password).

### Search Base

The search base to be used when iterating the directory. Specify a distinguished name. Some directories enable you to specify a blank string which defaults to whatever the server is configured to do. Other directory services require this to be a valid distinguished name in the directory.

### Search Filter

The search filter to be used when iterating the directory.

### Search Scope

This parameter is not used if the Connector is in AddOnly mode. The possible values are:

#### subtree

Return entries on all levels from search base and below.

#### onelevel

Only return entries that are immediately below searchbase.

### Time Limit

Searching for Entries must take no more than this number of seconds. **0 = no limit**.

### Size Limit

A search or iteration must return no more than this number of Entries. **0 = no limit**.

### Page Size

If specified, the LDAP Connector tries to use paged mode search. Paged mode causes the directory server to return a specific number of entries (called pages) instead of all entries in one chunk. Not all directory servers support this option.

### Comment

Your comments here.

### Authentication Method

Type of LDAP authentication. Can be one of the following:

- Simple (using **Login username** and **Login password**. Treated as anonymous if **Login username** and **Login password** not provided).
- MD5-CRAM.

- SASL (parameters for this type of authentication will need to be specified using the **Extra Provider Parameters** option).
- Anonymous (treated as Simple if **Login username** and **Login password** are supplied).

### Use SSL

If this is checked, use Secure Sockets Layer for communication with the LDAP server.

### Referrals

Specifies how referrals encountered by the LDAP server are to be processed. The possible values are:

- **follow** – Follow referrals automatically
- **ignore** – Ignore referrals
- **throw** – Throw a `ReferralException` when a referral is encountered. You need to handle this in an error Hook.

### Connector Flags

Flags to enable specific behavior.

#### **deleteEmptyStrings**

This flag causes the Connector to remove attributes containing only an empty string as value before updating the directory. If you are using an LDAP version 3 server, you must use this flag, as the value of an attribute cannot be an empty string.

### Extra Provider Parameters

Additional JNDI provider parameters. The format is one colon separated *name:value* pair on each line.

### Return attributes

List of attributes to return (one attribute per line). If you leave this empty, all non-operational (user) attributes are returned. Any operational attributes (such as `modifyTimestamp`) must still be listed explicitly in order to be returned.

### Binary Attributes

A list of attributes that are treated as binary. The format is one attribute name on each line. If this is not specified, a default list of attributes is used. The default list is:

- photo
- personalSignature
- audio
- jpegPhoto
- javaSerializedData
- thumbnailPhoto
- thumbnailLogo
- userPassword
- userCertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair
- x500UniqueIdentifier
- objectGUID
- objectSid

**Note:** An `AssemblyLine` can have one list of binary attributes only. If you have several LDAP Connectors in an `AssemblyLine`, the last Connector must define the list of binary attributes for all the LDAP Connectors in this `AssemblyLine` if you need to change this from the default.

## Auto Map AD Password

Used for adding or updating a user's password in Active Directory using LDAP. When checked, it maps the LDAP password (a **conn** attribute that must be called **userPassword**) to another name (**unicodePwd**). **unicodePwd** has a special format that the Connector translates into.

## LDAP Trace File

Trace LDAP BER packets to file.

## Sort Attribute

A new parameter to specify server side sorting. Does not work with Netscape/iPlanet 4.2.

**Note:** This increases the strain on the server.

## Virtual List View Page Size

Use Virtual List View for iterations. This might be efficient on some servers, but testing shows that some other servers (for example, Netscape/iPlanet 4.2) are very slow in this respect. However, it does provide a workaround to the out-of-memory problem.

**Attention:** This parameter causes the Connector to use the Virtual List View LDAP control. In TDI 6.1.1 this LDAP control and hence this configuration parameter is deprecated. See the "Virtual List View Control" section for more details. LDAP paging should be used instead of the LDAP Virtual List View - see the **Page Size** configuration parameter for more information.

## Simulate Rename

If the server does not support rename, simulate it with **delete** or **add** operations.

## Add Attribute (instead of replace)

This option changes the default behavior of the LDAP Connector when it modifies an entry.

If this checkbox is checked, the LDAP Connector sets the constraint **DirContext.ADD\_ATTRIBUTE**. If this checkbox is not checked, the LDAP Connector sets the constraint **DirContext.REPLACE\_ATTRIBUTE**.

By setting **DirContext.ADD\_ATTRIBUTE** constraint for the LDAP connection, you add new values to any attribute that goes through the AssemblyLine. This might mean that the same value gets repeatedly added to the entry if not used carefully. This might also result in an exception if the attribute in question is single-valued. If **DirContext.REPLACE\_ATTRIBUTE** is set, the behavior is the same as the old LDAP Connector (default behavior), that is, all values for the attribute are replaced by whatever might be in the work entry.

## Detailed Log

If this field is checked, additional log messages are generated.

## Virtual List View Control

In TDI 6.1.1 this LDAP control and hence the **Virtual List View Page Size** configuration parameter is deprecated. Newly created TDI 6.1.1 configurations as well as pre-TDI 6.1.1 configurations which didn't use this param (that is, used the default value 0) will have this attribute disabled in the GUI. Any pre-TDI 6.1.1 configurations which did use this parameter will still use it with 6.1 and the parameter will be enabled in the GUI. Note: In order to use the Virtual List View Control in TDI 6.1.1, the JNDI/LDAP Booster Pack from Sun Microsystems needs to be downloaded (<http://java.sun.com/products/jndi/downloads/index.html>). After downloading the Booster Pack the "ldapbp.jar" contained in the pack needs to be copied to the "<TDI\_install\_folder>\jars" folder before starting TDI. If the Virtual List View control is used, but the "ldapbp.jar" is unavailable, the AssemblyLine will fail with a corresponding error message.

## Handling memory problems in the LDAP Connector

Some servers return the whole search result in one go (for example, non paged search) and this typically causes memory problems. It might look to you that IBM Tivoli Directory Integrator leaks memory, but that is just because it is processing the entries from the server while the server continues to pour more and more entries into it.

LDAP servers such as Active Directory support the **Paged Search** extension that enables you to retrieve a page (the number of objects to return at a time), and this is the preferred way to handle big return sets (see the **Page Size** parameter for more info on this). You can always test if a server supports the paged search by clicking the button to the right of the **Page Size** parameter in the LDAP Connector Configuration tab.

If the **Page Size** parameter is not supported, you might have a problem, since there is little a client can do when being overwhelmed by the Server. Here are a couple of workarounds:

- See the **Virtual List View Page Size** parameter that lets you do a virtual list view. This might or might not be efficient, depending on the LDAP server you use.
- If you know that your directory is a size that can be kept in memory, you can increase the memory available to the Java VM. See the appendix "Increasing the memory available to the Virtual Machine" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*, and take particular notice of a current issue with the LDAP Connector deployed on AIX.
- A general solution to this problem is to use a server-specific utility to dump the LDAP database to an LDIF file or some other file format and then read or iterate that file using a file or URL Connector. A command line can be started in the prolog (before Connectors activated using **system.shellCommand**), producing the LDIF export and then the AssemblyLine reads that file. It is an effective solution, when possible to implement. Remember that if you are in a mode where you iterate whole, large directories, you are able to do implement as a batch.
- In some cases you can even use IBM Tivoli Directory Integrator to dump the directory search to file. This is possible because writing quickly to a file might enable IBM Tivoli Directory Integrator to access enough of the data to keep up with the feed (depending on the amount of data and the speed of the feed). If your AssemblyLine takes too long to process an entry (for example, if it is updating another directory), the entry flood happens sooner. However, this solution is very time dependent and must be avoided if you have a better method.

## LDAP Connector methods (API)

This section describes some of the methods available in the LDAP Connector. The exhaustive API reference is in the Javadocs; they can be viewed by choosing **Help>Low Level API** in the Config Editor.

### LDAP compare

```
public boolean compare(String compdn, String attname, String attvalue)
    throws Exception
```

where

- *compdn* is the DN on which you want to compare an attribute.
- *attname* is the name of the attribute you want to compare.
- *attvalue* is the value for *attvalue* that you want to check comparison for.

If the value is equal, **true** is returned. If the value is not equal, the value **false** is returned. For example, if you wanted to determine if the userpassword attribute for **cn=joe,o=ibm** was equal to **secret**, use the method: `compare("cn=joe,o=ibm", "userpassword", "secret")`.

### Adding a value to an attribute

This method adds a given value to an attribute:

```
public void addAttributeValue(String moddn, String modattr, String modval)
    throws Exception
```

where

- *moddn* is the DN to which you want to add the attribute value.
- *modattr* is the name of the attribute you want to add a value to.
- *modval* is the value you want to add to *modattr*.

For example, if you want to add **cn=bob** to the **members** attribute of **cn=mygroup**, use the method:  
`addAttributeValue("cn=mygroup", "members", "cn=bob")`

A `java.lang.Exception` is thrown when the underlying modify operation fails.

### Replacing an attribute value

This method replaces a given value for an attribute:

```
public void replaceAttributeValue(String moddn, String modattr, String modval)
    throws Exception
```

where

- *moddn* is the DN for which you want to replace the attribute value.
- *modattr* is the name of the attribute you want to replace a value for.
- *modval* is the value you want to replace for *modattr*.

For example, if you want to replace the **members** attribute of **cn=mygroup** with only **cn=bob**, use the method: `replaceAttributeValue("cn=mygroup", "members", "cn=bob")`

A `java.lang.Exception` is thrown when the underlying modify operation fails.

### Removing an attribute value

This method removes a given value from an attribute:

```
public void removeAttributeValue(String moddn, String modattr, String modval)
    throws Exception
```

where

- *moddn* is the DN for which you want to remove the attribute value.
- *modattr* is the name of the attribute from which you want to remove a value.
- *modval* is the value you want to remove from *modattr*.

For example, if you want to remove the value **cn=bob** from the attribute **members** in the DN **cn=mygroup**, use the method: `removeAttributeValue("cn=mygroup", "members", "cn=bob")`

A `java.lang.Exception` is thrown when the underlying modify operation fails.

### Removing all attribute values

This method removes all values for a given attribute:

```
public void removeAllAttributeValues(String moddn, String modattr)
    throws Exception
```

where

- *moddn* is the DN from which you want to remove the attribute values.
- *modattr* is the name of the attribute from which you want to remove all values.

For example, if you want to remove all values of the **members** attribute of **cn=mygroup**, use the method: `removeAllAttributeValues("cn=mygroup", "members")`

A `java.lang.Exception` is thrown when the underlying modify operation fails.



## Flag in Config Editor for default action for attribute add or replace

In the LDAP Connector Config Editor there is a checkbox named **Add Attributes (instead of replace)**. This option changes the default behavior of the LDAP Connector when it modifies an entry.

If this checkbox is checked, the LDAP Connector sets the constraint `DirContext.ADD_ATTRIBUTE`. If this checkbox is not checked, the LDAP Connector sets the constraint `DirContext.REPLACE_ATTRIBUTE`.

By setting `DirContext.ADD_ATTRIBUTE` constraint for the LDAP connection, you add new values to any attribute that goes through the `AssemblyLine`. This might mean that the same value gets repeatedly added to the entry if not used carefully. This might also result in an exception if the attribute in question is single-valued. If `DirContext.REPLACE_ATTRIBUTE` is set, the behavior is the same as the old LDAP Connector (default behavior), that is, all values for the attribute are replaced by whatever might be in the work entry.

You typically want this flag set when you are handling groups. If you want to add a **member** (a value) to a **group** (an attribute), you do not want to delete all the other values.

The old behavior was to replace the attribute with the new value. This behavior remains the default.

**Note:** This property can be set at any time while the Connector is running by setting the property `addAttribute` from your scripts. Use a command similar to the following:

```
work.setProperty("addAttribute", true)
```

**Note:** This property does not affect the behavior of the `addAttributeValue` and `replaceAttributeValue` methods described previously.

## Rebind

The LDAP Connector has a `rebind()` method which facilitates building advanced solutions like virtual directories and other solutions that map incoming authentication requests (use any of the support protocols) to LDAP.

## See also

“JNDI Connector” on page 129,

“Active Directory Changelog (v.2) Connector” on page 13,

“Exchange Changelog Connector” on page 71

“Netscape/iPlanet/Sun Directory Changelog Connector” on page 161,

“IBM Directory Server Changelog Connector” on page 97

“z/OS Changelog Connector” on page 233.



---

## LDAP Server Connector

The LDAP Server Connector accepts an LDAP connection request from an LDAP client on a well-known port set up in the configuration (usually 389). The LDAP Server Connector only operates in Server mode, and spawns a copy of itself to take care of any accepted connection until the connection is closed by the LDAP client.

This Connector can be used in conjunction with the IBM Password Synchronization plug-ins. For more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.

Each LDAP message received on the connection drives one cycle of the LDAP Server Connector logic. The main thread returns to listening for similar LDAP requests from other LDAP clients. At this point, Attribute Mapping will take place, and the appropriate attributes like the LDAP Operation should be mapped into the *work* object.

The rest of the AssemblyLine will be executed, and when the cycle reaches the Response channel the return message is built from Attributes mapped out, and sent back to the client. If it was an LDAP search command, the user will call the **add** method to build the data structure that is to be sent back to the client. The LDAP Server Connector goes back to listening for the next LDAP command on the existing connection.

The value of the LDAP operation is provided in the **LDAP.operation** attribute in the LDAP Server Connector *conn* entry, which should be mapped into the work entry for further processing (along with any other required attributes). Legal values are **SEARCH**, **BIND**, **UNBIND**, **COMPARE**, **ADD**, **DELETE**, **MODIFY**, and **MODIFYRDN**. The LDAP message provides a number of attributes for the specified LDAP operation.

## Scripting

The part of the AssemblyLine that follows the LDAP Server Connector must do work to determine the desired outcome of the LDAP message. The basic LDAP operations (**SEARCH**, **BIND**, **UNBIND**, **COMPARE**, **ADD**, **DELETE**, **MODIFY**, and **MODIFYRDN**) are provided as values in the LDAP Server EventHandler scripting environment to facilitate scripting, for example, if **LDAP.operation** equals **BIND**. The user code sends search result entries to the client by calling the **add ( entry )** method in the LDAP Server Connector. The entry must be formatted with legal LDAP attribute names plus the special attribute **\$dn** (the distinguished name of the entry).

## Returning the LDAP message returned values

The user-provided code in the AssemblyLine responds to each request by setting the **ldap.status**, **ldap.matcheddn** and **ldap.errorMessage** entry attributes. **ldap.matcheddn** and **ldap.errorMessage** are optional.

In the Response channel phase of the AssemblyLine, the LDAP Server Connector formats and returns some of the attributes of the *work* entry. These are:

- **LDAP.status**
- **LDAP.errorMessage**

**Note:** Only string is supported. The **resultCode** is by default set to 0 (success). A **resultCode** indicating anything other than successful must be specifically set by the user.

## Error handling

The LDAP Server Connector terminates the connection and records an error if the received message does not conform to the LDAP v3 format

**Note:** The LDAP Server Connector does not perform any validation on the incoming attributes. Any operation or parameter value is therefore accepted.

## Configuration

The Connector needs the following parameters:

### LDAP Port

The TCP port on which this Connector listens. You can choose one of the default values, or provide your own port number.

### Use SSL

If checked, the server connector will only accept SSL connections.

**Note:** Depending on your solution implementation, you may need to change the port number as well.

### Character Encoding

Specify the character set here. The default is **UTF-8**.

### Binary Attributes

A list of attributes that are treated as binary (a binary attribute is returned as a byte array, not a string). The format is one attribute name on each line.

**Note:** An AssemblyLine can have one list of binary attributes only. If you have several LDAP Connectors in an AssemblyLine, the last Connector must define the list of binary attributes for all the LDAP Connectors in this AssemblyLine (if you need to change this from the default).

### Comment

A comment for your own use.

### Detailed Log

If this field is checked, additional log messages are generated.

## See also

“LDAP Connector” on page 133

---

## Lotus Notes Connector

See “Lotus Notes Connector” on page 57.



---

## Mailbox Connector

This Mailbox Connector provides access to internet mailboxes (POP3 or IMAP). The Mailbox Connector can be used in Iterator, Lookup and Delete modes. The Mailbox Connector uses predefined attribute names for the most used headers. If you need more than this use the **mail.message** property to retrieve the native message object.

When the Mailbox Connector is used in Lookup or Delete mode the only searchable headers are:

- mail.from
- mail.to
- mail.cc
- mail.subject
- mail.messageid
- mail.messageid

On initialization, the Connector gets all available mail messages from the mailbox on the server and stores them into an internal Connector buffer. Later the Connector retrieves the messages one by one on each getNextEntry() call; that is, on each Iteration. When all the messages from the buffer have been retrieved, the parameter **Poll Interval** governs what happens next; see "Configuration." This is different from earlier implementations of this Connector.

If the IMAP protocol is specified the Mailbox Connector registers for notifications for messages added and messages removed from the mailbox on the server. When a notification that a message has been added to the mailbox is received, the Connector adds this message to its internal buffer. If a notification that a message has been removed from the mailbox is received, the Connector removes this message from its internal buffer.

### Notes:

1. Only one connection per user ID is supported. If the user fails to disconnect when using the schema tab, and then runs the AssemblyLine, this results in a connection refused error.
2. The Mailbox Connector does not support the Advanced Link Criteria (see "Advanced link criteria" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

## Configuration

### Mail Server

The POP/IMAP mail server hosting the mailbox. It might include a port number separated by a space (*url port*). For example:

```
domino.raleigh.ibm.com 110
```

### Use SSL

When checked, the Connector uses SSL connections. When unchecked, the Connector uses non-SSL connections.

### Mail Protocol

Specify **pop3** or **imap**.

### Username

The user name.

### Password

The password for **Username**.

### Mail Folder

Specifies the name of the user's mail folder on the mail server.

The user's mail folder stores the user's mail messages on the mail server. When using the POP3 mail protocol you must specify "INBOX" as the value for this parameter. When using the IMAP mail protocol you can specify any mail folder which exists on the mail server.

### **Poll Interval (seconds)**

After the AssemblyLine consumes all mail messages stored in the Mailbox Connector buffer, the Connector sleeps for a while and then reconnects to the mail server and checks for new messages. In other words, the Connector polls the server for new mail messages.

Specifies the amount of seconds that the Connector will sleep before polling the mail server for new mail messages.

A special value of "-1" means that the Connector will not poll for new mail messages after the initial poll. This means that the AssemblyLine will terminate after it has consumed all messages retrieved by the Connector on the initial poll.

### **Detailed Log**

If this parameter is checked, more detailed log messages are generated.

## **Predefined properties and attributes**

The Mailbox Connector uses the following predefined attributes and properties, which are available in the Input Map:

### **mail.from**

The **From** header

### **mail.to**

The **To** (recipient) headers

### **mail.cc**

The CC recipient headers

### **mail.replyto**

The mail address to reply to

### **mail.subject**

The subject header

### **mail.messageid**

The message ID header

### **mail.messageid**

The message's internal number

### **mail.sent**

The date the message was sent

### **mail.received**

The date the message was received

### **mail.body**

In case of a single part message this attribute contains the message body

### **mail.bodyparts**

In case of a multipart message this attribute contains a `javax.mail.Part` object.

### **mail.message**

This is the `javax.mail.Message` representing the message returned in the entry.

### **mail.originator**

The Connector object.



**event.originator**

The Connector object. This is the same object as the one stored in **mail.originator**. This Attribute ensures backward compatibility with the Mailbox EventHandler.

**mail.session**

The Java session object (javax.mail.Session).

**mailbox.session**

The Java session object (javax.mail.Session). This is the same object as the one stored in **mail.session**. This Attribute ensures backward compatibility with the Mailbox EventHandler.

**mail.store**

The message store object (javax.mail.Store).

**mailbox.folder**

The folder object (javax.mail.Folder). This is the same object as the one stored in **mail.folder**. This Attribute ensures backward compatibility with the Mailbox EventHandler.

**mail.operation**

The operation related to mail.message. For POP3 connections only *existing* entries are reported. For IMAP connections this property contains the value *new* or *deleted*.

**mailbox.operation**

The operation related to mailbox.message. This is the same object as the one stored in **mail.operation**. This Attribute ensures backward compatibility with the Mailbox EventHandler.

**See also**

“Mailbox EventHandler” on page 265.



---

## Memory Queue Connector

The MemQueue connector provides a connector like functionality to read and write to the memory queue feature (aka. MemBufferQ). This is an alternative to writing script to access a memory queue and is an extension of the “Memory Queue FC” on page 353 (function component).

The objects used to communicate between components are not persistent and are not capable of handling large return sets. For example, large data returned by an *ldapsearch* operation. In order to solve this problem, an internal threadsafe memory queue can be used as a communications data structure between AL components. It could contain embedded logic that would trigger whenever buffer is x% full/empty/data available.

This Connector supports AddOnly and Iterator modes only.

### Notes:

1. Because of the non-persistent nature of this Connector, you should use the “System Queue Connector” on page 171 instead, because that Connector relies on the underlying Java Messaging Service (JMS) functionality with persistent object storage.
2. By default, if the Memory Queue connector in Iterator mode starts reading from the queue but it doesn't exist, it will create it. If you don't want this behavior, you would need to set the system property **tdi.memq.create.queue.default=false**, in this case TDI will behave like previous versions; this implies that when the queue does not exist, an exception is thrown in Iterator Mode.

This Connector can also be used in connection with MemQueue pipes set up from JavaScript, although it is important to note that the a MemQueue pipe created by the MemQueue Connector will be terminated when the Connector closes.

The Memory queue buffer is a FIFO type of data structure, where adding and reading can occur simultaneously. It works as a pipe where additions happen at one end and reading happens at the other end and reading removes the data from queue.

The Memory queue buffer provides overflow storage using the System Store when a threshold value is reached, which is a function of the runtime memory available.

The Memory queue buffer should be constructed using the MemoryBufferQFactory.

## Memory queue components

### Paged memory buffer queue

A queue type buffer having the following functions:

1. Read and write
2. Finding the size
3. Registering and unregistering callback triggers
4. Generating triggers by calling callback methods
5. Option for setting the system store to use for paging

### Watermark

This is the maximum size of the queue; refer to the configuration page for operational details.

**Pages** Collection of objects, *pagesize* specified by the user, which does chunking of data before it is written to the system store, to optimize database writes. This is done by dividing the queue into pages and reading/writing one complete page to the system store so as to minimize the number of database read/write operations. This option is used only used when paging is use; when paging support is switched off, the queue is not divided into pages, but is purely a sequence of elements.

### **Threshold**

This is the number of pages that can exist in the memory and beyond which pages must be flushed to the system store. This is calculated depending on the page size entered by the user and runtime available memory.

### **System Store**

Database that stores the pages when the threshold is reached.

### **Global Lookup Table**

A global table that can store memory buffer objects. This is to support a named pipe mechanism of sharing between threads. A thread can lookup a memory buffer queue using a name in the table, if it exists a reference to the queue object is returned to the user else a new queue object is created with that name and added to the GLT.

## **High level workflow**

### **With Paging**

The Memory queue Buffer is a queue of pages containing objects. When a particular threshold is reached, new thread is created that starts writing to another buffer of pages, when a page is full, it transfers the page to either to the main queue or to the system store. When a page is read from the main queue, one page is transferred from system store to the main queue; in doing it also deletes that page from the system store.

### **Without paging**

The Memory queue Buffer is a queue of objects. When a particular watermark (specified by the user) is reached, the input is either blocked or it fails (can result in loss of data).

## **Configuration**

### **Instance**

Name of the Config instance. Current instance is assumed if it is null.

### **Queue**

Name of the queue or pipe which is to be created.

### **Read timeout**

The interval in milliseconds to wait for, before control returns, if no entries were found in the queue.

### **Watermark**

The Watermark parameter is either:

- With **Paging Off** (next parameter), it is the maximum queue size. When this size is reached, the **Blocking Add Parameter** determines if the read waits or fails since the queue is full.
- With **Paging On**, it is the threshold at which objects are persisted to the System Store. Note that the Page Size determines when pages are actually written, so the Watermark should be a multiple of the Page Size.

### **Enable paging using system store**

Check as to whether or not queue uses paging support using system store.

### **Page Size**

Number of entries in one page.

### **Database name**

System Store database name.

### **Username**

Username to connect to the System Store database.

### **Password**

Password to use when signing on to the database.

**Table name**

Database table name to be used.

**Blocking add operation**

Option to block or fail (and always log that data is lost) while adding, if queue is full and no paging used.

**Detailed Log**

Check for detailed log messages.

## Accessing the Memory Queue programmatically

The Memory Queue can be accessed directly from JavaScript, not only through the Connector.

1. To create new pipe - There are two methods for this.

- a. Paging disabled - `newPipe(String instName,String pipeName,int watermark)` // Does not require any DB related entries
- b. Paging enabled - `newPipe(String instName,String pipeName,int watermark,int pagesize)` // Requires DB initialization

An example script with paging enabled:

```
var memQ=system.newPipe( "inst","Q1",1000,10) ;
memq.initDB(dbName, jdbcLogin, jdbcPassword, tableName); // Required to Initialize DB
memQ.write(conn);
```

2. `getPipe(String instName,String pipeName)`

3. `purgeQueue()`

An example script would look something like this:

```
var q =system.getPipe("Inst1","Q1") ;
q.purgeQueue();
```

4. `deletePipe(String pipeName)`

Example:

```
var q =system.getPipe("Inst1","Q1");
q.deletePipe();
```

The following is an example script to read from the Memory Queue using API calls:

```
var memQ=system.getPipe( "inst","Q1") ;
var size=memQ.size();
```

```
for(var count=0;i<=size;count++){
  main.logmsg(memQ.read());
}
```



---

## Memory Stream Connector

The Memory Stream Connector can read from or write to any Java stream, but is most often used to write into memory, where the formatted data can be retrieved later. The allocated buffer is retrieved/accessed as needed.

**Note:** The memory stream is confined to the local JVM, so it's not possible to interchange data with a task running in another JVM; be it on the same machine or a different one.

The Connector can only operate in Iterator mode, AddOnly mode, or Passive state. The behavior of the Connector depends on the way it has been initialized.

### **initialize(null)**

This is the default behavior. The Connector writes into memory, and the formatted data can be retrieved with the method `getDataBuffer()`, only available in Memory Stream Connectors.

Assuming the Connector is named MM, this code can be used anywhere (for example, Prolog, Epilog, all Hooks, script components, and even inside attribute mapping):

```
var str = MM.connector.getDataBuffer();  
// use str for something.  
// To clear the data buffer and ready the Connector  
for more output, re-initialize  
MM.connector.initialize(null);
```

### **initialize(Reader r)**

The Connector reads from **r**. This can be used if you want to read from a stream.

### **initialize(Writer w)**

The Connector writes to **w**.

### **initialize(Socket s)**

The Connector can both read from and write to a Socket **s**.

**Note:** Do not reinitialize unless you want to start reading from or writing to another data stream. If you want to use the Connector Interface object, see “The Connector Interface object” on page 436. This Connector has an additional method, the `getDataBuffer()` method.

## Configuration

### **Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Parser** The name of a Parser to format the output or parse the input.





---

## MQe Password Store Connector

The MQe Password Store Connector supports Iterator mode only.

The MQe Password Store can use PKCS7 encryption to sign and encrypt the password change notification messages before it sends them to the MQe Password Store Connector.

### Notes:

1. See *MQ Everyplace Password Store Installation and Setup* (`pwsync_install_directory\IDS\readme_mqepwstore_ismp.htm`) for more information.  
In addition, for more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.
2. IBM Tivoli Directory Integrator 6.1.1 components can be deployed to take advantage of MQe Mini-Certificate authenticated access. To use these MQe features, it is necessary to download and install IBM WebSphere MQ Everyplace® 2.0.1.7 (or higher) and IBM WebSphere MQ Everyplace Server Support ES06. Use of certificate authenticated access prevents an anonymous MQe client Queue Manager or applications submitting a change password request to the MQe Password Store Connector.
3. The MQe Password Store Connector receives password update messages from an MQe QueueManager. See also the section on “MQe Initialization” on page 173 in the documentation of the “System Queue Connector” on page 171 on how these two connectors utilize MQe on the same JVM.
4. MQ Everyplace does not support IP Version 6 addressing; as a consequence, the MQe Password Store Connector can only reach MQe using traditional IPv4 addresses.

The MQe Password Store Connector supports receiving messages from multiple password stores.

The following is the MQe Password Store Connector workflow:

1. The MQe Password Store Connector requests a message from a predefined queue on its local MQe QueueManager using the JMS interface.
2. The retrieved message is verified and/or decrypted (this step is optional).
3. The message is parsed and an Entry object is created. The attributes of this Entry object represent the user ID, the password values and the type of password update.
4. This newly created Entry object is passed to the IBM Tivoli Directory Integrator AssemblyLine.

On initialization, the MQe Password Store Connector does the following:

- Gets a reference to the MQe QueueManager.
- Initiates a connection to the Storage Component and notifies the Storage Component that the MQe Password Store Connector QueueManager is up.

On getting a password update message, the Connector can operate in one of three modes:

### No wait

Checks if password update message is available in the QueueManager queue. If **yes**, the mode retrieves and parses the message. If **no**, the mode returns **NULL**, signalling the end of the Iterator.

### Number of milliseconds to wait

Waits for a specified number of milliseconds for a password update message to appear in the QueueManager queue. If the password update message appears, this mode retrieves and parses the message. If not, this mode returns **NULL**, signaling the end of the Iterator.

### Wait forever

The Connector waits until a password update message appears in the QueueManager queue. It never returns **NULL**, and when operating in this mode it must be stopped externally.

By default, the Connector automatically acknowledges every message it receives from the QueueManager JMS queue. However, you can change this behavior by de-selecting the **Auto Acknowledge** parameter; in that case, you are responsible for message acknowledgements yourself by calling the Connector's `acknowledge()` method at appropriate places in the AssemblyLine. Each time you call the Connector's `acknowledge()` method you acknowledge all messages delivered so far by the Connector.

## PKCS7 Encryption support

The MQe Password Store can use PKCS7 encryption to sign and encrypt the password change notification messages before it sends them to the MQe Password Store Connector. The use of PKCS7 encapsulation is optional; by default it is turned off. Both signing and encryption need certificates in order to function. Usage of PKCS7 is incompatible with the older PKI-based encryption mechanisms available in older versions of TDI.

With the PKCS7 option activated, it verifies the signature of each received message by comparing the Signer certificate with those in its trust store. In case of a match it verifies the message signature. If the signature verification is successful the Connector accepts the message and decrypts it with the Connector's private key from its own certificate.

**Note:** If PKCS7 needs to be used then both the MQe Password Store Connector and the MQe Password Store (all of them, if multiple Stores are used) need to be setup to use PKCS7. If only one side is configured to use PKCS7 then an error will occur.

The certificates are stored in a .jks file. The Connector has a .jks file and the MQe Password Store has another .jks file.

## Signing of messages

Signing is used to verify that the sender of the message is the one he/she claims to be.

In this particular scenario the MQe Password Store Connector needs to verify that the sender of a password change notification message is actually a trusted MQe Password Store.

It is possible to have several password stores sending messages to a single MQe Password Store Connector. In this case the Connector must be configured so that its .jks file contains the public keys of each of the trusted password stores.

## Encryption of messages

Encryption is achieved by having the password store use the public key of the Connector to encrypt the message. Then the Connector uses its private key to decrypt the message.

## Certificate management

A .jks file is required in order to be able to work with the PKCS7 functionality. It must contain not only MQe Password Store Connector's certificate, but also the certificates of all the password stores that send messages to it.

The MQe Password Store Connector's certificate is a self-signed personal certificate, whose private key is used to decrypt the messages from the password store.

The password stores' certificates are trusted signer certificates, which are supplied from each MQe Password Store's .jks file. Every received message is then verified: the public key, attached to it, is compared with the available in the .jks file. In case of a match the message signature is verified against the certificate and then the message is decrypted using the Connector's own private key.

**Certificate structure:** Certificates are stored in a .jks file. The Connector has a .jks file and the password store has another, corresponding, .jks file. The two .jks files need to contain the following so that PKCS7 can be used:

### MQe Password Store .jks file

- The public key of the Connector as a trusted signer certificate
- The private-public key pair of the password store

#### **MQe Password Store Connector .jks file**

- The public key of each trusted password store as a trusted signer certificate
- The private-public key pair of the Connector

**Creating certificates:** The primary tool used to handle .jks files is `ikeyman.exe`. `Ikeyman.exe` is a tool available with every JVM distributed with TDI.

It can be found in: `<TDI_Install>\jvm\jre\bin`, where `<TDI_Install>` is the installed directory of IBM Tivoli Directory Integrator. Below are the steps you can follow in order to create the required `keystore/truststore .jks` files.

#### **1. Creating a .jks file**

To create a new .jks file click on **Key Database File>New** and choose JKS together with the desired name and file path. You will be asked to enter a password. Remember it – it has to be provided later when setting up the components. You will need to create at least two such files – one for the `MQePasswordStore` and another one for the `MQePasswordStoreConnector`.

#### **2. Creating a certificate**

To create a new certificate click on the drop-down menu above the list of certificates and choose **Personal Certificates**. Next, click on **New Self-Signed...** and enter the appropriate information.

#### **3. Transferring certificates**

The last step is adding the just created self-signed certificates from the `MQePasswordStore`'s JKS to the `MQePasswordStoreConnector`'s and vice versa. For this purpose you have to extract the certificate as DER binary data: click on **Extract Certificate...** and then choose **Data Type-> DER Binary data**. Save it to an appropriate location with the desired name and open the other .jks file. Click **Add...** and find the file with the DER extracted data (Note: you must have chosen the **Signer Certificates** list before adding the new certificate).

**Note:** The implementation of PKCS7 in TDI 6.1.1 does not support certificates that are secured with an additional password except the one set for the .jks file.

### **Example**

The following example demonstrates how the MQe Password Store Connector can be configured to work with the configured MQe Password Store, described in *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*. Parameter **PKCS7** is checked – meaning that the PKCS7 encryption/certification option is enabled.

The path to the .jks file, parameter **PKCS7 Key Store File** is `C:\dev\di611_061025a\certs\mqeconnpkcs7.jks`. It must contain its self-signed certificate as well as the trusted signer certificate of the MQe Password Store (please refer to “Creating certificates” for more information about creating the necessary certificates). In our case the parameter **MQeConnector Certificate Alias** is specified as `“mqeconn”`.

For the needs of our example we need to create the two .jks files – ‘`mqepkcs7.jks`’ and ‘`mqeconnpkcs7.jks`’. The steps are as follows:

1. Open `iKeyman.exe` and click on **Key Database File-> New...**
2. Select the desired location of the file. For the example described above, save the .jks file under `C:\dev\061025a\certs` with the name `mqeconnpkcs7.jks`. By pressing the **OK** button, you will be asked to enter a password. To keep compatibility with the other data in the example, enter `“secret”` as password.

3. The next step is to create the MQe Password Store Connector's certificate itself. For this purpose select *Personal Certificates* from the drop-down menu and click **New Self-Signed...** The Key Label is the alias of the certificate in the .jks file. Set it to "*mqeconn*". The other options can be left with the default values.
4. Extract the just created self-signed certificate "*mqeconn*" as DER data in the same folder: C:\dev\di611\_061025a\certs. Choose a name that corresponds to the certificate itself (e.g. mqeconn). This file will be used later to import the MQe Password Store Connector's certificate in the .jks file of MQe Password Store.
5. Repeat the steps from 1 on page 157 to 4, but this time the location of the .jks file is: C:\Program Files\IBM\DiPlugins\mqepkcs7.jks and the password again: "*secret*". For Key Label of the MQe Password Store certificate set the value to "*mquestore*" and extract it as mquestore.der in the same directory: C:\Program Files\IBM\DiPlugins\.
6. Both created .jks files must exchange their certificates. Since the mqepkcs7.jks file is opened, import first the DER binary data that was extracted from mqeconnpkcs7.jks. Select *Signer Certificates* from the drop-down list and click on **Add...** In the window that popped up select "*Binary DER data*" as Data type and then browse to the location C:\dev\di611\_061025a\certs, where the .der file is saved. Select the mqeconn.der file and click "**OK**". A label for the imported certificate is required. To avoid confusion it is advisable to give it the same alias as in the other .jks file, in this case, mqeconn, because this value must be given in the properties file of the MQe Password Store for the property "*pkcs7MqeConnectorCertificateAlias*".
7. The same procedure must be performed on the mqeconnpkcs7.jks file (the key store holding the necessary certificates for the connector). First open the .jks file by clicking **Key Database File-> Open...** and navigate to the exact location. If you followed all the instructions precisely the path to the required file should be C:\dev\di611\_061025a\certs. The password will be prompted for again. Afterwards repeat step 6 with the new parameters. The location is C:\Program Files\IBM\DiPlugins and the certificate name is mquestore.der. For convenience name it "*mquestore*" again. With this step the example is completed.

## MQe Password Store Connector Entry structure

The MQe Password Store Connector constructs IBM Tivoli Directory Integrator Entry objects with the following fixed attribute structure:

### UserID

Contains a single string value.

### OperationType

Contains one of the following string values:

- **replace** (replace password values operation)
- **add** (add password values operation)
- **delete** (delete password values operation)

### Passwords

A multi-valued attribute. Each value is a string representing a password value.

## Configuration

### GetNext Timeout

Specify the number of milliseconds the Connector waits for a new password update message to appear in the QueueManager queue. Specify **-1** to wait forever, and **0** to return immediately if no message is available.

### Storage notification server(s)

Specify in a *host:port* format the Storage Component server that listens for notifications from the MQe Connector. The default value for the port is **41002** and the host must be the IP address of the machine where the Password Synchronizer and the Storage Component are deployed.

There can be multiple Storage Component servers; specify each on a separate line.

**Auto Acknowledge**

If checked each message is automatically acknowledged, otherwise messages should be acknowledged manually through the Connector's `acknowledge()` method. Default is selected.

**Decrypt messages**

Check this field if the Storage Component encrypts the password update messages and they need to be decrypted by the MQe Connector.

**Key Store File**

The path of the JKS file used to decrypt password data (only taken into account when the Decrypt messages field is selected).

**Key Store File Password**

The password of the JKS file (only taken into account when the Decrypt messages field is selected).

**Key Store Certificate Alias**

The alias of the key from JKS file (only taken into account when the Decrypt messages field is selected).

**Key Store Certificate Password**

The password used to retrieve the private key. If not specified, the **Key Store File Password** is used to retrieve the private key (only taken into account when the Decrypt messages field is selected).

**PKCS7**

This indicates whether PKCS7 encapsulation is used or not. The default value is disabled. All other parameters related to the PKCS7 functionality are considered if only this parameter is enabled.

**PKCS7 Key Store File**

This is the full path to the MQePasswordStoreConnector's JKS together with its name. There is no need for double slash "\\\" instead of single "\", when specifying the file path on Windows platforms.

**PKCS7 Key Store File Password**

The actual, plaintext value of the password for the JKS file (whereas for the MQePasswordStore's property the encrypted version is required).

**MQeConnector Certificate Alias**

The alias of the MQePasswordStoreConnector's certificate as it is saved in the .jks file without any extensions.

**Detailed Log**

Check this field for more detailed log messages.

**See Also**

"System Queue Connector" on page 171,

The chapter on System Queue in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*,  
MQe Password Store in *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.



---

## Netscape/iPlanet/Sun Directory Changelog Connector

The iPlanet Changelog Connector is a specialized instance of the LDAP Connector.

In iPlanet Directory Server 5.0, the format of the changelog was modified to a proprietary format. In earlier versions of iPlanet Directory Server, the change log was accessible through LDAP. Now the changelog is intended for internal use by the server only. If you have applications that must read the changelog, you will need to use the iPlanet Retro Change Log Plug-in for backward compatibility.

**Note:** The current name for Sun Microsystem's directory offering is "Directory Server 5".

Since it is not always possible to run the iPlanet Directory Server in Retro Changelog mode, the Connector is able to run in two different Delivery Modes:

1. *Changelog* mode – in this mode the Connector will iterate through the changelog (enabled by the iPlanet Retro Change Log Plug-in) and after delivering all Entries it will poll for new changes or use change notifications
2. *Realtime* mode – in this mode, only changes received as notifications will be delivered and offline changes will be lost. The Connector will not use the changelog in this mode. This delivery mode is necessary for Netscape/iPlanet Servers that do not support a changelog

This Connector supports Delta Tagging, in two different operation modes:

- In **Changelog** mode Delta tagging is supported at the Entry level, the Attribute level and the Attribute Value level. It is the LDIF Parser that provides delta support at the Attribute and Attribute Value levels.
- In **Realtime** mode Delta tagging will be performed at the Entry level only.

## Configuration

The Connector needs the following parameters:

### LDAP URL

The LDAP URL for the connection (`ldap://host:port`).

### Login username

The LDAP distinguished name used for authentication to the server. Leave blank for anonymous access.

### Login password

The credentials (password).

### Authentication Method

The authentication method. Possible values are:

- CRAM-MD5 (use the CRAM-MD5 (RFC-2195) SASL mechanism).
- none (use no authentication (**anonymous**)).
- simple (use weak authentication (cleartext password)).
- If not specified, default (simple) is used. If **Login username** and **Login password** are blank, then **anonymous** is used.

### Use SSL

If Use SSL is **true**, the Connector uses SSL to connect to the LDAP server. Note that the port number might need to be changed accordingly.

### ChangeLog Base

Specifies the search base where the Changelog is kept. The standard DN for this is **cn=changelog**. Also known as Notification Context for 'Realtime' Delivery Mode.

**Extra Provider Parameters**

Allows you to pass a number of extra parameters to the JNDI layer. It is specified as name:value pairs, one pair per line.

**Iterator State Key**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

**Start at changenumber**

Specifies the starting changenumber. Each Changelog entry is named **changenumber=intvalue** and the Connector starts at the number specified by this parameter and automatically increases by one. The special value **EOD** means start at the end of the Changelog.

**State Key Persistence**

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and choices are:

**After read**

Updates the System Store when you read an entry from the iPlanet Directory Server change log, before you continue with the rest of the AssemblyLine.

**End of cycle**

Updates the System Store with the change log number when all Connectors and other components in the AssemblyLine have been evaluated and executed.

**Manual**

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the iPlanet Directory Server Changelog Connector's *saveStateKey()* method, somewhere in your AssemblyLine.

**Delivery Mode**

Specifies whether to use changelog or notifications entries. If the LDAP Server doesn't maintain a changelog, **Realtime** is only applicable option. The default is **Changelog**.

**Use Notifications**

Specifies whether to use notification when waiting for new changes in iPlanet Directory Server. If enabled, the Connector will not sleep or timeout but instead wait for a Notification event from the iPlanet Directory Server.

**Batch retrieval**

Specifies how searches are performed in the changelog. When unchecked, the Connector will perform incremental lookups (backward compatible mode). When checked, and the server supports "Sort Control", searches will be performed with query 'changenumber>=some\_value', corresponding to the last retrieval you made; this works in conjunction with the next parameter, **Page Size**. By default, this option is unchecked.

**Page Size**

Specifies the size of the pages IDS will return entries on (default value is 500). It is used only when **Batch retrieval** is set to true (checked).

**Timeout**

Specifies the number of seconds the Connector waits for the next Changelog entry. The default is 0, which means wait forever.

**Sleep Interval**

Specifies the number of seconds the Connector sleeps between each poll. The default is 60.

**Detailed Log**

If this field is checked, additional log messages are generated.



## See also

"LDAP Connector" on page 133,

"Active Directory Changelog (v.2) Connector" on page 13,,

"Exchange Changelog Connector" on page 71

"IBM Directory Server Changelog Connector" on page 97

"z/OS Changelog Connector" on page 233.



---

## Properties Connector

This connector deals with "*property=value*" definitions, as in the configuration files `global.properties` and `solution.properties`, as well as other properties collections available in the IBM Tivoli Directory Integrator Property Store.

This Connector uses an internal memory buffer to hold all properties in a properties file. The connector can also be used to access the JavaVM system properties object.

The Connector supports Iterator, AddOnly, Update, Lookup and Delete mode.

Also see "Property Store" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for more information about the TDI Property Store concept.

## Configuration

The Properties Connector uses the following parameters:

### Collection

Specifies the properties file to read/write when collection type is File/URL. This parameter is required if the collection type is File/URL.

### Encryption

Set to True if parser should decrypt/encrypt the entire data stream. Default value is False.

### Cipher

The cipher algorithm to use when either Encryption=TRUE or the stream contains individually encrypted values. Specify SERVER to use TDI server encryption. Default cipher provided in `global.properties` / `solution.properties`

### Password

The secret key to use when encrypting/decrypting the stream/property values.

Required when encryption is active and Cipher is not SERVER.

### AutoRewrite

If true, the Connector will write back the contents if any auto-encrypted values were found.



---

## Server Notifications Connector

The Server Notifications Connector is an interface to the IBM Tivoli Directory Integrator (TDI) notification system. It listens for and reports, as well as issues, Server API notifications. The Connector provides the ability to monitor various processes taking place in the TDI Server, such as AssemblyLine stop and start processes, as well as issue custom server notifications.

The Server Notifications Connector supports the Iterator and AddOnly modes:

- In Iterator mode, when the Server API notification system issues an event, the event is acquired by the Server Notifications Connector and buffered in a queue internal to the Connector. On the next getNextEntry() method, the Connector returns the next event buffered in the internal Connector queue.
- In AddOnly mode, the Connector is capable of issuing custom Server API notifications, which can be handled by TDI components that have registered to listen for these notifications through the Server API.

## Encryption and Cryptography

The Server Notifications Connector provides the option to use Secure Sockets Layer (SSL) when the connection type is set to remote. If the remote TDI server accepts SSL connections only, the Server Notifications Connector automatically establishes an SSL connection provided that a trust store on the local TDI Server is configured properly. When SSL is used, the Connector uses a Server API SSL session, which runs RMI over SSL.

### Trust store

A trust store on the local TDI Server is needed because when the remote TDI server fires a notification a new SSL connection to the local TDI Server is created and in order for this new SSL connection session to be established the local TDI Server must trust (through its trust store) the remote TDI Server SSL certificate. A trust store is configured by setting the appropriate values for the javax.net.ssl.trustStore, javax.net.ssl.trustStorePassword and javax.net.ssl.trustStoreType properties in the global.properties or solution.properties files.

## Authentication

### SSL Authentication

The Server Notifications Connector is capable of authenticating by using a client SSL certificate. This is only possible when the remote TDI Server API is configured to use SSL and to require clients to possess SSL client certificates. A trust store must be configured properly on the local TDI server.

### Username and Password Authentication

The Server Notifications Connector is capable of using the Server API username and password authentication mechanism. The desired username and password can be set as a Connector parameter, in which case the Connector will use the Server API username and password authentication mechanism. If SSL is used and a username and password have been supplied as Connector parameters, then the Connector will use the supplied username and password and not an SSL client certificate to authenticate to the remote TDI Server.

## Configuration

The Server Notifications Connector uses the following parameters:

### connectionType

Determines whether the Server Notifications Connector will listen for and emit local or remote Server API notifications. The available values for this parameter are remote and local. local means that the Connector will only listen for and notifications in the local Java Virtual Machine. remote means that the Connector will connect to a remote TDI Server system and register for and emit notifications in the Java Virtual Machine of that remote system.

**url** Specifies the Remote Method Invocation (RMI) URL used to connect to the remote TDI Server system. This parameter is only taken into account if the `connectionType` parameter is set to `remote`. An example value for this parameter is:

```
rmi://127.0.0.1:1099/SessionFactory
```

**username**

Specifies the user name the Connector uses to authenticate to the TDI server. This parameter is only taken into account if the `connectionType` parameter is set to `remote`.

**password**

Specifies the password the Connector uses to authenticate to the TDI server. This parameter is only taken into account if the `connectionType` parameter is set to `remote`.

**configInstanceId**

Specifies a Config Instance ID, which the Connector will use to filter event notifications. If this parameter is specified, the Connector will only report notifications that have this Config Instance ID. This parameter is only taken into account if the Connector mode is `Iterator`.

**notificationId**

Specifies a Notification ID, which the Connector will use to filter event notifications. If this parameter is specified the Connector will only report notifications which have the specified notification ID. This parameter is only taken into account if the Connector mode is `Iterator`.

**timeOut**

Specifies the maximum number of seconds to wait for a notification. After this timeout expires, the Connector will terminate. If this parameter value is set to "0", then the Connector will wait forever. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_all** Specifies if "di.\*" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_ci\_all**

Specifies if "di.ci.\*" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_ci\_start**

Specifies if "di.ci.start" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_ci\_stop**

Specifies if "di.ci.stop" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_ci\_file\_updated**

Specifies if "di.ci.file.updated" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_al\_all**

Specifies if "di.al.\*" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_al\_start**

Specifies if "di.al.start" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_al\_stop**

Specifies if "di.al.stop" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_eh\_al**

Specifies if "di.eh.\*" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is `Iterator`.

**di\_eh\_start**

Specifies if "di.eh.start" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is Iterator.

**di\_eh\_stop**

Specifies if "di.eh.stop" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is Iterator.

**di\_server\_stop**

Specifies if "di.server.stop" notifications will be received by the Connector. This parameter is only taken into account if the Connector mode is Iterator.

**hasCustomNotifications**

Specifies whether the Connector will receive any additional or custom notifications. If it is checked the additional/custom notifications can be specified in the "customNotifications" Connector parameter. This parameter is only taken into account if the Connector mode is Iterator.

**customNotifications**

Specifies the notification types of additional or custom Server API notifications which the Server Notifications Connector will listen to and report. Each notification type must be typed on a separate line. This parameter takes effect only if the hasCustomNotifications parameter is true, and is only taken into account if the Connector mode is Iterator.

**Debug**

Turns on debug messages. This parameter is globally defined for all TDI components.





---

# System Queue Connector

## Introduction

The System Queue provides a subsystem similar to Java Message Service (JMS) for IBM Tivoli Directory Integrator. It is designed for storing and forwarding general messages and TDI Entry Objects, between TDI Servers and AssemblyLines.

The System Queue Connector is the mechanism for AssemblyLines to interface with the System Queue. To learn more about the System Queue and its configuration, refer to the System Queue section in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.

The System Queue Connector can be used with AssemblyLines in Iterator and AddOnly modes:

- In Iterator mode, the Connector retrieves TDI Entry objects from a specified message queue.
- In AddOnly mode, the Connector stores TDI Entry objects in the specified message queue.

**Note:** If two JMS clients retrieve messages from the same JMS queue simultaneously, an error might occur. Avoid solutions which use several instances of the System Queue Connector retrieving messages from the same JMS queue simultaneously. However, an instance of the System Queue Connector writing to a queue and another instance of the Connector reading from that same queue at the same time is acceptable.

The System Queue Connector uses the Server API to access the System Queue. The Connector uses both the local and remote interfaces of the Server API, allowing the Connector to operate on a TDI System Queue running on a remote computer. The Connector's ability to operate on a remote computer, coupled with the System Queue's capability to connect to remote JMS servers, results in the ability to use some quite complex deployment scenarios. For example: a TDI server and a System Queue Connector deployed on machine A, working through the remote Server API with the TDI server and System Queue on machine B, which in turn interface with a JMS server deployed on machine C.

## Configuration

The System Queue Connector uses the following parameters:

### Connection Type

This parameter determines whether the System Queue Connector works with the System Queue of the local TDI server or with the System Queue of a remote TDI server. The available values for this parameter are *local* and *remote*.

- The value *local* specifies that the Connector will use the local Server API interfaces and will work with the System Queue of the local TDI server.

The value *remote* specifies that the Connector will use the remote Server API interfaces and will work with the System Queue of a remote TDI server. In that case, the RMI URL parameter is required, the Connector configuration (both the Connector parameters and the SSL configuration of the local TDI Server) must match the configuration of the remote TDI Server.

### RMI URL

The Remote Method Invocation (RMI) URL used to connect to the remote TDI Server system. An example value for this parameter is:

```
rmi://127.0.0.1:1099/SessionFactory
```

This parameter is taken into account only if the `connectionType` parameter is set to `remote`.

### Username

Used to authenticate to the remote TDI server using the user name and password authentication mechanism of the Server API. This parameter is taken into account only if the `connectionType` parameter is set to `remote`.

**Password**

Used to authenticate to the remote TDI server. This parameter is taken into account only if the `connectionType` parameter is set to *remote*.

**Queue Name**

Specifies the name of the JMS queue with which the Connector will work. In Iterator mode, the Connector retrieves Entry objects from this queue. In Add-Only mode, the Connector stores Entry objects in this queue.

**Timeout**

Specifies the amount of time in seconds the Connector will wait before returning a null Entry object. If a value of zero (0) is specified for this parameter, the Connector will immediately return if there are no available Entry objects in the queue. If a negative value is specified for this parameter then the Connector will wait indefinitely or until an Entry object becomes available in the queue.

**Detailed Log**

This parameter turns on debug messages. This parameter is globally defined for all TDI components.

## Security, Authentication and Authorization

### Encryption

When the connection type is set to *remote* and the remote TDI server is configured to use Secure Sockets Layer (SSL), then the System Queue Connector uses SSL, provided that a trust store on the local TDI Server is configured properly. When SSL is used, the Connector uses a Server API SSL session, which runs RMI over SSL.

**Note:** Of the standard JMS Drivers only the driver for MQ supports SSL out of the box. The MQe JMS Driver only works with a local Queue Manager – this is mandated by the MQe architecture. The JMS Script Driver is a generic driver which supports whatever the corresponding user-provided Javascript supports.

### Authentication

**Username and password authentication:** The System Queue Connector can use the remote Server API username and password authentication. The Connector does not implement any authentication itself. The username and password supplied to the Server API are configured as Connector configuration parameters.

**SSL certificate-based authentication:** The System Queue Connector is capable of authenticating by using a client SSL certificate. This is only possible when the remote TDI Server API is configured to use SSL and to require clients to possess SSL client certificates. A trust store must be configured properly on the local TDI server.

If SSL is used and a user name and password have been supplied as Connector parameters then the Connector will use the supplied user name and password and not the SSL client certificate to authenticate to the remote TDI Server.

### Authorization

The Server API authorization mechanism is applied to the Server API session the System Queue Connector establishes to the TDI Server. With the TDI 6.1.1 Server API once the System Queue Connector is authenticated it can use the TDI System Queue.

### See Also

"JMS Connector" on page 115,

"System Queue" in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.

## MQe Initialization

There are two Connectors that can initialize MQ Everyplace (MQe): the “MQe Password Store Connector” on page 155 and the “System Queue Connector” on page 171. Because there can be only one instance of MQe in an instance of the JVM, it is necessary that MQe be initialized only once. To resolve the conflict that might arise by the MQe Password Store Connector and the System Queue Connector initializing MQe separately, the initialization of MQe takes place in a central location: the System Queue Engine.

**Note:** Because of these limitations, you should not attempt to start MQe yourself from within the same JVM that TDI runs in (for example, from Java or JavaScript), otherwise problems will occur if you attempt to use any of the aforementioned Connectors.

Components that need MQe will be able to get the necessary MQe objects from the SystemQueueEngine.

MQe is initialized on TDI server startup. To ensure compatibility with the SystemQueue Connector, the MQePasswordStore Connector has been modified so that it retrieves the required MQe objects from the System Queue instead of initializing MQe itself.

If you need to change the default MQe parameters, you would use the MQe Configuration Utility. This utility is described in a section named “MQe Configuration Utility” in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.



---

## Windows Users and Groups Connector

The Windows Users and Groups Connector (in older versions of TDI this was called the NT4 Connector) operates with the Windows NT<sup>®</sup> security database. It deals with Windows users and groups (the two basic entities of the Windows NT security database). This Connector can both read and modify Windows NT security database on the local Windows machine, the Primary Domain Controller machine and the Primary Domain Controller machine of another domain.

**Note:** This Connector is dependent on a Windows NT API, and only works on the Windows platform.

The Connector is designed to connect to the Windows NT4 and Windows 2000 SAM databases through the Win32 API for Windows NT and Windows 2000/2003 user and group accounts. You can connect to a Windows 2000 SAM database, but the Connector only reads or writes attributes that are backward-compatible with NT4 (in other words, the Windows Users and Groups Connector has a predefined and static attribute map table consisting of NT4 attributes). Windows 2000/2003 native attributes or user-defined attributes are therefore not supported by this Connector.

See “Windows Users and Groups Connector functional specifications and software requirements” on page 178 for a full functional specification of the Connector, architecture description as well as hardware and software requirements.

### Preconditions

To successfully run the Windows Users and Groups Connector and obtain all of its functionality, the Connector must be run in a process owned by a user who is a member of the local Administrators group, and have logon privileges to the domain controller and other domains (if accessed). This precondition can be omitted if the **UserName** and **Password** parameters of the Connector are set to specify an account with the requirements stated above.

The Windows Users and Groups Connector is designed and implemented to work in the following modes:

- Iterator
- Lookup
- AddOnly
- Delete
- Update

**Note:** This Connector does not support Advanced Link Criteria (see “Advanced link criteria” in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

### Configuration

The Connector needs the following parameters:

#### Computer Name

The name of the machine (for example, **ntserver01** ) or its IP address (for example, **212.52.2.218**) where the Connector operates. The machine IBM Tivoli Directory Integrator is running on must be in the same Domain or Workgroup as the target system.

#### Username

If blank, no logon to the specified machine is performed and the Connector has the privileges of the process in which IBM Tivoli Directory Integrator is run. If some value is set, then the Connector attempts to log on to the **Computer Name** machine with this user name and the password specified by the **Password** parameter.

#### Password

The value of this parameter is taken into account only when the parameter **Username** is set with a non-blank value. It then specifies the password used for the logon operations.

### Entry Type

Must be set to **User** (specifying that the Connector operates with data structured by Users) or **Group** (specifying that the Connector operates with data structured by Groups).

### Page Size

Specifies the number of Entries (Users and Global Groups) that Windows NT or Active Directory return in one chunk when the Connector retrieves Users and Global Groups. Must be a number between 1 and 100.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Constructing Link Criteria

Construct link criteria when using the Windows Users and Groups Connector in Lookup, Update and Delete modes. The Connector supports Link Criteria that uniquely identifies one entry only. The format is strict, and passing a Link Criteria that doesn't match this format results in the following exception:

Unsupported Link Criteria structure.

The following is the Link Criteria structure that must be used, depending on Entry Type:

**User** Windows Users and Groups Connector **Entry Type** parameter is set to **User**. This parameter consists of just one row where:

- Connector attribute is set to **UserName**.
- Operand is set to **equals**.
- Value is set to a name of a user account (for example, **user name**) or configured by a template to receive the name of a user account.

**Group** Windows Users and Groups Connector **Entry Type** parameter is set to **Group**. This parameter consists of two rows as follows:

1. Initial row:
  - Connector attribute is set to **GroupName**.
  - Operand is set to **equals**.
  - Value is set to a name of a group account (for example, **group name**) or configured by a template to receive the name of a group account.
2. Second Row:
  - Windows Users and Groups Connector attribute is set to **IsGlobal**.
  - Operand is set to **equals**.
  - Value is set to **True** to indicate that the group account specified in the first row is global, or **False** to indicate that the group account is local. Can also be configured by a template to receive **True** or **False** values indicating global or local group accounts.

## Other

**User and Group account names:**

### On Domain Controller Machine

Users and groups are retrieved and must be accessed in the following formats:

*USER\_NAME, GROUP\_NAME*

### On Non-Domain Controller Machine

Local users and groups are retrieved and must be accessed in the following format:

*USER\_NAME, GROUP\_NAME*

Global groups and domain users (can be members of a local group on a non-domain controller machine) are retrieved and must be accessed in the following format:

*DOMAIN\_NAME\GLOBAL\_GROUP\_NAME, DOMAIN\_NAME\USER\_NAME*

**Creating a new user:** When creating a new user with the Windows Users and Groups Connector, if any of the following attributes are omitted or assigned a **null** value, they are automatically assigned a default value as follows:

**Flags** The account is marked as **normal account** and **user password never expires**.

**AccountExpDate**

A value that indicates that the **account never expires** is set.

**LogonHours**

A value that indicates that there is no time restriction set (for example, the user can log on always).

## Setting user password

Remember that a user password value cannot be retrieved. Windows stores this in a format that cannot be read. If an AssemblyLine copies users from one Windows machine to another, you must set the **Password** attribute value manually.

When adding a user, passing the **Password** attribute with no value results in creating a user with an empty password.

When modifying a user, passing the **Password** attribute with no value results in retaining the old password.

## Setting user Primary Group/global groups membership

All Domain Users must be members of their Primary Groups. This means that the value set in the **PrimaryGroup** attribute must be present in the **GlobalGroups** attribute. If there is no value for the PrimaryGroup attribute then it will be set to "Domain Users".

## Operating with groups

There are certain groups that are predefined and special for Windows, and there are certain operations that are not enabled on these groups. Such operations are delete, rename and modification of some of their attributes. Any attempt to try such an invalid operation over any of these groups results in an exception thrown.

Here is the list of these groups, structured by Windows installations:

Domain Controller:

- Global groups
  - Domain admins
  - Domain users
- Local groups
  - Administrators
  - Users
  - Guests
  - Backup operators
  - Replicator
  - Account operators
  - Print operators
  - Server operators

Non-Domain Controller:

- Local groups
  - Administrators

- Users
- Guests
- Backup operators
- Replicator
- Power Users

## Character sets

Unicode is supported.

## Examples

Navigate to the *root\_directory/examples/NT4* directory of your IBM Tivoli Directory Integrator installation.

## Windows Users and Groups Connector functional specifications and software requirements

The Windows Users and Groups Connector implements Windows Users and Groups database access for both user and group management on Windows systems according to Windows definitions and restrictions as outlined below.

### Functionality

**Extract user and group data:** The Windows Users and Groups Connector reads both user and group information from the Windows Users and Groups repository, including group and user metadata as well as relationship information (for example, **users** group and **groups** group membership). The Connector reads both local and domain user or group data. Data is read from Windows, then organized and provided in the containers expected by IBM Tivoli Directory Integrator.

**Add user and group data:** The Windows Users and Groups Connector adds user information to both local machines and domain controllers, and it adds group information to both local machines and domain controllers. When operating with a domain controller, the Connector can create both local and global groups. When operating with a machine that is not a domain controller, the Connector can only create local groups, according to security restrictions set by Windows.

**Modify group membership:** The Windows Users and Groups Connector modifies group membership for both local and global groups. In accordance with Windows NT security restrictions, members can be assigned to groups as follows:

- A global group can have users from its domain as members only.
- A local group can have global groups and users from its domain or any trusted domain as members. However, a local group cannot contain other local groups.
- Users on a local machine can exist without being members of a group.
- Each user on a domain controller must belong to a Primary Group. The Primary Group for a user can be any global group in the domain. While the user's Primary Group can be changed, he is always a member of his Primary Group.

**Modify user and group data:** The Windows Users and Groups Connector modifies external and group properties on both local machines and domain controllers. When connected to a domain controller, the Connector is able to modify the properties of both local and global groups.

**Delete user and group data:** The Windows Users and Groups Connector can remove users from both local machines and domain controllers, and it can remove local groups from both local machines and domain controllers. When operating with a domain controller, the Connector can remove both local and global groups.



---

## System Store Connector

The System Store Connector (named "*ibmdi.PESConnector*" in the create new Connector dialog) provides access to the underlying System Store. The primary use of the System Store Connector is to store **Entry** objects into the System Store tables. However, you can also use the connector to connect to an external CloudScape, DB2 8.1, Oracle or MS SQL\*Server database, not just the database configured as the System Store. Each **Entry** object is identified by a unique value called the key attribute.

The System Store Connector creates a new table in a specified database if one does not already exist. If you iterate on a non-existing table, the (empty) table is created, and the Iterator returns no values.

The System Store Connector uses the following SQL statements to create a table and set the primary key constraint on the table (Cloudscape syntax):

```
"CREATE TABLE {0} (ID VARCHAR(VARCHAR_LENGTH) NOT NULL, ENTRY BLOB );  
ALTER TABLE {0} ADD CONSTRAINT {0}_PRIMARY Primary Key (ID);"
```

For Cloudscape and DB2, these SQL statements are pre-set, but you may modify them to suit your needs. For other databases, you must enter your own, equivalent SQL statements (multiple ones, if required) by specifying these in the **Create Table Statement** parameter. The parameter can not be empty; in that case, an exception is thrown.

### Notes:

1. The `VARCHAR_LENGTH` value is picked up from the `com.ibm.di.store.varchar.length` property set in the Properties Store (TDI-P). The default `VARCHAR_LENGTH` is set to 512. You can change this value by setting the value of the `com.ibm.di.store.varchar.length` in the Properties Store.
2. Another attribute, `tdi.pesconnector.return.wrapped.entry`, exists for TDI 6.0 backward compatibility. If you define this property in the TDI `global.properties` file and set it to `true`, then TDI reverts back to its earlier behavior where for example, the `findEntry()` method (used by the system in Iterator, Lookup and Update modes) would return an Entry object of the format: [ENTRY: <Instance of Entry object containing Attributes passed by user>]. In TDI 6.0, in order to obtain the original passed attributes, you would need to write JavaScript code something like this:

```
Entry e = (Entry)conn.getAttribute("ENTRY");
```

at some appropriate place, after which *e* contains the Attributes originally passed in when writing to the System Store. You could do this in the Input Attribute Map Hook where you would have to carefully map the Attributes in *e* to the *work* entry, or use a Script Component after this Connector to unpack the composite *entry* attribute in the *work* entry using the aforementioned JavaScript example (substitute *work* for *conn*.)

In TDI 6.1.1, by default the entry is unwrapped and therefore all attributes passed by you are now directly available as attributes in the Entry. The above scripting will not be needed any longer (unless you set the `tdi.pesconnector.return.wrapped.entry` attribute to `true`.)

3. The System Store Connector operates in the following modes: AddOnly, Update, Delete, Iterate, Lookup. However, AddOnly, Update and Delete operations are not permitted on the Delta Tables, Checkpoint/Restart (CPR) tables and Property store tables.

The Connector supports both simple and advanced Link Criteria.

The System Store Connector along with the System Store provides an alternative to the Btree Connector. It is recommended to use the System Store Connector and System Store rather than the Btree Connector to store Entry Objects.

This Connector, like the JDBC Connector it is based upon, in principle can handle secure connections using the SSL protocol. However, it may require driver specific configuration steps in order to set up the SSL support. Refer to the manufacturer's driver documentation for details.

## Configuration

The System Store Connector requires the following parameters.

### Database

The location of the database. This is an optional parameter; if left blank, the System Store as configured in property `com.ibm.di.store.database` in the `global.properties` file is used. Note that this is the value displayed in the Store | View System Store screen.

### Username

The name of the user used to make a JDBC connection to the specified database. Only the tables available to this user are shown. If this is not specified then the value of the `com.ibm.di.store.jdbc.user` property set in the `global.properties` file is used as the default value.

### Password

The password of the user used to make a JDBC connection to the specified database. If this is not specified then the value of the `com.ibm.di.store.jdbc.password` property set in the `global.properties` file is used as the default value.

### Key Attribute Name

The attribute name giving the unique value for the entry. This is a required parameter.

**Note:** You can specify multiple Key Attribute Names separated by the "+" sign. The System Store Connector will concatenate these into a single `varchar(255)` key to obtain a unique key.

### Selection Mode

Specify **All**, **Existing** or **Deleted**. In order to use the **Existing** and **Deleted** keywords, the Connector must reference a Delta table in the System Store. When Delta is enabled on an Iterator, the AssemblyLine stores a sequence property in the database, adding a sequence number to each entry read from the source. This parameter is to be used on Delta tables only.

**Note:** Delta table names in TDI 6.0 and above, have an "IDI\_DS\_" prefix added to the *identifier* specified in "Delta Store" field of the Delta configuration tab. Similarly, CPR table names are prefixed with "IDI\_CP\_" and the property store table names are prefixed with "IDI\_PS\_".

### Table Name

The table name to store the entries in. This is a required parameter. The System Store Connector will create a table with the specified table name if it does not exist.

#### Notes:

1. The "Select" button in the Connector configuration tab of the connector provides a list of tables in the connected database. Only the tables available to the user specified in the Username field are shown.
2. The "Delete" button in the Connector configuration tab can be used to delete a selected table. Ideally, the Delete button should be used when an AL has run and you would now want to delete the table created by the System Store Connector. This does not work with the Delta and CPR tables.

### Select Database Driver

Select the database to connect to. You can select CloudScape, DB2 or other.

### Create Table Statement

The "CREATE TABLE" SQL statement(s) used to create the tables in the selected data source. Each statement must end with semicolon. This depends on the choice of the driver in the "Select Database Driver" parameter. If the database driver specified is Cloudscape or DB2 then the appropriate CREATE TABLE statements for these databases are displayed; you may modify them to suit your needs. If the database driver selected is "Other" then you are *required* to enter the correct CREATE TABLE statement(s) corresponding to the database that you choose to connect to.

### Delete table on close

If this value is set to **true** then the table created by the System Store Connector will be dropped when the Connector terminates.

### SQL Select

The select statement to execute when selecting entries for iteration. Specifies the WHERE clause. This will be used as a search filter to return the data set in Iterator mode. If this is left blank, the default construct (SELECT \* FROM TABLE) is used, where TABLE is the name specified in the "Table Name" field.

### Commit

Controls when database transactions are committed. Options are:

- After every database operation
- On Connector Close
- Manual

**Manual** means user must call the *commit()* method of the System Store Connector — or, alternatively, *rollback()* if your logic requires this.

### Detailed Log

If this field is checked, additional log messages are generated.

## Using the Connector

The System Store Connector provides access to the tables created in the **System Store**. The System Store could be located on a CloudScape Database server, a DB2 Database server, an Oracle database server or an MS\*SQL Server. Furthermore, if the System Store uses CloudScape, it can be configured to run in either embedded or networked mode. The only change that needs to be made while using the System Store Connector with the above mentioned configurations of System Store is the **Database** field.

The correct way to specify the database for different configurations of System Store is given below.

**Note:** The examples are specific to Windows.

### Using System Store Connector with embedded CloudScape server configured as System Store

**Database:** f:\Program Files\IBM\IBMDirectoryIntegrator/CloudScape

**Note:** In the embedded mode of operation, the CloudScape server is automatically started and the specified database is booted into the database if it exists. If it does not exist a new database is created at the specified location.

### Using System Store Connector with networked CloudScape server configured as System Store

**Database:** jdbc:derby://localhost:1527/E:\TDI\TDISysStore;create=true

#### Notes:

1. It is important to specify the "create=true" flag in the database URL. This will create the database if it does not exist. This is required when CloudScape is configured to run in networked mode.
2. In networked mode of operation, the CloudScape server has to be started manually. For details regarding the ways in which a CloudScape server can be started in networked mode, please refer to the chapter on *System Store* in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*

### Using System Store Connector with DB2 8.1 server as System Store

**Database:** jdbc:db2://machine-name:50000/testDB

#### Notes:

1. The DB2 instance and the DB2 database must be created ahead of time for it to be used as System Store.

2. The specified instance must be running on the specified port in the database URL.

## **See also**

“Btree Object DB Connector” on page 25,

The chapter on *System Store* in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*,  
*Appendix A — Using CloudScape Database* in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*

---

# RAC Connector

## Introduction

"RAC" stands for Remote Agent Controller, however the current name for this technology is *Agent Controller*.

The Agent Controller is a server that enables client applications to interact with agents under its domain: <http://help.eclipse.org/help32/index.jsp?topic=/org.eclipse.tptp.platform.agentcontroller.doc.user/tasks/rac/tworkwac.html>

A Generic Log Adapter (GLA) transforms proprietary log and trace data to the Common Base Event format (<http://www.ibm.com/developerworks/library/specification/ws-cbe/>). The rationale for a Generic Log Adapter is that reading log files is messy and making parsers for all types of logs is not scalable and one tends to customize anyway. A GLA can act as an agent of an Agent Controller so that clients can monitor remote application logs.

More information about Agent Controller and Generic Log Adapter can be found on [www.eclipse.org/tptp/](http://www.eclipse.org/tptp/).

The RAC Connector can read data from and write data to RAC:

- In **AddOnly** mode the RAC Connector publishes Common Base Events through a Logging Agent. In this mode, the RAC Connector uses an instance of the "CBE Generator Function Component" on page 347 to help convert the input schema attributes into a single Common Base Event object.

It registers as an agent within the local Agent Controller and sends it the Common Base Event objects, which it receives from the AssemblyLine.

The RAC Connector does not require the local Agent Controller to be running at the time it is initializing. As soon as the local Agent Controller is launched, the Logging Agent is registered and gets ready to be monitored by clients.

The important point is that the Connector will not report an error if the local Agent Controller is not active.

The Connector will not complain even if there is no Agent Controller installation on the local machine. Of course, no Logging Agent will be registered then.

- In **Iterator** mode the RAC Connector acts as a client of a remote Logging Agent.

As such, it contacts the Agent Controller on the remote machine, obtains a handle to a certain Logging Agent and starts receiving log data in the form of Common Base Event objects.

If the remote Agent Controller goes down the Connector hangs waiting for a response from the Agent Controller (this is due to the current client library realization). – thus any reconnect logic cannot be used.

The Connector uses an internal queue to store the incoming Common Base Events (CBEs). As a result the Connector can keep fetching CBEs even after the Agent Controller has gone down because the queue could still have events in it. Due to restrictions caused by the Agent Controller client library, the Connector can not process Common Base Event objects, which when serialized as XML are larger than 8Kb. If a data portion larger than 8Kb arrives, the Connector will not process any more events and will wait until the remote Logging Agent dies. This is a limitation of the client library implementation.

On termination, the Connector detaches from the remote agent. If this procedure is skipped for some reason (for example the JVM is killed), no other client will be able to monitor the agent. Moreover, the agent will still think that it is being monitored.

For example, if one runs the Connector from the Config Editor and manually stops the AssemblyLine, the Connector will not have a chance to detach from the Logging Agent. So if the Connector is run again, it will not receive any data from the agent, because the Agent Controller (and the agent) thinks that the agent is already being monitored.

Only one client can monitor a Logging Agent at a given time, so no two RAC Connectors in Iterator mode should be pointed at the same agent at the same time.

## Configuration

The Connector's title, shown in the Configuration panel is "RAC Connector". Parameters are:

### Remote Logging Agent Name

Used in Iterator Mode.

The name of the remote Logging Agent to be monitored.

### Agent Controller Host

Used in Iterator Mode.

Host of the remote Agent Controller. Default value is "localhost".

### Agent Controller Port

Used in Iterator Mode.

Port of the remote Agent Controller. Default value is 10006.

### Receiving Queue Size

Used in Iterator Mode.

The size of the queue, where the received events are buffered before the Connector manages to read them. Default value is 1024.

### Wait For Dead Agent's Data

Used in Iterator Mode.

Timeout (in seconds) for each data reception after the remote agent dies. If this timeout expires, the agent's data is considered depleted and the Connector terminates. Default value is 5000.

### Logging Agent Name

Used in AddOnly Mode.

The name of the Logging Agent within the local Agent Controller. Default value is "tdi\_logging\_agent".

### Wait to be monitored

Used in AddOnly Mode.

Time to wait (in seconds) for the agent to be monitored before data is sent to RAC. If zero, waits forever. Default value is 0.

### Detailed log

When checked, additional log messages will be generated.

## Using the Connector

### AddOnly Mode

**Post-install Configuration for AddOnly Mode:** The AddOnly mode of the RAC Connector requires that the binaries of the Agent Controller (.dll, .so) are available to the dynamic library loader of the operating system. The preferred way to achieve this is to include the binaries folder of the Agent Controller in the PATH environment variable on Windows platforms, and in the LD\_LIBRARY\_PATH environment variable on Linux platforms. This can be done either globally or just for the process of the TDI Server. For example:

- On Windows: modify the PATH environment variable from "My Computer" -> "Properties" -> "Advanced" -> "Environment variables"; add the required path to the Agent Controller libraries.
- On Linux: add lines like the following in the startup scripts (ibmdisrv and ibmditk) after the PATH definition and before the startup line:

```
LD_LIBRARY_PATH=/AgentController/lib
export LD_LIBRARY_PATH
```

If you have LD\_LIBRARY\_PATH elements of your own, add these to the LD\_LIBRARY\_PATH definition.

When operating in AddOnly mode, the first RAC Connector on the TDI Server registers a Logging Agent with the local Agent Controller.

All Common Base Event objects received from the AssemblyLine, are serialized as XML and written to the Logging Agent. The Logging Agent stays operational as long as the master process of the TDI server is alive. During its lifetime it can be monitored by clients even if the Connector which registered it has already closed. When the TDI server stops (or crashes), however, the Agent Controller (RAC) terminates the TDI Logging Agent's registration.

The Connector will wait a specified amount of time for a monitoring client to arrive before starting to write data to the Logging Agent. In particular, it can wait forever. This is specified by the **Wait to be monitored** Connector parameter. When a client starts monitoring the agent, the agent starts transferring data to the Agent Controller. The Agent Controller then sends the data to the client.

Waiting happens before each Connector write attempt.

If the waiting time expires and there is still no monitoring client, the Connector throws an Exception. However, if a client starts monitoring the agent while the Connector is waiting, the waiting is interrupted and the agent starts transferring data to the Agent Controller.

Depending on the **Wait to be monitored** Connector parameter value the Connector could potentially wait indefinitely for a client to start monitoring the agent. This would cause the entire AssemblyLine to block indefinitely. Precisely for this reason the following Connector method is available to you:

```
public boolean isLogging();
```

This method returns *true* if there is a client monitoring/listening for data from this Connector and *false* otherwise. This method is accessible through JavaScript and can be invoked on the Connector object (that is, `thisConnector.isLogging()`.)

You can use this method in order to detect whether the Connector will block when the AssemblyLine execution reaches the Connector. If blocking is not desirable, but losing data is unacceptable, then you could implement a solution which temporarily stores the data into a queue (possibly the TDI Memory Queue) when the `isLogging()` method returns false.

## Iterator Mode

In Iterator mode the RAC Connector acts as a client of a remote Agent Controller. It connects to the Agent Controller to obtain a handle to the Logging Agent, whose name is specified in the Connector's configuration. After that the Connector starts monitoring the Logging Agent. During the monitoring, the Connector receives data produced by the Logging Agent.

Data reception is handled asynchronously by the Agent Controller client library and queued there. The Connector is notified when data reception occurs, and when the Connector reads from the queue a buffer is received with the incoming binary data. The queue is blocking, so the Connector will wait if no data is available and the data processor will wait if there is no free space in the queue.

The received binary data contains a `CommonBaseEvent` object serialized as XML in UTF-8 encoding. In addition, the `CommonBaseEvent` is decoded from the buffer and made available to the Connector in the Input Map.

If there is no active agent with the specified name when the Connector contacts the Agent Controller, the Connector waits until such an agent is registered.

If at some point the agent gets deregistered (while the Connector is listening for events), the Connector will wait for another agent with the same name to appear. Essentially the Connector never stops unless its connection to the Agent Controller fails.

The Connector exposes a method, which provides access to the Common Base Event object obtained by the Connector on the current AssemblyLine iteration (the last event, processed by the 'getNextEntry' method of the Connector):

```
public CommonBaseEvent getCurrentCbeObject();
```

### **Schema**

The connector internally uses the "CBE Generator Function Component" on page 347, and uses that particular FC's schema.

### **See Also**

"GLA Connector" on page 80



---

## RDBMS Changelog Connector

The RDBMS Changelog Connector enables IBM Tivoli Directory Integrator to detect when changes have occurred in specific RDBMS tables. Currently, setup scenarios are provided for tables in either Oracle or DB2 databases.

RDBMS's have no common mechanism to inform the outside world of the changes that have been taking place on any selected database table. To address this shortcoming, IBM Tivoli Directory Integrator assumes that some RDBMS mechanism (such as a trigger, stored procedures or other) is able to maintain a separate change table containing one record per modified record in the target table. Sequence numbers are also maintained by the same mechanism.

Similar to an LDAP Changelog Connector, the RDBMS Changelog Connector communicates with the change table that is structured in a specific format that enables the connector to propagate changes to other systems. The format is the same that IBM DB2 Information Integrator (version 8) uses, providing IBM Tivoli Directory Integrator users with the option to use DB2II to create such tables, or create the tables in some other manner. The RDBMS Changelog Connector keeps track of a sequence number so that it only reports changes since the last iteration through the change table.

The RDBMS Changelog Connector uses JDBC to connect to a specific RDBMS table. See the "JDBC Connector" on page 103 for more information about JDBC driver issues.

The RDBMS Changelog Connector only operates in Iterator mode.

This connector supports Delta Tagging at the Entry level only.

The RDBMS Changelog Connector reads specific fields to determine new changes in the change table (see " "Change table format" on page 189"). The RDBMS Changelog Connector reads the next change table record, or discovers the first change table record. If the RDBMS Changelog Connector finds no data in the change table, the RDBMS Changelog Connector checks whether it has exceeded the maximum wait time. If the RDBMS Changelog Connector has exceeded the maximum wait time, the RDBMS Changelog Connector returns **null** to signal end of the iteration. If the RDBMS Changelog Connector finds no data in the change table, and has not exceeded the maximum wait time, the RDBMS Changelog Connector waits for a specific number of seconds (**Poll Interval**), then reads the next change table record.

If the Connector returns data in the change table, the RDBMS Changelog Connector increments and updates the **nextchangelog** number in the User Property Store (an area in the System Store tailored for this type of persistent information).

For each Entry returned, control information (counters, operation, time/date) is moved into Entry properties. All non-control information fields in the change table are copied as is to the Entry as attributes. The Entry objects operation (as returned by **getOperation**) is set to the corresponding changelog operation (Add, Delete or Modify).

During Checkpoint of the RDBMS Changelog Connector in Iterator mode, the change number will be saved as Connector Restart Info.

This Connector in principle can handle secure connections using the SSL protocol; but it may require driver specific configuration steps in order to set up the SSL support. Refer to manufacturer's driver documentation for details.

## Configuration

The Connector needs the following parameters:

**JDBC URL**

See documentation for your JDBC provider. It is called JDBC URL in the IBM Tivoli Directory Integrator Config Editor.

**Username**

This is the user ID with which the Connector signs on to the RDBMS. Only the tables available to this user are shown.

**Password**

The password for the user.

**Schema**

The schema (that is, the owner) of the table of the database that you want to use. If left blank, the value of the **Username** parameter is used.

**JDBC Driver**

The JDBC driver class name. The default value for this parameter is `com.ibm.db2.jcc.DB2Driver`.

**Table Name**

The table or view to operate on.

**Remove Processed Rows**

Select to remove all previously processed table rows before the next poll attempt.

**Iterator State Key**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

**State Key Persistence**

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and choices are:

**After Read**

Updates the System Store when you read an entry from the RDBMS Server change log, before you continue with the rest of the AssemblyLine.

**End of Cycle**

Updates the System Store when all Connectors and other components in the AssemblyLine have been evaluated and executed.

**Manual**

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the RDBMS Changelog Connector's `saveStateKey()` method, somewhere in your AssemblyLine.

**Sleep Interval**

Specifies the time (in seconds) that IBM Tivoli Directory Integrator waits between polls of the change table.

**Timeout**

Specifies the time (in seconds) to wait for new changes. A value of **0** (zero) causes the Connector to wait indefinitely.

**Commit**

Controls when database transactions are committed. Options are:

- **After every database operation**
- **On Connector close**
- **Manual**

**Manual** means user must call `commit()`.

## Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Change table format

This example change table captures the changes from a table containing the fields NAME and EMAIL. Elements in bold are common for all Changelog table. The syntax for this example is for Oracle.

**IBMSNAP\_COMMITSEQ** is used as our changelog-nr.

**IBMSNAP\_OPERATION** takes on of the values I (Insert), U (Updated) or D (Deleted).

```
CREATE TABLE "SYSTEM"."CCDCHANGELOG"
(
IBMSNAP_COMMITSEQ RAW(10) NOT NULL,
IBMSNAP_INTENTSEQ RAW(10) NOT NULL,
IBMSNAP_OPERATION CHAR(1) NOT NULL,
IBMSNAP_LOGMARKER DATE NOT NULL,
NAME VARCHAR2 ( 80 ) NOT NULL,
EMAIL VARCHAR2 ( 80 )
)#
```

The RDBMS changelog connector does not work if the **ibmsnap\_commitseq** column name used internally in the connector does not match exactly with the actual column in the database. This is true only when case-sensitivity is turned on for data objects in the Database the RDBMS changelog connector is iterating on.

To handle this the column name is externalized as a connector configuration parameter. This provides the DBA an easy way to set **ibmsnap\_commitseq** with the same case as used in his Database table. However, this parameter is not visible in connector config tab. To configure this parameter, you will have to set this manually in the *before initialize* hooks of the RDBMS changelog connector. This will enable multiple RDBMS changelog connectors to have their own copy of the column name value set for the change table the connector iterates on. For example,

```
myConn.connector.setParam("rdbms.chlog.col","IBMSNAP_COMMITSEQ");
```

sets the name of the **ibmsnap\_commitseq** column to literally, **IBMSNAP\_COMMITSEQ**. The default is lowercase otherwise.

## Creating change tables in DB2

The following example creates triggers in a DB2 database to maintain the change table as described previous:

```
connect to your_username
```

```
drop table email
drop table ccdemail
```

```
create table email ( \
  name varchar(80), \
  email varchar(80) \
)
```

```
create table ccdemail ( \
  ibmsnap_commitseq integer, \
  ibmsnap_intentseq integer, \
  ibmsnap_logmarker date, \
  ibmsnap_operation char, \
  name varchar(80), \
  email varchar(80) \
)
```

```
drop sequence ccdemail_seq
create sequence ccdemail_seq
```

```
create trigger t_email_ins after insert on email referencing new as n \
```

```

for each row mode db2sql \
  INSERT INTO your_username.ccdemail VALUES (nextval for ccdemail_seq, 0,
  CURRENT_DATE, 'I', n.name, n.email )

create trigger t_email_del after delete on email referencing old as n \
for each row mode db2sql \
  INSERT INTO your_username.ccdemail VALUES (nextval for ccdemail_seq, 0,
  CURRENT_DATE, 'D', n.name, n.email )

create trigger t_email_upd after update on email referencing new as n \
for each row mode db2sql \
  INSERT INTO your_username.ccdemail VALUES (nextval for ccdemail_seq, 0,
  CURRENT_DATE, 'U', n.name, n.email )

```

## Creating change tables in Oracle

Given that your username is "ORAIID", then

```

-- create source email table in Oracle.
---This will be the table that the RDBMS changelog connector will detect changes on.
CREATE TABLE ORAIID.EMAIL
(
  NAME VARCHAR2(80),
  EMAIL VARCHAR2(80)
);
-- Sequence generators used for Intentseq and commitseq
CREATE SEQUENCE ORAIID.SGENERATOR001
MINVALUE 100 INCREMENT BY 1 ORDER;

CREATE SEQUENCE ORAIID.SGENERATOR002
MINVALUE 100 INCREMENT BY 1 ORDER;

-- create change table and index for email table
CREATE TABLE ORAIID.CCDEMAIL
(
  IBMSNAP_COMMITSEQ RAW(10) NULL,
  IBMSNAP_INTENTSEQ RAW(10) NOT NULL,
  IBMSNAP_OPERATION CHAR(1) NOT NULL,
  IBMSNAP_LOGMARKER DATE NOT NULL,
  NAME ( 80 ),
  EMAIL ( 80 )
);

CREATE UNIQUE INDEX ORAIID.IXCCDEMAIL ON ORAIID.CCDEMAIL
(
  IBMSNAP_INTENTSEQ
);

-- create TRIGGER to capture INSERTs into email
CREATE TRIGGER ORAIID.EMAIL_INS_TRIG
AFTER INSERT ON ORAIID.EMAIL
FOR EACH ROW BEGIN INSERT INTO ORAIID.CCDEMAIL
( NAME,
  EMAIL,
  IBMSNAP_COMMITSEQ,
  IBMSNAP_INTENTSEQ,
  IBMSNAP_OPERATION,
  IBMSNAP_LOGMARKER )
VALUES (
  :NEW.NAME,
  :NEW.EMAIL,
  NULL,
  LPAD(TO_CHAR(ORAIID.SGENERATOR002.NEXTVAL),20,'0'),
  'I',
  SYSDATE);END;

```

```

-- create TRIGGER to capture DELETE ops on email
CREATE TRIGGER ORAID.EMAIL_DEL_TRIG
AFTER DELETE ON ORAID.EMAIL
FOR EACH ROW BEGIN INSERT INTO ORAID.CCDEMAIL
( NAME,
  EMAIL,
  IBMSNAP_COMMITSEQ,
  IBMSNAP_INTENTSEQ,
  IBMSNAP_OPERATION,
  IBMSNAP_LOGMARKER)
VALUES
( :OLD.NAME,
  :OLD.EMAIL,
  NULL,
  LPAD(TO_CHAR(ORAID.SGENERATOR002.NEXTVAL),20,'0'),
  'D',
  SYSDATE);END;

```

## Creating Change table and triggers in MS SQL

```

-- Source table msid.email.
-- This will be the table that the RDBMS changelog connector will detect changes on.
CREATE TABLE msid.email
(
  NAME  VARCHAR (80),
  EMAIL VARCHAR (80)
)#

-- CCD table to capture changes. The RDBMS changelog connector uses the CCD table to capture
-- all the changes in the source table. This table needs to be created in the following format.
CREATE TABLE msid.ccdemail
(
  IBMSNAP_MSTMSTMP timestamp,
  IBMSNAP_COMMITSEQ  BINARY(10)  NOT NULL,
  IBMSNAP_INTENTSEQ  BINARY(10)  NOT NULL,
  IBMSNAP_OPERATION  CHAR(1)     NOT NULL,
  IBMSNAP_LOGMARKER  DATETIME    NOT NULL,
  NAME  VARCHAR (80),
  EMAIL VARCHAR (80)
)#

```

You also need to create triggers to capture the insert, update and delete operations performed on the email table.

```

CREATE TRIGGER msid.email_ins_trig ON msid.email
FOR INSERT AS
BEGIN
  INSERT INTO msid.ccdemail
(NAME,
  EMAIL,
  IBMSNAP_COMMITSEQ,
  IBMSNAP_INTENTSEQ,
  IBMSNAP_OPERATION,
  IBMSNAP_LOGMARKER )
SELECT
  NAME,
  EMAIL,
  @@DBTS,
  @@DBTS,
  'I',
  GETDATE() FROM inserted
END;#

```

**Note:** : @@DBTS returns the value of the current timestamp data type for the current database. This timestamp is guaranteed to be unique in the database.

```

-- creating DELETE trigger to capture delete operations on email table
CREATE TRIGGER msid.email_del_trig ON msid.email
FOR DELETE AS
BEGIN
    INSERT INTO msid.ccdemail
    (
        NAME,
        EMAIL,
        IBMSNAP_COMMITSEQ,
        IBMSNAP_INTENTSEQ,
        IBMSNAP_OPERATION,
        IBMSNAP_LOGMARKER
    )
    SELECT
        NAME,
        EMAIL,
        @@DBTS,
        @@DBTS,
        'D',
        GETDATE() FROM deleted
END;#

```

```

-- creating UPDATE trigger to capture update operations on email table
CREATE TRIGGER msid.email_upd_trig ON msid.email
FOR UPDATE AS
BEGIN
    DECLARE @COUNTER INT
    SELECT @COUNTER=COUNT(*) FROM deleted
    IF @COUNTER>1
    BEGIN
        DECLARE @NAME VARCHAR (80)
        DECLARE @EMAIL VARCHAR (80)
        DECLARE insertedrows CURSOR FOR SELECT * FROM inserted
        OPEN insertedrows
        WHILE 1=1 BEGIN
            FETCH insertedrows INTO
            @NAME,
            @EMAIL
            IF @@fetch_status<>0 BREAK
            ELSE INSERT INTO msid.ccdemail
            (
                NAME,
                EMAIL,
                IBMSNAP_COMMITSEQ,
                IBMSNAP_INTENTSEQ,
                IBMSNAP_OPERATION,
                IBMSNAP_LOGMARKER
            )
            VALUES
            (
                @NAME,
                @EMAIL,
                @@DBTS,
                @@DBTS,
                'U',
                GETDATE()
            )
        END
        DEALLOCATE insertedrows
    END ELSE INSERT INTO msid.ccdemail(
    NAME,
    EMAIL,
    IBMSNAP_COMMITSEQ,
    IBMSNAP_INTENTSEQ,
    IBMSNAP_OPERATION,
    IBMSNAP_LOGMARKER
    )

```

```

SELECT
  I.NAME,
  I.EMAIL,
  @@DBTS,
  @@DBTS,
  'U',
  GETDATE() FROM inserted I
END;#

```

## Creating change table and triggers in Informix

-- Create Source table infxid.email. This will be the table that the RDBMS changelog connector will detect changes on.

```

CREATE TABLE infxid.email
(
  NAME VARCHAR(80),
  EMAIL VARCHAR(80),
)#

```

-- create ccdemail table to capture DML operations on email table

```

CREATE TABLE "infxid"."ccdemail"
(
  IBMSNAP_COMMITSEQ CHAR(10) NOT NULL,
  IBMSNAP_INTENTSEQ CHAR(10) NOT NULL,
  IBMSNAP_OPERATION CHAR(1) NOT NULL,
  IBMSNAP_LOGMARKER DATETIME YEAR TO FRACTION(5) NOT NULL,
  NAME VARCHAR(80),
  EMAIL VARCHAR(80)
)#

```

-- create an additional table (ibmsnap\_seqtable) for processing commitseq and intentseq.

```

CREATE TABLE "infxid"."ibmsnap_seqtable"
(SEQ INTEGER NOT NULL,
  HEXREP CHAR(128)
)#

```

-- insert values into ibmsnap\_seqtable. This example below shows how to insert a hex value

```

INSERT INTO ASN.IBMSNAP_SEQTABLE VALUES (1000000000,
X'0102030405060708090A0B0C0D0E0F101112131415161718191A1B1C1D1E1F202122232425262728292A2B2C2D2E2F303132333435363738393A3B3C3D3E3F404142434445464748495051525354555657585960616263646566676869707172737475767778798081828384858687888990919293949596979899A0A1A2A3A4A5A6A7A8A9B0B1B2B3B4B5B6B7B8B9C0C1C2C3C4C5C6C7C8C9D0D1D2D3D4D5D6D7D8D9E0E1E2E3E4E5E6E7E8E9F0F1F2F3F4F5F6F7F8F9

```

-- procedure to capture INSERTs into email table

```

CREATE PROCEDURE infxid."email_ins_proc"
(
  NNAME VARCHAR(80),
  NEMAIL VARCHAR(80))
DEFINE VARHEX CHAR(128);
DEFINE I1 INTEGER;
DEFINE I2 INTEGER;
DEFINE X1 INTEGER;
DEFINE X2 INTEGER;
DEFINE X3 INTEGER;
DEFINE X4 INTEGER;
DEFINE Y1 INTEGER;
DEFINE Y2 INTEGER;
DEFINE Y3 INTEGER;
DEFINE Y4 INTEGER;
DEFINE NEWSYNCH CHAR(10);
SELECT HEXREP
  INTO VARHEX
  FROM "infxid"."ibmsnap_seqtable";
LET X1 = I1 / 268435456;
LET X2 = I1 / 2097152;
LET X3 = I1 / 16384;
LET X4 = I1 / 128;
LET Y1 = I2 / 268435456;
LET Y2 = I2 / 2097152;
LET Y3 = I2 / 16384;
LET Y4 = I2 / 128;

```

```

LET NEWSYNCH =
SUBSTR(VARHEX , MOD( X1, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( X2, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( X3, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( X4, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( I1, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y1, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y2, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y3, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y4, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( I2, 128 ) + 1 , 1 );
INSERT INTO "infxid"."ccdemail"
(NAME,
EMAIL,
IBMSNAP_COMMITSEQ,
IBMSNAP_INTENTSEQ,
IBMSNAP_OPERATION,
IBMSNAP_LOGMARKER )
VALUES
(NNAME,
NEMAIL,
NEWSYNCH,
NEWSYNCH,
'I',
CURRENT YEAR TO FRACTION(5));END PROCEDURE;#

```

```

-- now create the trigger for INSERTs into ccdemail
CREATE TRIGGER "infxid"."email_ins_trig"
INSERT ON "infxid"."email"
REFERENCING NEW AS NEW FOR EACH ROW( EXECUTE PROCEDURE
"infxid"."email_ins_proc"
( NEW.NAME,
NEW.VARCHAR
) ); #

```

```

-- create procedure to capture DELETes on email table
CREATE PROCEDURE "infxid"."email_del_proc"
(
ONAME VARCHAR(80),
OEMAIL VARCHAR(80)
)
DEFINE VARHEX CHAR(128);
DEFINE I1 INTEGER;
DEFINE I2 INTEGER;
DEFINE X1 INTEGER;
DEFINE X2 INTEGER;
DEFINE X3 INTEGER;
DEFINE X4 INTEGER;
DEFINE Y1 INTEGER;
DEFINE Y2 INTEGER;
DEFINE Y3 INTEGER;
DEFINE Y4 INTEGER;
DEFINE NEWSYNCH CHAR(10);
SELECT HEXREP
INTO VARHEX
FROM "infxid"."ibmsnap_seqtable";
LET X1 = I1 / 268435456;
LET X2 = I1 / 2097152;
LET X3 = I1 / 16384;
LET X4 = I1 / 128;
LET Y1 = I2 / 268435456;
LET Y2 = I2 / 2097152;
LET Y3 = I2 / 16384;
LET Y4 = I2 / 128;
LET NEWSYNCH =

```



```

SUBSTR(VARHEX , MOD( X1, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( X2, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( X3, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( X4, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( I1, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( Y1, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( Y2, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( Y3, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( Y4, 128 ) + 1 , 1 ) ||
SUBSTR(VARHEX , MOD( I2, 128 ) + 1 , 1 );
INSERT INTO "infxid"."ccdemail"
(NAME,
EMAIL,
IBMSNAP_COMMITSEQ,
IBMSNAP_INTENTSEQ,
IBMSNAP_OPERATION,
IBMSNAP_LOGMARKER )
VALUES
(ONAME,
OEMAIL,
NEWSYNCH,
NEWSYNCH,
'D',
CURRENT YEAR TO FRACTION(5));END PROCEDURE;#

-- create DELETE trigger
CREATE TRIGGER "infxid"."email_del_trig"
DELETE ON "infxid"."email"
REFERENCING OLD AS OLD FOR EACH ROW( EXECUTE PROCEDURE
"infxid"."email_del_proc"
(OLD.NAME,
OLD.EMAIL,
) ); #

-- create PROCEDURE to capture updates
CREATE PROCEDURE "infxid"."email_upd_proc"
(
NNAME VARCHAR(80),
NEMAIL VARCHAR(80),
)
DEFINE VARHEX CHAR(128);
DEFINE I1 INTEGER;
DEFINE I2 INTEGER;
DEFINE X1 INTEGER;
DEFINE X2 INTEGER;
DEFINE X3 INTEGER;
DEFINE X4 INTEGER;
DEFINE Y1 INTEGER;
DEFINE Y2 INTEGER;
DEFINE Y3 INTEGER;
DEFINE Y4 INTEGER;
DEFINE NEWSYNCH CHAR(10);
SELECT HEXREP
INTO VARHEX
FROM "infxid"."ibmsnap_seqtable";
LET X1 = I1 / 268435456;
LET X2 = I1 / 2097152;
LET X3 = I1 / 16384;
LET X4 = I1 / 128;
LET Y1 = I2 / 268435456;
LET Y2 = I2 / 2097152;
LET Y3 = I2 / 16384;
LET Y4 = I2 / 128;
LET NEWSYNCH =
SUBSTR(VARHEX , MOD( X1, 128 ) + 1 , 1 ) ||

```

```

SUBSTR(VARHEX , MOD( X2, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( X3, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( X4, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( I1, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y1, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y2, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y3, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( Y4, 128 ) + 1 , 1 )
SUBSTR(VARHEX , MOD( I2, 128 ) + 1 , 1 );
INSERT INTO "infxid"."ccdemail"
(NAME,
EMAIL,
IBMSNAP_COMMITSEQ,
IBMSNAP_INTENTSEQ,
IBMSNAP_OPERATION,
IBMSNAP_LOGMARKER)
VALUES
(NNAME,
NEMAIL,
'U',
CURRENT YEAR TO FRACTION(5));END PROCEDURE;#

```

```

-- create TRIGGER to capture UPDATES
CREATE TRIGGER "infxid"."email_upd_trig"
UPDATE ON "infxid"."email"
REFERENCING NEW AS NEW OLD AS OLD FOR EACH ROW( EXECUTE PROCEDURE
"infxid"."email_upd_proc"
(NEW.NAME,
NEW.EMAIL,
) ); #

```

## Creating change table and trigger for SYBASE

```

-- Create Source table sybid.email.
-- This will be the table that the RDBMS changelog connector will detect changes on.
CREATE TABLE sybid.email
(
NAME VARCHAR (80),
EMAIL VARCHAR (80)
)#

```

```

-- Create CCD table to captures changes on email table
CREATE TABLE sybid.CCDEMAIL
(
IBMSNAP_SYBTMSTMP timestamp,
IBMSNAP_COMMITSEQ BINARY(10) NOT NULL,
IBMSNAP_INTENTSEQ BINARY(10) NOT NULL,
IBMSNAP_OPERATION CHAR(1) NOT NULL,
IBMSNAP_LOGMARKER DATETIME NOT NULL,
NAME VARCHAR(80),
EMAIL VARCHAR(80)
)#

```

```

-- Create TRIGGER to capture INSERTs on email table
CREATE TRIGGER sybid.EMAIL_INS_TRIG ON sybid.EMAIL
FOR INSERT AS
BEGIN
INSERT INTO sybid.CCDEMAIL
(NAME,
EMAIL,
IBMSNAP_COMMITSEQ,
IBMSNAP_INTENTSEQ,
IBMSNAP_OPERATION,
IBMSNAP_LOGMARKER )
SELECT
NAME,
EMAIL,

```

```

@@DBTS,
  @@DBTS,
  'I',
  GETDATE() FROM inserted
END;#

```

NOTE: @@DBTS is a special database variable that yields the next database timestamp value

```

-- create TRIGGER to captures DELETE ops on EMAIL table
CREATE TRIGGER sybid.EMAIL_DEL_TRIG ON sybid.EMAIL
FOR DELETE AS
BEGIN
  INSERT INTO sybid.CCDEMAIL
  (
    NAME,
    EMAIL,
    IBMSNAP_COMMITSEQ,
    IBMSNAP_INTENTSEQ,
    IBMSNAP_OPERATION,
    IBMSNAP_LOGMARKER
  )
  SELECT
    NAME,
    EMAIL,
    @@DBTS,
    @@DBTS,
    'D',
    GETDATE() FROM deleted
END;#

```

```

-- create TRIGGER to capture UPDATES on email
CREATE TRIGGER sybid.EMAIL_UPD_TRIG ON sybid.EMAIL
FOR UPDATE AS
BEGIN
  DECLARE @COUNTER INT
  SELECT @COUNTER=COUNT(*) FROM deleted
  IF @COUNTER>1
  BEGIN
    DECLARE @NAME VARCHAR ( 80 )
    DECLARE @EMAIL VARCHAR ( 80 )
    DECLARE insertedrows CURSOR FOR SELECT * FROM inserted
    OPEN insertedrows
    WHILE 1=1 BEGIN
      FETCH insertedrows INTO
      @NAME,
      @EMAIL,
      IF @@fetch_status<>0 BREAK
      ELSE INSERT INTO sybid.CCDEMAIL
      (
        NAME,
        EMAIL,
        IBMSNAP_COMMITSEQ,
        IBMSNAP_INTENTSEQ,
        IBMSNAP_OPERATION,
        IBMSNAP_LOGMARKER
      )
      VALUES
      (
        @NAME,
        @EMAIL,
        @@DBTS,
        @@DBTS,
        'U',
        GETDATE()
      )
    END
    DEALLOCATE insertedrows
  END

```

```
END ELSE INSERT INTO sybid.CCDEMAIL(  
  NAME,  
  EMAIL,  
  IBMSNAP_COMMITSEQ,  
  IBMSNAP_INTENTSEQ,  
  IBMSNAP_OPERATION,  
  IBMSNAP_LOGMARKER  
)  
SELECT  
  I.NAME,  
  I.EMAIL,  
  @@DBTS,  
  @@DBTS,  
  'U',  
  GETDATE() FROM inserted I  
END;#
```

---

## runtime-provided Connector

A runtime provided Connector is a Connector Interface that is provided at runtime. When an AssemblyLine is started by an EventHandler or from a script, you can supply only one Connector to the AssemblyLine as a parameter. The Connector is used for those AssemblyLine Connectors configured as type **runtime provided**. You can use the supplied Connector several times in the AssemblyLine.

The following is an example of how to use a runtime provided Connector from an EventHandler:

```
var myConnector = system.getConnector ("ibmdi.FileSystem");
myConnector.setParam ("filePath", "mypath.txt");
myConnector.initialize ( null );
// Start the AssemblyLine
var al = main.startAL ( "AssemblyLine1", myConnector );
```

The following is an example that includes an initial working entry:

```
var myConnector = system.getConnector ("ibmdi.FileSystem");
myConnector.setParam ("filePath", "mypath.txt");
myConnector.initialize ( null );
var entry = system.newEntry();
entry.setAttribute ("cn", "My Name");
entry.setAttribute ("mail", "(my.name@dot.com)");
var al = main.startAL ( "AssemblyLine2", myConnector, entry );
```

## Configuration

The Connector might need parameters, but the names and values of these parameters depend on the actual Connector.

## See also

"IBM Tivoli Directory Integrator concepts – The AssemblyLine" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.



---

## Script Connector

The Script Connector enables you to write your own Connector in JavaScript.

A Script Connector must implement a few functions to operate. If you plan to use it for iteration purposes only (for example, reading, not searching or updating), you can operate with two functions only. If you plan to use it as a fully qualified Connector, you must implement all functions. The functions do not use parameters. Passing data between the hosting Connector and the script is enabled by using predefined objects. One of these predefined objects is the **result** object, which is used to communicate status information. Upon entry in either function, the **status** field is set to **normal**, which causes the hosting Connector to continue calls. Signaling **end-of-input** or **error** is done by setting the **status** and **message** fields in this object. Two other script objects are defined upon function entry, the **entry** object and the **search** object.

**Note:** When you modify a Script Connector or Parser, the script gets copied from the Library where it is stored, into your configuration file. This enables you to customize the script, but with the caveat that new versions are not known to your AssemblyLine.

One workaround is to remove the old Script Connector from the AssemblyLine and reintroduce it. Remember to copy over code from your hooks.

## Predefined script objects

### The result object

**setStatus (code)**

- 0 - End of Input
- 1 - Status OK
- 2 - Error

**setMessage (text)**

Error message.

### The config object

This object gives you access to the configuration of this AL component, and its Input and Output schema — note that the `getSchema()` method of this object has a single Boolean parameter: *true* means to return the Input Schema while *false* gets *you* the Output Schema.

### The entry object

The **entry** object corresponds to the **conn** Entry for a Connector (or Function, when scripting an FC.)

See “The Entry object” on page 436 for more details.

### The search object

The **search** object gives you access to the `searchCriteria` object (built based on Link Criteria settings.) See “The Search (criteria) object” on page 438 for more details.

## Functions

The following functions can be implemented by the Script Connector. Even though some functions might never be called, it is recommended that you insert the functions with an error-signaling code that notifies the caller that the function is unsupported.

### **selectEntries**

This function is called to prepare the Connector for sequential read. When this function is called it is typically because the Connector is used as an Iterator in an AssemblyLine.

### getNextEntry

This function must populate the Entry object with attributes and values from the next entry in the input set. When the Connector has no more entries to return, it must use the **result** object to signal end-of-input back to the caller.

### findEntry

The **findEntry** function is called to find an entry in the connected system that matches the criteria specified in the **search** object. If the Connector finds a single matching entry, then the Connector populates the **entry** object. If no entries are found, the Connector must set the error code in the **result** object to signal a failure to find the entry. If more than one entry is found, then the Connector might populate the array of duplicate entries. Otherwise, the same procedure is followed as when there are no entries found.

### modEntry

This function is called to modify an existing entry in the connected system. The new entry data is given by the **entry** object, and the **search** object specifies which entry to modify. Some Connectors might silently ignore the **search** object, and use the **entry** object to determine which entry to modify.

### putEntry

This function adds the **entry** object to the connected system.

### deleteEntry

This function is called to delete an existing entry in the connected system. The **search** object specifies which entry to delete. Some Connectors might silently ignore the **search** object, and use the **entry** object to determine which entry to delete.

### queryReply

This function is called when the Connector is used in Call/Reply mode.

### querySchema

This function is used to discover schema for a connection. If implemented, a vector of **Entry** objects is returned for each column/attribute it discovered. The querySchema function is only called when you "Open/Query" in the attribute map (not when you click the quick discovery button).

In order to support Schema discovery your Script Connector or -FC could contain code like this:

```
function querySchema() {
    config.getSchema(true).newItem("name-in");
    config.getSchema(true).newItem("address-in");
    config.getSchema(false).newItem("name-out");
    config.getSchema(false).newItem("address-out");
}
```

This would create two items in the input and output schemas respectively. Check the SchemaConfig and SchemaItemConfig API (in the Javadocs) for more details.

According to the various modes, these are the minimum required functions you need to implement:

Table 8. Required functions

| Mode     | Function you must implement       |
|----------|-----------------------------------|
| Iterator | selectEntries()<br>getNextEntry() |
| AddOnly  | putEntry()                        |
| Lookup   | findEntry()                       |
| Delete   | findEntry()<br>deleteEntry()      |



Table 8. Required functions (continued)

| Mode      | Function you must implement             |
|-----------|---|
| Update    | findEntry()<br>putEntry()<br>modEntry() |
| CallReply | queryReply()                            |

## Configuration

The Connector needs the following parameters:

### External Files

If you want to include external script files at runtime, specify them here. Specify one file on each line. These files are started before your script.

### Include Global scripts

Include global scripts from the Script Library.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Script** This tab is where you can create your own script code.

## Examples

Navigate to the *root\_directory/examples/script\_connector* directory of your IBM Tivoli Directory Integrator installation.

## See also

“Script Parser” on page 305,

“Scripted FC” on page 345

“JavaScript Connector” in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.



---

## SNMP Connector

This Connector listens for SNMP traps sent on the network and returns an entry with the name and values for all elements in an SNMP PDU.

### Notes:

1. In Client mode, a request is retried 5 times with increasing intervals over a period of 13 seconds. Timeout occurs if no answer is received.
2. If you want to send SNMP Traps, the `system.snmpTrap()` method is available.
3. The SNMP Connector does not support the Advanced Link Criteria (see "Advanced link criteria" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*).

## Configuration

The Connector needs the following parameters:

### Community String

Use `public` to test the Connector.

**Mode** Trap Listener or Client. The Client mode can use Connectors in AddOnly mode (SNMP Set), Lookup mode (SNMP Get) or Iterator mode (Walk).

Trap listener can only Iterate, listening to traps on the local host.

### SNMP Trap Port

Port in Trap mode. Unused in Client mode.

### Trap wait timeout

Timeout in Trap mode. The number of milliseconds to wait for the next Protocol Data Unit (PDU). If value is zero or less, the Connector waits forever.

### SNMP Host (for get)

Only used for Get in Client mode. Not used in Trap mode.

### SNMP Port

Client port (for client mode). Not used in Trap mode.

### SNMP Walk OID (iterate)

Used only in Client mode, Iterator Connector. Indicates the OID tree to walk.

### SNMP Version

The default version for get/walk is the Client mode. Unused in trap mode.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Note:** Link Criteria are treated differently for this Connector. In Lookup mode, the connector performs a get request returning the **oid/value** for the requested oid. The link criteria specifies **oid**, as well as **server**, **port** and **version**. An example link criterion might be "**oid**" = "1.1.1.1.1.1".

## Examples

Go to the `root_directory/examples/snmpTrap` directory of your IBM Tivoli Directory Integrator installation.



---

## SNMP Server Connector

The SNMP Server Connector supports SNMP v1. SNMP v2 is supported without the SNMP v2 authentication and encryption features.

The Connector does not support SNMP TRAP messages.

The SNMP Server Connector operates in server mode only. The transport protocol it uses is UDP and not TCP. UDP is an unreliable transport protocol, and SSL cannot run on top of an unreliable transport protocol. That is why the Connector cannot use SSL to protect the transport layer. The SNMP EventHandler can be run in single or multithreaded mode, depending on the value of the **network.mode** parameter. The Connector, on the other hand, works only in multi-threaded mode as the Connector in Server Mode framework requires.

The SNMP Server Connector (contrary to other Connectors in Server Mode) uses DatagramSockets. That is why there is no notion of connection. The SNMP Server Connector uses a single DatagramSocket which receives SNMP packets from many different SNMP managers on the network.

In the getNextClient() method, the socket blocks on the receive() method until an SNMP packet is received. Then, the Connector creates a new instance of itself, passes the received packet to the child Connector and returns the child Connector.

The getNextEntry() method extracts the SNMP request packet attributes and sets them in the *conn* Entry, ready for Input Attribute Mapping.

The replyEntry() method extracts the Attributes from the *conn* Entry and creates an SNMP response packet and returns it to the client; the *conn* Entry should be populated using Output Attribute Mapping.

The replyEntry() method uses the parent Connector's DatagramSocket to send back the response. Since the parent Connector's DatagramSocket is shared among all child Connectors the access to the DatagramSocket is synchronized.

## Connector Schema

The SNMP Server Connector makes the following Attributes available for Input Attribute Mapping:

### **snmp.operation**

java.lang.String object, which represents the SNMP operation invoked. The supported operation types are GET, GETNEXT and SET.

### **snmp.community**

Defines an access environment for a group of Network Management Systems (NMSs). NMSs within the community are said to exist within the same administrative domain. Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

### **snmp.remoteip**

IP address of the SNMP client (dot notation).

### **snmp.errorcode**

Indicates one of a number of errors and error types. Only the response operation sets this field. Other operations set this field to zero.

### **snmp.errorindex**

Associates an error with a particular object instance. Only the response operation sets this field. Other operations set this field to zero.

### **snmp.request-id**

Associates SNMP requests with responses.

**snmp.PDU**

Protocol Data Unit. SNMP PDUs contain a specific command (Get, Set, etc.) and operands that indicate the object instances involved in the transaction.

**snmp.oid**

OID is an address of a MIB structure, indicating a specific variable or attribute to be read or modified in the target system. A GET can contain a list of OIDs, while a SET can also include the corresponding values to be set for those variables in the target system. However, most SNMP deployments use only one OID per SNMP message.

**snmp.oidvalue**

Contains the corresponding value of one OID. This is a String representation.

**snmp.oidvalue.raw**

Contains the corresponding value of one OID. This is an Object representation.

## Configuration

The SNMP Server Connector uses the following parameters:

**UDP Port**

Specifies the UDP port on which the Connector (1) receives incoming SNMP request packets and from which (2) sends SNMP response packets. The default value is 161, which is the standard port for SNMP GET/SET operations.

**Verify Community**

Specifies the SNMP Community name. SNMP Community names serve as a weak form of authentication because devices that do not know the proper community name are precluded from SNMP operations.

If set, the Connector discards all messages not matching this community string. If blank, the Connector allows all community strings.

The default value is "public".

**Detailed Log**

If enabled, will generate detailed Log messages.

---

# TAM Connector

## Introduction

The IBM Tivoli Directory Integrator 6.1.1 Connector for Tivoli Access Manager enables the provisioning and managing of Tivoli Access Manager Users, Groups, Policies, Domains, SSO Resources, SSO Resource Groups and SSO User Credentials.

This component enables the provisioning and management of Tivoli Access Manager User accounts, Groups, Policies, Domains, SSO Resources, SSO Resource Groups, and SSO User Credentials to external applications (with respect to Tivoli Access Manager). The Connector uses the Tivoli Access Manager Java API.

The key features and benefits of the Connector are:

- Support for Create, Read, Update, and Delete operations for Tivoli Access Manager User accounts, Groups, Policies, Domains, SSO Resources, SSO Resource Groups, and SSO User Credentials.

**Note:** The Connector uses the TAM 6 Java API to manipulate the attributes of the targeted TAM objects. Therefore, this Connector can't support TAM 5.1 because of JRE support restrictions for the TAM 5.1 Runtime Environment (RTE). It supports TAM 6.0 only.

SSL communication with the TAM Server is supported.

## Connector Modes

The Connector supports the Lookup, Iterator, Update, AddOnly, and Delete modes. Refer to "Using the Connector" on page 211 for specific usage of the various modes.

## Configuration

Before attempting to use the connector in an AssemblyLine, Tivoli Access Manager version 6.0 must be installed on the target machine: The Tivoli Access Manager Java Runtime Environment (JRTE) must also be installed on the same machine as TDI.

### Configuring the Tivoli Access Manager Java Run Time

The Connector makes use of the Tivoli Access Manager Java API and therefore the Tivoli Access Manager Runtime for Java must be installed on the TDI machine. For information on how to install and configure Tivoli Access Manager Runtime for Java on the TDI machine, refer to the *Tivoli Access Manager Installation Guide*.

When entering the parameters to the configuration utility (**pdjrtecfg**):

- Check that both the policy server and registry server are running.
- Ensure that Tivoli Directory Integrator is not running.
- Specify the location of the TDI JRE directory. For example, on a Linux machine the default TDI JRE directory is:

```
/opt/IBM/IBMDirectoryIntegrator/jvm/jre
```

- Specify a configuration type of Full. For example, from the Policy\_Director/sbin directory, enter the following command (as one line):

```
pdjrtecfg -action config -host TAM_hostname -java_home  
"/opt/IBM/IBMDirectoryIntegrator/jvm/jre"
```

where *TAM\_hostname* is the name of the host where Tivoli Access Manager Policy Server is installed.

## Configuring secure communication to the Tivoli Access Manager policy server

To configure secure communication between TDI and Tivoli Access Manager policy server and authorization server, and for TDI to become an authorized Tivoli Access Manager Java application, run the `SvrSslCfg` utility on the TDI machine.

For example, from the `<TDI_install>/jvm/jre/bin` directory, enter the following command (as one line). This command must be run with the JRE IBM 1.5sr3 java executable:

```
java com.tivoli.pd.jcfg.SvrSslCfg -action config -admin_id sec_master
    -admin_pwd password -appsvr_id appsvr -mode remote -port 999
    -policysvr policy_svr:7135:1 -authzsvr auth_svr:7136:1 -cfg_file
    cfg_file_name -key_file keyfile_name -mode remote
```

For complete information on the `SvrSslCfg` utility, refer to the *Tivoli Access Manager Authorization Java Classes Developer Reference* (specifically *Appendix A*).

## Configuring the Connector

The TDI Connector for Tivoli Access Manager can be added directly into an assembly line. The following section lists the configuration parameters that are available.

### TAM ID

The Connector attempts to log on to Tivoli Access Manager with this user name and the password specified by the Password parameter. Default value: `sec_master`

### TAM Password

The value of this parameter is taken in account only when the parameter **TAM ID** is set to a non-blank value. It then specifies the password used for the logon operation. The default value is blank.

### Domain

Specifies the TAM Domain. The default is blank. Pressing the "Domains" button next to this parameter queries the TAM Server for a list of Domains, from which you can select the appropriate one. The Connector attempts to log on to Tivoli Access Manager with the **TAM ID** and **TAM Password** parameters.

### TAM Program Name

The name used by Tivoli Access Manager to identify this Connector. Default value: `IDI`

### TAM Configuration File

File pathname for the Tivoli Access Manager configuration file created by the `SvrSslCfg` configuration utility.

### Entry Type

Must be set to one of the following:

- User (specifying that the Connector operates with data structured by Tivoli Access Manager Users),
- Group (specifying that the Connector operates with data structured by Tivoli Access Manager Groups),
- Policy (specifying that the Connector operates with data structured by Tivoli Access Manager User Policies),
- Domain (specifying that the Connector operates with data structured by Tivoli Access Manager Domains),
- SSOCred (specifying that the Connector operates with data structured by Tivoli Access Manager SSO Credentials).

### Import Users/Groups from Registry

When checked, Tivoli Access Manager will import users/groups from the User Registry instead of creating users in the User Registry during an add operation.



## Delete Users/Groups/Domains from Registry

When checked, Tivoli Access Manager will delete users/groups/domains from the User Registry during a delete operation. The UserName, RegistryUID, Firstname and Lastname attributes are mandatory for this operation to find the correct LDAP registry user name of the TAM account to import.

## Detailed Log

If this field is checked, additional debug log messages are generated.

## Using the Connector

This section describes how to use the Connector in each of the supported IBM Tivoli Directory Integrator Connector modes. The section also describes the Tivoli Directory Integrator Entry schema supported by the Connector.

**Note:** When the Connector executes in the Assembly line, a Tivoli Access Manager Context is created in the Initialize method of the Connector. For performance reasons, so that a Context is not created for every Tivoli Access Manager Connector Instance, the Tivoli Access Manager Connector should be cached (pooled) within the AssemblyLine. The caching of a Connector within the AssemblyLine can be configured within TDI. Please refer to the *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for more information.

When the Connector is configured to manipulate TAM Policy objects, special consideration is required when supply attribute values in the work entry that will feed the Connector in **AddOnly** or **Update** Modes. The policy object attributes are grouped together for related policy items. The attributes can be broken up into sets where each set of attributes requires a value to update or apply any of the individual attributes for that policy item. For example, when manipulating the Policy item Account Expiry Date, you must supply values for each of the attributes AcctExpDateEnforced, AcctExpDateUnlimited, and AcctExpDate. If you wish to then modify any of these attributes for Account Expiry Date, you must again also supply values for each of the three attributes and the UserName attribute.

The following defines the Policy items and their attribute groupings.

Table 9. Policy Items

| Policy item                               | Set of Required Policy Entry Attributes   |
|---|---|
| Account Expiry Date                       | AcctExpDateEnforced, AcctExpDateUnlimited, AcctExpDate.                           |
| Account Disable Time                      | AcctDisableTimeEnforced, AcctDisableTimeUnlimited, AcctDisableTime                |
| Account Password Spaces                   | PwdSpacesAllowedEnforced, PwdSpacesAllowed  |
| Account Maximum Password Age              | MaxPwdAgeEnforced, MaxPwdAge  |
| Account Maximum Repeat Characters         | MaxPwdRepCharsEnforced, MaxPwdRepChars  |
| Account Minimum Alphabetic Characters     | MinPwdAlphasEnforced, MinPwdAlphas  |
| Account Minimum Non-Alphabetic Characters | MinPwdNonAlphasEnforced, MinPwdNonAlphas  |
| Account Time Of Day Access                | TodAccessEnforced, AccessibleDays, AccessStartTime, AccessEndTime, AccessTimezone |
| Account Minimum Password Length           | MinPwdLenEnforced, MinPwdLen  |
| Account Maximum Failed Login Attempts     | MaxFailedLoginsEnforced, MaxFailedLogins  |

## AddOnly Mode

When deployed in **AddOnly** mode, the Connector is able to create a range of data in the Tivoli Access Manager database. The Connector should be added to the **Flow** section of a TDI AssemblyLine. The **Output Map** must define a mapping for the following attributes, these attributes can be also be retrieved through querying the Connector Schema.

**Notes:**

1. Attributes marked with an asterisk (\*) are mandatory.
2. For a detailed description of all attributes, please refer to “Connector Input Attribute Details” on page 217.
3. Keep in mind the caveats on manipulating Policy items and their required Policy Entry attributes as stipulated in Table 9 on page 211.

*Table 10. Attributes by Entry Type in AddOnly Mode*

| <b>Entry Type</b> | <b>Attribute</b>               |
|-------------------|--------------------------------|
| <b>User</b>       | UserName*                      |
|                   | RegistryUID*                   |
|                   | FirstName*                     |
|                   | LastName*                      |
|                   | Description                    |
|                   | Password                       |
|                   | IsAccountValid                 |
|                   | IsPasswordValid                |
|                   | IsSSOUser                      |
|                   | NoPasswordPolicyOnCreate       |
|                   | MaxFailedLogins                |
|                   | Groups (Multivalued attribute) |
|                   |                                |
|                   |                                |
| <b>Group</b>      | GroupName*                     |
|                   | RegistryGID*                   |
|                   | CommonName                     |
|                   | Description                    |
|                   | ObjectContainer                |
|                   | Users (Multivalued attribute)  |
|                   |                                |
| <b>Policy</b>     | UserName*                      |
|                   | AcctExpDateEnforced            |
|                   | AcctExpDateUnlimited           |
|                   | AcctExpDate                    |
|                   | AcctDisableTimeEnforced        |
|                   | AcctDisableTimeUnlimited       |
|                   | AcctDisableTimeInterval        |
|                   | PwdSpacesAllowedEnforced       |
|                   | PwdSpacesAllowed               |
|                   | MaxPwdAgeEnforced              |
|                   | MaxPwdAge                      |
|                   | MaxPwdRepCharsEnforced         |
|                   | MaxPwdRepChars                 |
|                   | MinPwdAlphas                   |

Table 10. Attributes by Entry Type in AddOnly Mode (continued)

| Entry Type                | Attribute                             |
|---------------------------|---------------------------------------|
|                           | MinPwdNonAlphasEnforced               |
|                           | MinPwdNonAlphas                       |
|                           | TodAccessEnforced                     |
|                           | AccessibleDays                        |
|                           | AccessStartTime                       |
|                           | AccessEndTime                         |
|                           | AccessTimezone                        |
|                           | MinPwdLenEnforced                     |
|                           | MinPwdLen                             |
|                           | MaxFailedLoginsEnforced               |
|                           | MaxFailedLogins                       |
|                           |                                       |
| <b>Domain</b>             | DomainName*                           |
|                           | Description                           |
|                           |                                       |
| <b>SSO Credentials</b>    | UserName*                             |
|                           | ResourceName*                         |
|                           | ResourceType*                         |
|                           | ResourceUser*                         |
|                           | ResourcePassword*                     |
|                           |                                       |
| <b>SSO Resource</b>       | SSOResourceName*                      |
|                           | Description*                          |
|                           |                                       |
| <b>SSO Resource Group</b> | SSOResourceGroupName*                 |
|                           | Description                           |
|                           | SSOResources* (Multivalued attribute) |

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

## Update Mode

When deployed in **Update** mode, the Connector is able to modify existing data in the Tivoli Access Manager database. The Connector should be added to the **Flow** section of a Tivoli Directory Integrator AssemblyLine. The **Output Map** must define a mapping for the following attributes. These attributes can be also be retrieved through querying the Connector Schema.

Keep in mind the caveats on manipulating Policy items and their required Policy Entry attributes as stipulated in Table 9 on page 211.

Attributes marked with an asterisk (\*) are mandatory.

Table 11. Attributes by Entry Type in Update Mode

| Entry Type    | Attribute                      |
|---------------|--------------------------------|
| <b>User</b>   | UserName*                      |
|               | Description                    |
|               | Password                       |
|               | IsAccountValid                 |
|               | IsPasswordValid                |
|               | IsSSOUser                      |
|               | MaxFailedLogins                |
|               | Groups (Multivalued attribute) |
| <b>Group</b>  | GroupName*                     |
|               | Description                    |
|               | Users (Multivalued attribute)  |
| <b>Policy</b> | UserName*                      |
|               | AcctExpDateEnforced            |
|               | AcctExpDateUnlimited           |
|               | AcctExpDate                    |
|               | AcctDisableTimeEnforced        |
|               | AcctDisableTimeUnlimited       |
|               | AcctDisableTimeInterval        |
|               | PwdSpacesAllowedEnforced       |
|               | PwdSpacesAllowed               |
|               | MaxPwdAgeEnforced              |
|               | MaxPwdAge                      |
|               | MaxPwdRepCharsEnforced         |
|               | MaxPwdRepChars                 |
|               | MinPwdAlphas                   |
|               | MinPwdNonAlphasEnforced        |
|               | MinPwdNonAlphas                |
|               | TodAccessEnforced              |
|               | AccessEndTime                  |
|               | AccessibleDays                 |
|               | AccessStartTime                |
|               | AccessTimezone                 |
|               | MinPwdLenEnforced              |
|               | MinPwdLen                      |
|               | MaxFailedLoginsEnforced        |
|               | MaxFailedLogins                |

Table 11. Attributes by Entry Type in Update Mode (continued)

| Entry Type                | Attribute                             |
|---------------------------|---------------------------------------|
| <b>Domain</b>             | DomainName*                           |
|                           | Description                           |
| <b>SSO Credentials</b>    | UserName*                             |
|                           | ResourceName*                         |
|                           | ResourceType*                         |
|                           | ResourceUser*                         |
|                           | ResourcePassword*                     |
| <b>SSO Resource</b>       | Not Supported                         |
| <b>SSO Resource Group</b> | SSOResourceGroupName*                 |
|                           | SSOResources* (Multivalued attribute) |

Additionally, any mandatory fields mentioned above should be defined in the **Link Criteria** of the Connector. The Link Criteria is required by the AssemblyLine, since the AssemblyLine will invoke the Connectors findEntry() method to verify the existence of the given user. The value of the attribute, as defined in the Link Criteria, must match the value of the element present in the **Output Map**.

The only operator supported for Link Criteria is an **equals exact match**. Wildcard search criteria are not supported. The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

## Delete Mode

When deployed in **Delete** mode, the Connector is able to delete existing data from the Tivoli Access Manager database. The Connector should be added to the **Flow** section of an AssemblyLine.

Attributes marked with an asterisk (\*) are mandatory.

Table 12. Attributes by Entry Type in Delete Mode

| Entry Type             | Attribute        |
|------------------------|------------------|
| <b>User</b>            | UserName*        |
|                        |                  |
| <b>Group</b>           | GroupName*       |
|                        |                  |
| <b>Policy</b>          | UserName*        |
|                        |                  |
| <b>Domain</b>          | DomainName*      |
|                        |                  |
| <b>SSO Credentials</b> | UserName*        |
|                        | ResourceName*    |
|                        | ResourceType*    |
|                        |                  |
| <b>SSO Resource</b>    | SSOResourceName* |
|                        |                  |

Table 12. Attributes by Entry Type in Delete Mode (continued)

| Entry Type         | Attribute             |
|--------------------|-----------------------|
| SSO Resource Group | SSOResourceGroupName* |

The mandatory attribute must be defined in the **Link Criteria** of the Connector. The Link Criteria is required by the AssemblyLine, since the AssemblyLine will invoke the Connector's findEntry() method to verify the existence of the given user.

The only operator supported for Link Criteria is an **equals exact match**. Wildcard search criteria are not supported. The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

## Lookup Mode

When deployed in **Lookup** mode, the Connector is able to obtain all details of the required Tivoli Access Manager data. The Connector should be added to the **Flow** section of an AssemblyLine. The mandatory attribute must be defined in the **Link Criteria** of the Connector.

Attributes marked with an asterisk (\*) are mandatory.

Table 13. Attributes by Entry Type in Lookup Mode

| Entry Type         | Attribute             |
|--------------------|-----------------------|
| User               | UserName*             |
|                    |                       |
| Group              | GroupName*            |
|                    |                       |
| Policy             | UserName*             |
|                    |                       |
| Domain             | DomainName*           |
|                    |                       |
| SSO Credentials    | UserName*             |
|                    | ResourceName*         |
|                    | ResourceType*         |
|                    |                       |
| SSO Resource       | SSOResourceName*      |
|                    |                       |
| SSO Resource Group | SSOResourceGroupName* |

The Connector's findEntry() method is the main code executed. The only operator supported for **Link Criteria** is an equals exact match. Wildcard search criteria are not supported.

The Connector does not support duplicate or multiple entries. The Connector will return only one entry at a time.

## Iterator Mode

When deployed in **Iterator** mode, the Connector is able to retrieve the details of each data entry in the Tivoli Access Manager database, in turn, and make those details available to the AssemblyLine.

When deployed in this mode, the Tivoli Directory Integrator AssemblyLine will first call the Connector's selectEntries() method to obtain and cache a list of all data entries in the Tivoli Access Manager database. The AssemblyLine will then call the Connector's getNextEntry() method. This method will maintain a pointer to the current name cached in the list.

## Troubleshooting

Problems may be experienced for any of the following reasons:

### TAM Connector not installed properly

Check the configuration and re-configure if necessary.

### Query Schema Issues

When performing a schema query using the Connectors with the TDI GUI, an attempt to connect to the data source may result in an exception. These exceptions can be ignored. Any subsequent use of the **discover** schema button will succeed. The Connectors do not support the *Get Next Entry* style of schema query. The Connectors do support the torch button *Discover the Schema of the Data Source* style of schema discovery.

### Changing Mode of Connectors Already in AssemblyLine

During testing, it was observed that changing the mode of Connector in the AssemblyLine did not always work. The Connector sometimes appeared to execute in its original mode, resulting in AssemblyLine errors. If this occurs, delete the Connector and add it to the AssemblyLine in the new mode.

## Connector Input Attribute Details

This section details the attributes for connector input.

### User

Table 14.

| Attribute                 | Description  | Example                        | Default |
|---------------------------|--|--------------------------------|---------|
| UserName                  | The User Name  | maryl                          |         |
| RegistryUID               | The LDAP User Distinguished Name (DN)  | cn=mary ,o=companyabc,<br>c=au |         |
| FirstName                 | The User's First Name  | Mary                           |         |
| LastName                  | The User's Last Name   | Lou                            |         |
| Description               | A Description  | Contractor                     |         |
| Password                  | User's password<br><br>(If the 'NoPasswordPolicyOnCreate' attribute is set to FALSE, the password must confirm to the current password policy in Tivoli Access Manager.)   | m3ry10u                        |         |
| IsAccountValid            | TRUE to activate the account. FALSE to leave the account inactive.   | TRUE or FALSE                  | TRUE    |
| IsPasswordValid           | Set to FALSE if user is to change the password on next login. TRUE to remain unchanged.  | TRUE or FALSE                  | TRUE    |
| IsSSOUser                 | TRUE to enable Single Sign-on capabilities for this user. FALSE to disable.  | TRUE or FALSE                  | FALSE   |
| NoPasswordPolicy OnCreate | FALSE will enforce the password policy on the "Password" attribute and as a result it will be checked against the password policy settings the first time it is created. TRUE will not enforce the password policy on the password when it is created. | TRUE or FALSE                  | TRUE    |
| MaxFailedLogins           | Set the maximum number of failed logins a user can have before the account is disabled.  | 8                              | 10      |

Table 14. (continued)

| Attribute                      | Description  | Example  | Default |
|--------------------------------|--|--|---------|
| Groups (Multivalued attribute) | This is a multi-valued attribute. Please refer to the <i>IBM Tivoli Directory Integrator 6.1.1: Users Guide</i> about how to set multi-valued attributes. Any Group listed in this attribute should already exist as a valid group in Tivoli Access Manager. | Groups1 -> itSpecialists<br>Groups2 -> programmers |         |

## Group

Table 15.

| Attribute       | Description  | Example   |
|-----------------|--|---|
| GroupName       | The Group Name   | programmers   |
| RegistryGID     | The LDAP Group DistinguishedName (DN)  | cn=programmers, cn=SecurityGroups, secAuthority=Default |
| CommonName      | The LDAP Common Name (CN)  | programmers   |
| Description     | The Group Description  | Fulltime Programmers                                    |
| ObjectContainer |  |   |
| Users           | This is a multi-valued attribute. Please refer to the <i>IBM Tivoli Directory Integrator 6.1.1: Users Guide</i> about how to set multi-valued attributes. Any user listed in this attribute should already exist as a valid user in Tivoli Access Manager. | Users1 -> maryl<br>Users2 -> johnd                      |

## Policy

Table 16.

| Attribute                | Description  | Example  |
|--------------------------|--|--|
| UserName                 | The User Name the policy will be set for. Must be a valid Tivoli Access Manager user.  | maryl  |
| AcctExpDateEnforced      | If TRUE then enforce the Account Expiration Date.  | TRUE or FALSE  |
| AcctExpDateUnlimited     | If TRUE then set the Account Expiration Date to be unlimited.  | TRUE or FALSE  |
| AcctExpDate              | Sets the expiry date for the user account<br><br>The attribute must be of type java.util.Date, or java.lang.String. If a String value is provided the required date string format is "yyyyMMdd" where 'yyyy' us the four digit year, 'MM' is the two digit month, and 'dd' is the two digit day; i.e. 20091231 is the value for the date 31st December 2009. | Refer to the Tivoli Access Manager Java API Reference. |
| AcctDisableTimeEnforced  | If TRUE then enforce the Account Disable Time.   | TRUE or FALSE  |
| AcctDisableTimeUnlimited | If TRUE then set the Account Disable Time to be unlimited.   | TRUE or FALSE  |
| AcctDisableTimeInterval  | Set the Account Disable Time Interval.   | Refer to the Tivoli Access Manager Java API Reference. |



Table 16. (continued)

| Attribute                | Description   | Example  |
|--------------------------|---|--|
| PwdSpacesAllowedEnforced | If TRUE enforce the value of the 'PwdSpacesAllowed' attribute             | TRUE or FALSE  |
| PwdSpacesAllowed         | If TRUE allow spaces in the password                                      | TRUE or FALSE  |
| MaxPwdAgeEnforced        | If TRUE enforce the Maximum Password Age value                            | TRUE or FALSE  |
| MaxPwdAge                | Sets the Maximum Password Age   | Refer to the Tivoli Access Manager Java API Reference. |
| MaxPwdRepCharsEnforced   | If TRUE enforce the Maximum Password Repeatable characters number         | TRUE or FALSE  |
| MaxPwdRepChars           | Sets the Maximum Password Repeatable Characters                           | 5  |
| MinPwdAlphasEnforced     | If TRUE enforce the Minimum number of Alphanumeric characters allowed     | TRUE or FALSE  |
| MinPwdAlphas             | Sets the Minimum number of Alphanumeric characters allowed                | 6  |
| MinPwdNonAlphasEnforced  | If TRUE enforce the Minimum number of non-alphanumeric characters allowed | TRUE or FALSE  |
| MinPwdNonAlphas          | Sets the Minimum number of non-alphanumeric characters allowed            | 3  |
| TodAccessEnforced        | If TRUE enforce the access times set for the user                         | TRUE or FALSE  |
| AccessibleDays           | Sets the days accessible for the user account                             | Refer to the Tivoli Access Manager Java API Reference. |
| AccessStartTime          | Sets the access start time for the user account                           | Refer to the Tivoli Access Manager Java API Reference. |
| AccessEndTime            | Sets the access end time for the user account                             | Refer to the Tivoli Access Manager Java API Reference. |
| AccessTimezone           | Sets the time zone for the user account                                   | Refer to the Tivoli Access Manager Java API Reference. |
| MinPwdLenEnforced        | If TRUE enforce the Minimum Password Length                               | TRUE or FALSE  |
| MinPwdLen                | Sets the Minimum Password Length  | 8  |
| MaxFailedLoginsEnforced  | If TRUE then enforce the Maximum Failed Login setting.                    | TRUE or FALSE  |
| MaxFailedLogins          | Sets the Maximum Failed Logins for the user                               | 8  |

## Domain

Table 17.

| Attribute   | Description            | Example            |
|-------------|------------------------|--------------------|
| DomainName  | The name of the domain | MyDomain           |
| Description | The Domain description | Sample domain name |

## SSO Credentials

Table 18.

| Attribute        | Description  | Example                        |
|------------------|--|--------------------------------|
| UserName         | The name of the user the credentials will be set for                               | maryl                          |
| ResourceName     | The SSO Resource Name. (Must be a valid Tivoli Access Manager SSO Resource entry). | myResource1                    |
| ResourceType     | Specifies whether this resource is a single resource of a resource group           | Web Resource or Resource Group |
| ResourceUser     | Sets the Resource User Name  | marylou                        |
| ResourcePassword | Sets the User Name Password for the specified resource                             | b1ddy4                         |

## SSO Resource

Table 19.

| Attribute       | Description                      | Example              |
|-----------------|----------------------------------|----------------------|
| SSOResourceName | The Single sign-on Resource Name | MyResource1          |
| Description     | The Description                  | Development Server 1 |

## SSO Resource Group

Table 20.

| Attribute            | Description   | Example  |
|----------------------|---|--|
| SSOResourceGroupName | The Single sign-on Resource Group Name  | MyResourceGroup1   |
| Description          | The Description   | All Development Servers                                      |
| SSOResources         | This is a multi-valued attribute. Please refer to the <i>IBM Tivoli Directory Integrator 6.1.1: Users Guide</i> about how to set multi-valued attributes. Any SSO Resources listed in this attribute should already exist as a valid SSO Resource in Tivoli Access Manager. | SSOResources1 -> myResource1<br>SSOResources2 -> myResource2 |

---

## TCP Connector

The TCP Connector is a transport Connector using TCP sockets for transport. You can use the TCP Connector in Iterator and AddOnly mode only.

### Iterator Mode

When in Iterator mode, the TCP Connector waits for incoming TCP calls on a specific port. When a connection is established, the `getNext` method returns an entry with the following properties:

**socket** The TCP socket object (for example, the TCP input and output streams)

**in** An instance of a `BufferedReader` using the socket's input stream

**out** An instance of a `BufferedWriter` using the socket's output stream

The **in** and **out** objects can be used to read and write data to or from the TCP connection. For example, you can do the following to implement a simple echo server (put the code in the **After GetNext** Hook):

```
var ins = conn.getProperty("in");
var outs = conn.getProperty("out");
var str = ins.readLine();
outs.write("You said==>" + str + "<==");
outs.flush();
```

Because you are using a `BufferedWriter`, it is important to call the `out.flush()` method to make sure data is actually sent out over the connection.

If you specify a `Parser`, then the `BufferedReader` is passed to the `Parser`, which in turn reads and interprets data sent on the stream. The returned entry then includes any attributes assigned by the `Parser` as well as the properties listed previously (**socket**, **in**, and **out**).

If the TCP Connector is configured in `serverMode=true` then the connection is closed between each call to the `getNext` method. If `serverMode=false` the connection to the remote host is kept open for as long as the TCP Connector is active (for example, until the `AssemblyLine` stops).

### AddOnly Mode

When the TCP Connector works in this mode, the default implementation is to write entries in their string form, which is not useful. Typically, you specify a `Parser` or use the **Override Add** hook to perform specific output. In the **Override Add** hook you access **thein** or **out** objects by calling the Connector Interface's `getReader()` and `getWriter()` methods, for example:

```
var in = mytcpconnector.connector.getReader();
var out = mytcpconnector.connector.getWriter();
```

You can also use the **Before Add** and **After Add** hooks to insert headers or footers around the output from your `Parser`.

## Configuration

### TCP Port

The TCP port number to connect or listen to (depends on the value of `servermode`).

### TCP Host

The remote host to which connections are made (`servermode = false`).

### Connection Backlog

This represents the maximum queue length for incoming connection indications (a request to connect). If a connection indication arrives when the queue is full, the connection is refused.

**Server Mode**

If **true**, then Iterating listens for incoming requests. If **false**, then Iterating connects to a remote server.

**Use SSL**

If checked, the Connector will deploy the Secure Socket Layer (SSL) on the connection.

**Need Client Authentication over SSL**

If checked and if SSL is enabled in Server Mode (that is, listening for incoming connections), client authentication is necessary.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

You can select a Parser for this Connector from the Parser pane, where you select a parser by clicking the bottom-right **Inherit From:** button.

**See also**

“File system Connector” on page 77,

“Direct TCP /URL scripting” on page 29,

“TCP Server Connector” on page 223

“URL Connector” on page 227.

---

## TCP Server Connector

This Connector supports Server and Iterator modes only.

In Server mode, this Connector waits for incoming TCP connections on a specified port and spawns a new thread to handle the incoming request. When the new thread has started, the original Server mode Connector goes back to listening mode. When the newly created thread has completed, the thread stops and the TCP connection is closed.

In Iterator mode, the Connector is single-threaded, in that it waits for a connection on the IP address of the local machine and the port specified. Once the connection is received, the Connector will generate Entries based on received data until the Client closes the connection.

## Configuration

### TCP Port

The TCP port on which to listen for incoming connections.

### Connection Backlog

This represents the maximum queue length for incoming connection indications (a request to connect). If a connection indication arrives when the queue is full, the connection is refused.

### Use SSL

If checked, the Connector will deploy the Secure Socket Layer (SSL) on the connection.

### Require Client Authentication

If checked, the Connector will require clients to supply client-side SSL certificates that can be matched to the configured TDI trust store.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Connector Schema

The Connector makes the following properties available in the Input Attribute Map:

### **tcp.originator**

The Connector object.

### **event.originator**

The Connector object. This is the same object as the one stored in **tcp.originator**. This Attribute ensures backward compatibility with the now deprecated TCP Port EventHandler.

### **tcp.inputstream**

TCP socket input stream (java.io.InputStream)

### **event.inputstream**

TCP socket input stream (java.io.InputStream). This is the same object as the one stored in **tcp.inputstream**. This Attribute ensures backward compatibility with the TCP Port EventHandler.

### **tcp.outputstream**

TCP socket output stream (java.io.OutputStream).

### **event.outputstream**

TCP socket output stream (java.io.OutputStream). This is the same object as the one stored in **tcp.outputstream**. This Attribute ensures backward compatibility with the TCP Port EventHandler.

### **tcp.remoteIP**

Remote IP address (dot notation).

### **tcp.remotePort**

Remote TCP port number.

**tcp.remoteHost**

Remote hostname.

**tcp.localIP**

Local IP address (dot notation).

**tcp.localPort**

Local TCP port number.

**tcp.localHost**

Local hostname.

**tcp.socket**

TCP Socket object (java.net.Socket).

The TCP Server Connector does not use its Output Attribute Map – it just closes the Connection to the client application when done.

The **tcp.inputstream** and **tcp.outputstream** Attribute values are meant to be used via scripting in the AssemblyLine to read the client request and write the response respectively.

**See Also**

“TCP Connector” on page 221.

---

## Timer Connector

The timer waits for a specified time; then it returns from sleep and resumes an `AssemblyLine`, that is, it starts a new cycle. This Connector runs in Iterator mode only.

On attribute mapping, there is one attribute you can map into the work entry: a timestamp, which is of type `java.util.Date`. It will contain the time when it started the cycle.

Using Delta functionality with this Connector does probably not make much sense.

Previous versions of this Connector used a Unix crontab-style **schedule** parameter to set up the exact time at which to run the Connector; when such a schedule is encountered in a Config file it is automatically converted to the new format as outlined below.

### Configuration

This Connector needs the following parameters:

#### Month

Select a month to run the Timer Connector (\* = any)

**Day** Day of the month to run the Timer Connector on(\* = any)

#### Weekday

Select a weekday to run the Timer Connector(\* = any)

**Hour** The hour at which to run the Timer Connector (\* = any)

#### Minute

The minute at which to run the Timer Connector

#### Detailed Log

If this field is checked, additional log messages are generated.





---

## URL Connector

The URL Connector is a transport Connector that requires a Parser to operate. The Connector opens a stream specified by a URL.

**Note:** When forced through a firewall that enforces a proxy server, the URL Connector does not work. The URL Connector needs to have the right proxy server set.

This Connector supports AddOnly and Iterator modes.

The Connector, in principle, can handle secure communications using the SSL protocol, but it may require driver-specific configuration steps in order to set up SSL support.

## Configuration

The Connector needs the following parameters:

**URL** The URL to open (for example, `http://host/file.csv`).

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

From the Parser configuration pane, you can select a Parser to operate upon the stream. You select a parser by clicking on the bottom-right **Inherit from:** button.

## Supported URL protocol

The supported URL protocols are:

- HTTP
- HTTPS

## See also

“File system Connector” on page 77,

“TCP Connector” on page 221,

“Direct TCP /URL scripting” on page 29.



---

## Web Service Receiver Server Connector

The Web Service Receiver Server Connector is part of the TDI Web Services suite.

This Connector is basically an HTTP Server specialized for servicing SOAP requests over HTTP. It operates in Server mode only.

AssemblyLines support an Operation Entry (op-entry). The op-entry has an attribute *\$operation* that contains the name of the current operation executed by the AssemblyLine. In order to process different web service operations easier, the Web Service Receiver Server Connector will set the *\$operation* attribute of the op-entry.

The Web Service Receiver Server Connector supports generation of a WSDL file according to the input and output schema of the AssemblyLine. As in TDI 6.1.1 AssemblyLines support multiple operations, the WSDL generation can result in a web service definition with multiple operations. There are some rules about naming the operations:

- Pre-6.1 TDI configuration files contain only one input and one output schema referred to as default operation schemas. When a pre-6.1 TDI configuration is used the only operation generated is named as the name of the AssemblyLine as in TDI 6.0.
- In TDI 6.1.1 configurations if there is an operation named "Default", the corresponding operation in the WSDL file is named as the name of the AssemblyLine.
- In TDI 6.1.1 configurations if there is an operation named "Default" and there is also an operation with a name as the name of the AssemblyLine, both operations preserve their names in the WSDL file.
- In all other cases the operations appear in the WSDL file as they are named in the AssemblyLine configuration.

### Hosting a WSDL file

The Web Service Receiver Server Connector provides the *"wsdlRequested"* Connector Attribute to the AssemblyLine.

If an HTTP request arrives and the requested HTTP resource ends with *"?WSDL"* then the Connector sets the value of the *"wsdlRequested"* Attribute to **true**; otherwise the value of this Attribute is set to **false**.

This Attribute's value tells the AssemblyLine whether the request received is a SOAP request or a request for a WSDL file, and allows the AssemblyLine to distinguish between pure SOAP requests and HTTP requests for the WSDL file. The AssemblyLine can use a branch component to execute only the required piece of logic – (1) when a request for the WSDL file has been received, then the AssemblyLine can read a WSDL file and send it back to the web service client; (2) when a SOAP request has been received the AssemblyLine will handle the SOAP request. Alternatively, you could program the `system.skipEntry()`; call at an appropriate place (in a script component, in a hook in the first Connector in the AssemblyLine, etc.) to skip further processing.

It is the responsibility of the AssemblyLine to provide the necessary response to either a SOAP request or a request for a WSDL file.

The Connector implements a public method:

```
public String readFile (String aFileName) throws IOException;
```

This method can be used from TDI JavaScript in a script component to read the contents of a WSDL file on the local file system. The AssemblyLine can then return the contents of the WSDL in the *"soapResponse"* Attribute, and thus to the web service client in case a request for the WSDL was received.

# Configuration

## Parameters

### TCP Port

The port number the service is running (listening) on.

### Connection Backlog

This represents the maximum queue length for incoming connection indications (a request to connect). If a connection indication arrives when the queue is full, the connection is refused.

### Input the SOAP message as

Specifies the type of the SOAP Request message input to the AssemblyLine. This drop-down list allows you to choose either **String** or *"DOMElement"*.

### Return the SOAP message as

Specifies the type of the SOAP Response message output from the AssemblyLine. This drop-down list allows you to choose either **String** or *"DOMElement"*.

### Tag Op-Entry

When this parameter is checked (that is, "true") the Connector will tag the op-entry even if the currently executed operation is not on the list of exposed operations in the AssemblyLine/WSDL. It is up to the TDI solution implementation to handle this case appropriately.

### Use SSL

If checked the server will only accept SSL (https) connections. The SSL parameters (keystore, etc.) are specified as values of Java system properties in the `global.properties` file located in the TDI installation folder.

### Require Client Authentication

Specifies whether this Connector will require clients to authenticate with client SSL certificates. If the value of this parameter is **true** (that is, checked) and the client does not authenticate with a client SSL certificate, then the Connector will drop the client connection. If the value of this parameter is **true** and the client does authenticate with a client SSL certificate, then the Connector will continue processing the client request. If the value of this parameter is **false**, then the Connector will process the client request regardless of whether the client authenticates with a client SSL certificate.

### Auth Realm

The basic-realm sent to the client in case authentication is requested.

### Use HTTP Basic Authentication

This connector supports HTTP basic authentication. To activate, check the "Use HTTP Basic Authentication" checkbox. If activated, the server checks if any credentials are already sent and if not, the server sends authorization request to client. After the client sends the needed credentials, the Connector then sets two attributes: "http.username" and "http.password". These two attributes contain the username and password of the client. It is responsibility of the AssemblyLine to check if this pair of username and password is valid. If the client is authorized successfully then "http.credentialsValid" work Entry Attribute must be set to true. If the client is not authorized then "http.credentialsValid" work Entry Attribute must be set to false. If the client is not authorized then the server sends a "Not Authorized" HTTP message.

### Comment

Your own comments go here.

### Detailed Log

If checked, will generate additional log messages.

### WSDL Output to Filename

The name of the WSDL file to be generated when the **Generate WSDL** button is clicked. This parameter is only used by the WSDL Generation Utility – this parameter is not used during the Connector execution.

### Web Service provider URL

The address on which web service clients will send web service requests. Also this parameter is only used by the WSDL Generation Utility – this parameter is not used during the Connector execution.

The **Generate WSDL** button runs the WSDL generation utility.

The WSDL Generation utility takes as input the name of the WSDL file to generate and the URL of the provider of the web service (the web service location). This utility extracts the input and output parameters of the AssemblyLine in which the Connector is embedded and uses that information to generate the WSDL parts of the input and output WSDL messages. It is mandatory that for each Entry Attribute in the "Initial Work Entry" and "Result Entry" Schema the "Native Syntax" column be filled in with the Java type of the Attribute (for example, "java.lang.String"). The WSDL file generated by this utility can then be manually edited.

The operation style of the SOAP Operation defined in the generated WSDL is *rpc*.

The WSDL generation utility cannot generate a <types...>...</types> section for complex types in the WSDL.

## Connector Operation

The Web Service Receiver Server Connector stores the following information from the HTTP/SOAP request into Attributes of the Connector's *conn* entry, ready to be mapped into the *work* entry:

- The name of the host to which the request is sent (the local host) – stored into the "host" Attribute
- The requested HTTP resource – stored into the "requestedResource" Attribute
- The value of the "soapAction" HTTP header – stored into the "soapAction" Attribute
- If the value of the **Input the SOAP message as FC** parameter is **String** then the SOAP request message is stored as a java.lang.String object in the "soapRequest" Attribute.
- If the value of the **Input the SOAP message as FC** parameter is **DOMELEMENT** then the SOAP request message is stored as an org.w3c.dom.Element object in the "soapRequest" Attribute.
- Whether a WSDL file was requested — in the "wsdlRequested" Attribute. If this is the case (that is, the value is **true**, no other Attributes will be set).

When reaching the Response stage of the AssemblyLine, this Connector requires the SOAP response message in text XML form or as *DOMELEMENT* from the "soapResponse" Attribute of the *work* Entry to be mapped out:

- If the value of the **Return the SOAP message as FC** parameter is **String** then the SOAP response message must be stored as a java.lang.String object in the "soapResponse" Attribute by the AssemblyLine.
- If the value of the **Return the SOAP message as FC** parameter is **DOMELEMENT** then the SOAP response message must be stored as a org.w3c.dom.Element in the "soapResponse" Attribute by the AssemblyLine.

The Connector then wraps the SOAP response message into an HTTP response and returns it to the web service client.

## See also

"Axis Easy Web Service Server Connector" on page 21.



---

## z/OS Changelog Connector

The z/OS Changelog Connector is a specialized instance of the LDAP Connector. It is configured for usage with a z/OS Directory Server, accessed using the LDAP protocol over TCP/IP.

This connector supports Delta Tagging, at the Entry level, the Attribute level and the Attribute Value level. It is the LDIF Parser that provides delta support at the Attribute and Attribute Value levels. .

### Configuration

The Connector needs the following parameters:

#### LDAP URL

The LDAP URL for the connection (`ldap://host:port`).

#### Login username

The LDAP distinguished name used for authentication to the server. Leave blank for anonymous access.

#### Login password

The credentials (password).

#### Authentication Method

The authentication method. Possible values are:

- CRAM-MD5 (use the CRAM-MD5 (RFC-2195) SASL mechanism).
- none (use no authentication (**anonymous**)).
- simple (use weak authentication (cleartext password)).
- SASL

If not specified, default (simple) is used. If **Login username** and **Login password** are blank, then **anonymous** is used.

#### Use SSL

If Use SSL is **true** (that is, checked), the Connector uses SSL to connect to the LDAP server. Note that the port number might need to be changed accordingly.

#### ChangeLog Base

The search base where the Changelog is kept. The standard DN for this is **cn=changelog**.

#### Extra Provider Parameters

Allows you to pass a number of extra parameters to the JNDI layer. It is specified as name:value pairs, one pair per line.

#### Iterator State Key

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

#### Start at changenumber

Specifies the starting changenumber. Each Changelog entry is named **changenumber=intvalue** and the Connector starts at the number specified by this parameter and automatically increases by one. The special value **EOD** means start at the end of the Changelog.

#### State Key Persistence

Governs the method used for saving the Connector's state to the System Store. The default is **End of Cycle**, and choices are:

##### After read

Updates the System Store when you read an entry from the directory server's change log, before you continue with the rest of the AssemblyLine.

**End of cycle**

Updates the System Store with the change log number when all Connectors and other components in the AssemblyLine have been evaluated and executed.

**Manual**

Switches off the automatic updating of the System Store with this Connector's state information; instead, you will need to save the state by manually calling the z/OS Changelog Connector's *saveStateKey()* method, somewhere in your AssemblyLine.

**Timeout**

Specifies the number of seconds the Connector waits for the next Changelog entry. The default is 0, which means wait forever.

**Sleep Interval**

Specifies the number of seconds the Connector sleeps between each poll. The default is 60.

**Detailed Log**

If this field is checked, additional log messages are generated.

**See also**

"LDAP Connector" on page 133,

"Active Directory Changelog (v.2) Connector" on page 13,

"Exchange Changelog Connector" on page 71,

"IBM Directory Server Changelog Connector" on page 97,

"Netscape/iPlanet/Sun Directory Changelog Connector" on page 161.



---

## Chapter 3. EventHandlers

EventHandlers are used to extend the functionality of AssemblyLines and Connectors by providing a framework to control how they are run. This framework is particularly useful when an incoming event (for example, an incoming http, an LDAP change trigger or a JMS message) can trigger the start of a number of different AssemblyLines depending on the content in the incoming data. A few EventHandlers have been pre-programmed to make things easier.

### Notes:

1. EventHandlers and the EventHandler concept are deprecated since version 6.0 of IBM Tivoli Directory Integrator, and will be phased out completely in a future version of TDI
2. EventHandlers can now only be added to your solution by using **Object->New EH** in the CE.
3. You can always override EventHandler behavior by using your own scripts. (Note however. that the concept of EventHandlers will be removed in the future, so if you heavily customize one you may find that your EventHandler has disappeared when opening the Config file in a future version of TDI 6.1.1.)

---

## Migration from ChangeLog EventHandlers to ChangeLog Connectors

When opening Config Files created with TDI 6.0, existing Connector references will not need migration – old configuration files will continue to work with the updated Connectors.

As the EventHandler concept is deprecated and will be removed from future versions of TDI, you might however want to migrate from deprecated Changelog EventHandlers to Changelog Connectors.

For each EventHandler a corresponding AssemblyLine must be created. Then an Iterator Connector corresponding to the EventHandler must be inserted into the AssemblyLine “Feeds” section. Then the Connector parameters must be set – this is specific for each EventHandler/Connector pair, but generally the Connector parameters must be set the same values as the corresponding EventHandler parameters (which usually have the same names).

Any processing performed in the EventHandler Action Map must be re-implemented in the AssemblyLine “Flow” section.

The functionality of the “enabled” EventHandler parameter (otherwise known as “Auto-start service”) is also available for AssemblyLines. If you want your AssemblyLine to be started right after the TDI Server is started, go to the Config/AutoStart folder in the Config Editor and add your AssemblyLine.

No migration is necessary for the JNDI Connector.

---

## EventHandler types

The following EventHandler types are included in IBM Tivoli Directory Integrator:

### Standard EventHandler

The Standard EventHandler is the most used EventHandler. You can specify conditions and actions using a number of predefined conditions and actions. It also provides hooks where you can start script code for full control. See “LDAP EventHandler” on page 259 for more information.

### Primitive EventHandler (simple EventHandler, trigger or port listener)

The Primitive EventHandler enables you to script everything. With this EventHandler you have full control of the EventHandler’s actions but you must code the EventHandler manually. See

“Generic thread (primitive EventHandler)” on page 271 and “Timer EventHandler (primitive EventHandler)” on page 273 for more information.

### Advanced EventHandler

The Advanced EventHandler wraps up even more than the Standard EventHandler in the Config Editor.

---

## When are they started?

When TDI server starts, it scans through the table of EventHandlers and checks each one for the auto startup flag. If the auto startup flag is set, the EventHandler is spawned as a thread inside the TDI server process. When the EventHandler thread stops, TDI server does not restart the EventHandler.

**Note:** You can force an EventHandler to start regardless of its auto start flag using command line options.

See “Starting the EventHandler” in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for further discussion on how to start EventHandlers from the Config Editor.

---

## What do they do?

EventHandlers perform a variety of functions but typically they enable external events to trigger actions in the TDI server. These actions can be specific to each site and each person, but one common action can be specific to an AssemblyLine. The timer is such an example where the external event is the clock reaching a specific time. Other events are asynchronous, such as when the TCP port EventHandler waits for incoming TCP connections, or can initiate some connection and poll for events, such as the Mailbox Connector EventHandler. Consult each EventHandler’s configuration for more information.

---

## Data flow

The EventHandlers, like AssemblyLines, have a Prolog and an Epilog. The Prolog is started before the action flow of each event.

---

## Passing input/output file names to an AssemblyLine

To pass a filename from the EventHandler to the AssemblyLine, use an **entry** object. Here the filename is called **myFileName**, and a property is used instead of an attribute:

```
var entry = system.newEntry();
entry.setProperty("inputFileName","myFileName");
// start AssemblyLine
var al = main.startAL ("myAssemblyLine", entry);
al.join (); // wait for al to finish
```

On the AssemblyLine side you have code in your Prolog, in the **Before Connectors Initialized** hook (because you want your parameters to be used when the Connectors are initialized):

```
workEntry = task.getWork(); // gets the initial entry
var FileName = workEntry.getProperty("inputFileName");
// Set the relevant parameter of the (Connector)
myFileConnector.connector.setParam("filePath",FileName);
// If you don't want the AssemblyLine to run with the initial entry, clear it
task.setWork(null);
```

There are a couple of finer points here:

1. Clearing the **work** entry ensures that control is passed to the first Iterator. Do not clear any entries that need to be processed. If there is a valid **work** entry when the AssemblyLine is initiated, then any

Iterators in the AssemblyLine are bypassed for that work cycle, and processing starts at the first non-Iterator. See "Connector Modes" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for more information.

2. Using properties instead of attributes ensures that the AssemblyLine does not map the attribute later (automatically mapping all attributes).

---

## EventHandler availability

The following EventHandlers are included in TDI:

- "Active Directory Changelog EventHandler" on page 239
- "Connector EventHandler" on page 243
- "DSMLv2 EventHandler" on page 245
- "Exchange Changelog EventHandler" on page 249
- "HTTP EventHandler" on page 253
- "IBM Directory Server EventHandler" on page 255
- "LDAP EventHandler" on page 259
- "LDAP Server EventHandler" on page 263
- "Mailbox EventHandler" on page 265
- "SNMP EventHandler" on page 267
- "TCP Port EventHandler" on page 269
- "Generic thread (primitive EventHandler)" on page 271
- "Timer EventHandler (primitive EventHandler)" on page 273
- "z/OS LDAP Changelog EventHandler" on page 275

---

## Migration of Changelog EventHandlers

The EventHandler concept in IBM Tivoli Directory Integrator 6.1.1 is deprecated, and all ChangeLog EventHandlers in particular may be removed in a future version of IBM Tivoli Directory Integrator.

Therefore, you might consider to migrate from deprecated Changelog EventHandlers to Changelog Connectors. For each EventHandler a corresponding AssemblyLine must be created. Then an Iterator Connector corresponding to the EventHandler must be inserted into the AssemblyLine "Feeds" section. Then the Connector parameters must be set – this is specific for each EventHandler/Connector pair, but generally the Connector parameters must be set the same values as the corresponding EventHandler parameters (which usually have the same names).

Any processing performed in the EventHandler Action Map must be re-implemented in the AssemblyLine "Flow" section. The functionality of the "enabled" EventHandler parameter (otherwise known as "Auto-start service") is also available for AssemblyLines. If you want your AssemblyLine to be started right after the TDI Server is started, go to the Config/AutoStart folder in the Config Editor and add your AssemblyLine.

For a more detailed description of how this is done for the Active Directory Changelog EventHandler, see "Migration from Active Directory Changelog EventHandler to Active Directory Changelog (v.2) Connector" on page 18.



---

## Active Directory Changelog EventHandler

The Active Directory Changelog EventHandler detects and sends notification of changes that occur in Active Directory. It reports changed Active Directory objects so that other data sources can be synchronized with Active Directory. The LDAP protocol is used both for registering for change notification and retrieving changed objects.

The EventHandler uses internally the Active Directory Changelog Connector to get changed objects from Active Directory. Changed objects retrieval is based on the **uSNChanged** mechanism.

See “Active Directory Changelog (v.2) Connector” on page 13 for details about the order of changes retrieval, the structure of the delivered Entries, and specific details about handling deleted and moved objects.

The EventHandler uses the LDAPv3 Server Notification request control to block until new changes occur in Active Directory.

### Behavior

When the EventHandler starts, it connects to Active Directory and retrieves all recent directory changes that have happened while the EventHandler was offline. Then it blocks, waiting for a new change in Active Directory - when this happens it retrieves all new changes, blocks again waiting for further changes, and so on. There is no risk of losing notifications when the EventHandler is not running, because each time it starts it retrieves the changes that it missed while offline.

The Active Directory Changelog EventHandler can be interrupted any time during the synchronization process. It saves the state of the synchronization process in the User Property Store of the IBM Tivoli Directory Integrator (after each Entry retrieval), and the next time the EventHandler is started it successfully continues the synchronization from the point it was interrupted.

If the Active Directory goes offline, the EventHandler does not stop and tries to reconnect until it either succeeds or a stop is requested.

### Access to the USN synchronization values in the User Property Store

The state of synchronization at any time is represented by four update sequence number (USN) numbers:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

These values are packed and stored in the User Property Store. Do not change these values manually. You might want to archive the numbers corresponding to a certain stage of synchronization and later use these numbers to replay synchronization from that stage.

The following script code can be used in IBM Tivoli Directory Integrator to get USN values stored in the User Property Store:

```
// Retrieve USN values from User Property Store
var usn = system.getPersistentObject("ad_sync");
var startUsn = usn.getString("START_USN");
var endUsn = usn.getString("END_USN");
var currentUsnCreated = usn.getString("CURRENT_USN_CREATED");
var currentUsnChanged = usn.getString("CURRENT_USN_CHANGED");

main.logmsg("START_USN: " + startUsn);
main.logmsg("END_USN: " + endUsn);
main.logmsg("CURRENT_USN_CREATED: " + currentUsnCreated);
main.logmsg("CURRENT_USN_CHANGED: " + currentUsnChanged);
```

"ad\_sync" is the name of a parameter already stored in the User Property Store. The EventHandler parameter **Persistent Parameter Name** specifies this value. The previous example dumps the values to the screen, however, you might want to perform other actions, such as saving values in a file and backing up this file.

The next example of script code shows how the USN values can be stored in the User Property Store:

```
// Store USN values in the User Property Store
var usn = system.newEntry();
usn.setAttribute("START_USN", startUsn);
usn.setAttribute("END_USN", endUsn);
usn.setAttribute("CURRENT_USN_CREATED", currentUsnCreated);
usn.setAttribute("CURRENT_USN_CHANGED", currentUsnChanged);
system.setPersistentObject("ad_sync", usn);
```

This code assumes that the variables *startUsn*, *endUsn*, *currentUsnCreated* and *currentUsnChanged* contain the USN numbers as strings. This example saves the USN values under the "ad\_sync" parameter, so "ad\_sync" must be specified in the EventHandler parameter **Persistent Parameter Name** to continue synchronization from the desired point.

## Access to the runtime EventHandler's USN synchronization values

The Active Directory Changelog EventHandler provides the following public methods to access its current USN values:

**public Entry getUsnValues ();**

Returns an Entry object with the following attributes:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

The value of each of the attributes is of type **java.lang.Integer** and represents the corresponding EventHandler's USN value.

**public void setUsnValues (Entry usnEntry);**

Sets the EventHandler's current USN synchronization values to the values specified in the usnEntry parameter. The structure of the usnEntry parameter must be the same as the structure of the Entry returned by getUsnValues(). The values of the usnEntry attributes must be either **java.lang.Integer** or the string representations of the corresponding numbers.

**Note:** Be careful when changing the USN values at runtime. Specifying inconsistent values can result in improper synchronization.

## Configuration

The EventHandler needs the following parameters:

### LDAP URL

The LDAP URL of the Active Directory service you want to access. The LDAP URL has the form `ldap://hostname:port` or `ldap://server_IP_address:port`. For example, **ldap://localhost:389**

**Note:** The default LDAP port number is 389. When using SSL the default LDAP port number is 636.

### Login username

The distinguished name used for authentication to the service. For example, **cn=admin,dc=your\_domain,dc=com**.

**Note:** If you use **Anonymous** authentication, you must leave this parameter blank.

**Login password**

The credentials (password).

**Note:** If you use **Anonymous** authentication, you must leave this parameter blank.

**Authentication Method**

The authentication method to be used. Possible values are:

- Anonymous (use no authentication)
- Simple (use weak authentication (cleartext password))

**Use SSL**

Specifies whether to use Secure Sockets Layer for LDAP communication with Active Directory.

**LDAP Search Base**

The Active Directory sub-tree that is polled for changes. For example, **dc=your\_domain,dc=com**.

**Note:** This must be a Naming Context in the directory.

**Persistent Parameter Name**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

**Start at**

Specifies either **EOD** or **0**. **EOD** means report only changes that occur after the EventHandler is started. **0** means perform full synchronization, that is, report all objects available in Active Directory Service. This parameter is taken into account only when the parameter specified by the **Persistent Parameter Name** parameter is not found in the User Property Store.

**Detailed Log**

Specifies whether more detailed debug information is written to the log file.

**Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

**See also**

“Migration of Changelog EventHandlers” on page 237.





---

## Connector EventHandler

This EventHandler uses any Connector as an input event generator. The EventHandler calls the Connector's getNext method to obtain the next entry from the Connector. When a Connector reaches end of input, it returns null. This EventHandler continues to call the Connector's input method even after the Connector returns null. For some Connectors this can make sense whereas for others it does not.

For example, using the File System Connector makes sense because the file read by the Connector can have data appended to it at any time. Connectors selecting a finite set of entries eventually run out of entries and the EventHandler continues forever waiting for new data.

## Configuration

This EventHandler needs the following parameters:

### Global Connector

The Connector to use for input.

### Poll Interval

The number of seconds between each call to the Connector after a **NULL** entry has been received from the Connector.

### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

### Detailed Log

Specifies whether more detailed log information is written to the log file.

## Objects/properties/attributes

The EventHandler sets the following event properties:

### event.originator

The EventHandler object

### event.connector

The Connector object used by this EventHandler

The event object also contains any attribute returned by the Connector.

## See also

"Starting the EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.



---

## DSMLv2 EventHandler

The Directory Services Markup Language v1.0 (DSMLv1) enables the representation of directory structural information as an XML document. DSMLv2 goes further, providing a method for expressing directory queries and updates (and the results of these operations) as XML documents. DSMLv2 documents can be used in a variety of ways. IBM Tivoli Directory Integrator provides an EventHandler which acts as a DSML server and listens to the DSMLv2 request over HTTP (optionally taking advantage of secure communications by means of SSL). After it receives the request, it parses the request and sends the request to an AssemblyLine to process. The result is sent back to the client over HTTP.

The DSMLv2 EventHandler is a simple Web server that provides a way to process a DSMLv2 request that is transferred as HTTP body in an HTTP request message. The DSMLv2 EventHandler automatically parses the client request into an event object and calls a user-defined AssemblyLine configured for the operation of the request. This AssemblyLine often consists of one single Connector in the appropriate mode. See "Configuration." Also, the EventHandler implements HTTP basic authentication if an authenticator Connector is specified.

**Note:** This DSML implementation does not comply fully with the DSMLv2 Specification. It supports limited bindings and operations, and is expressly designed for usage with ITIM only.

An example DSMLv2 EventHandler can be found in the examples directory (*<TDI\_installation directory>\examples\event\_handler\_dsmlv2\_http\DSML\_EH\_Test.xml*).

## Transportation (binding)

DSMLv2 requests and responses are transported over HTTP as HTTP body to or from the DSML Client and the DSMLv2 EventHandler. SOAP and File bindings are not part of this EventHandler.

## EventHandler Workflow

Here is how the EventHandler processes a DSMLv2 request:

1. The DSMLv2 EventHandler receives a batch DSML request as a single event.
2. Each individual request from the batch request is parsed by the DSMLv2 Parser into a single Entry and fed to the AssemblyLine configured to process the operation type of that individual request (search, modify, add, etc.).
3. Result Entry(ies) generated by an AssemblyLine is (are) parsed into individual DSMLv2 response message which is accumulated.
4. When all individual requests are processed and the resulting DSML response messages are created, a batch response message containing all individual response messages is returned by the EventHandler to the client.

For RootDSE search requests, the EventHandler never initiates an AssemblyLine. It returns a list of Root Naming Contexts that are configured.

The DSMLv2 EventHandler ignores and does **not** execute the "Action Map" workflow.

## Operations

The DSMLv2 EventHandler uses internally the DSMLv2 Parser to parse and create DSML messages. Therefore it supports the following DSML operations: **Modify**, **Add**, **Delete**, **Search**, **ModifyDN** and **Compare**.

## Configuration

The EventHandler needs the following parameters:

### HTTP Port

The TCP port on which this Event Handler will be listening.

### Auth Realm

The authentication realm sent to the client when requesting authentication.

### Auth Connector

The authenticator Connector. If you specify a Connector, it must exist in your Connector library and be configured for Lookup.

**Note:** Do not use any of the possible Hooks in the Auth Connector, as the Connector is called internally by the EventHandler and is not executed in the context of an AssemblyLine; the normal environment for Hooks does not apply.

This EventHandler issues authentication requests to any client (for example, Web browser) that tries to access this service. When the client provides the username and password, the EventHandler calls the authenticator Connector's Lookup method providing the username and password attributes. Therefore, your authenticator Connector must be configured using a Link Criteria where you use the \$username and \$password. A typical link criteria might be:

```
username equals $username
password equals $password
```

If the search fails, the EventHandler denies the request and sends an authentication request back to the client. If the search succeeds, the authentication is considered successful and your code in the EventHandler is processed. You can access the username by retrieving the HTTP attribute or property **http.remote\_user**. You can access the entry returned by the authenticator Connector by retrieving the event Property **auth.entry**, by using code similar to the following:

```
var auth = event.getProperty("auth.entry");
var fullName = auth.getString("FullName");
```

### Headers As Properties

If this checkbox is checked, all HTTP headers are accessible using the `getProperty` method of the event object. If not checked, all HTTP headers appear as attributes (for example, **getAttribute**).

### Use SSL

Check this checkbox if you want to use SSL.

**Note:** In order to use SSL, you must generate your own certificate in your keystore (with `keytool`). The client must import this certificate.

### Chunked Transfer Coding

If this field is checked, the body of the response message is transferred as a series of chunks.

**Note:** The Chunked Transfer Coding is incompatible with ITIM.

### Binary Attribute

This field is used to specify user-defined binary attributes. Each attribute is checked to determine if it is a binary attribute. If it is a binary attribute, it is decoded before sending it to the AssemblyLine and encoded (if it is not encoded already) before sending the response to the client.

### Naming Context

The root naming context to be associated with the set of operation AssemblyLines (specified below). Value for the Distinguished Name (dn) in the request is used to match the proper Root Naming Context. More than one naming context can be specified and each one has its own set of AssemblyLines associated.

### AssemblyLine for search

The name of the AssemblyLine to be used for a search operation for the selected Root Naming Context. All Entries returned from the AssemblyLine's iterations are accumulated and returned to the client as multiple DSML search result entries.

**AssemblyLine for add**

The name of the AssemblyLine to be used for an add operation for the selected Root Naming Context.

**AssemblyLine for modify**

The name of the AssemblyLine to be used for a modify operation for the selected Root Naming Context. If Update LDAP Connector is used to modify an entry in LDAP server, Link criteria must be:

```
$dn equals $$dn
```

**AssemblyLine for delete**

The name of the AssemblyLine to be used for delete operation for the selected Root Naming Context. The link criteria of a Delete LDAP Connector in the AssemblyLine must be:

```
$dn equals $$dn
```

**AssemblyLine for compare**

The name of the AssemblyLine to be used for a compare operation for the selected Root Naming Context. The AssemblyLine does compare the value of the matching entry. If Lookup LDAP Connector is used to compare, you can use the code similar to the following in the **In Prolog->Before Initialize** hook:

```
name = work.getString("dsml.compare_name") + "";
value = work.getString("dsml.compare_value") + "";
```

and in the **Data Flow->Overwrite Lookup** hook:

```
if (compare_conn.connector.compare($dn,name,value))
    conn.setAttribute ("dsml.compare_result", "true");
else
    conn.setAttribute ("dsml.compare_result", "false");
```

**AssemblyLine for modify DN**

The name of the AssemblyLine to be used for a modifyDN operation for the selected Root Naming Context. If Update LDAP Connector is used to modify the DN of an entry in LDAP server, Link criteria must be:

```
$dn equals $$dn
```

In the Output Map, you add \$dn to be modified.

**Auto-start Service**

If this checkbox is checked, this EventHandler is started when the IBM Tivoli Directory Integrator Server instance is started.

**Detailed Log**

If this checkbox is checked, additional log messages are generated.

**Comment**

A comment for your own use.



---

## Exchange Changelog EventHandler

The Exchange Changelog EventHandler detects changes that occur in Exchange Directory Service and notifies a user about these changes. It reports changed Exchange objects so that other data sources can be synchronized with Exchange.

**Note:** The “Exchange Changelog EventHandler” is deprecated for this release, and will be removed in future versions of TDI.

The LDAP protocol is used for retrieving changed objects.

The EventHandler uses the Exchange Changelog Connector internally to get changed objects from Exchange Directory Service. Changed objects retrieval is based on the “USN-Changed” mechanism.

See “Exchange Changelog Connector” on page 71 for details about the order of changes retrieval, structure of the delivered Entries, and specific details about handling deleted objects.

### Notes:

1. Exchange Changelog EventHandler works with Exchange 5.5 only. If you are attempting to connect to Exchange 2000, use the Active Directory Changelog EventHandler instead.
2. The Exchange 5.5 Service Pak 4 must be installed on the Exchange Server.

## Behavior

When the EventHandler starts, it connects to Exchange Directory Service and retrieves all recent directory changes that have happened while the EventHandler was offline. Then the EventHandler sleeps for a configurable period of time, then it again polls Exchange for new changes, and so on.

Notifications are not lost when the EventHandler is not running. Each time the EventHandler is started, it retrieves the changes that it missed while it was offline.

The Exchange Changelog EventHandler can be interrupted at any time during the synchronization process. The EventHandler saves the state of the synchronization process in the User Property Store of the IBM Tivoli Directory Integrator (after each Entry retrieval), and the next time that the EventHandler is started, the EventHandler successfully continues the synchronization from the point when it was interrupted.

In case Exchange goes offline the EventHandler does not stop and tries to reconnect until either it succeeds or a stop is requested.

## Access to the USN synchronization values in the User Property Store

The state of synchronization at any time is represented by four USN numbers:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

These values are packed and stored in the User Property Store. Do not change these values manually. You might want to archive the numbers corresponding to a certain stage of synchronization and later use these numbers to replay synchronization from that stage.

The following script code can be used in IBM Tivoli Directory Integrator to get USN values stored in the User Property Store:

```
// Retrieve USN values from User Property Store
var usn = system.getPersistentObject("exchange_sync");
var startUsn = usn.getString("START_USN");
```

```

var endUsn = usn.getString("END_USN");
var currentUsnCreated = usn.getString("CURRENT_USN_CREATED");
var currentUsnChanged = usn.getString("CURRENT_USN_CHANGED");

main.logmsg("START_USN: " + startUsn);
main.logmsg("END_USN: " + endUsn);
main.logmsg("CURRENT_USN_CREATED: " + currentUsnCreated);
main.logmsg("CURRENT_USN_CHANGED: " + currentUsnChanged);

```

"exchange\_sync" is the name of a parameter already stored in the User Property Store. The EventHandler parameter **Persistent Parameter Name** specifies this value. The previous example dumps the values to the screen, however, you might want to perform other actions such as saving values in a file and backing up this file.

The next example of script code shows how the USN values can be stored in the User Property Store:

```

// Store USN values in the User Property Store
var usn = system.newEntry();
usn.setAttribute("START_USN", startUsn);
usn.setAttribute("END_USN", endUsn);
usn.setAttribute("CURRENT_USN_CREATED", currentUsnCreated);
usn.setAttribute("CURRENT_USN_CHANGED", currentUsnChanged);
system.setPersistentObject("exchange_sync", usn);

```

This code assumes that the variables *startUsn*, *endUsn*, *currentUsnCreated* and *currentUsnChanged* contain the USN numbers as strings. This example saves the USN values under the "exchange\_sync" parameter, and so "exchange\_sync" must be specified in the EventHandler's **Persistent Parameter Name** parameter to continue synchronization from the desired point.

## Access to the runtime EventHandler's USN synchronization values

The Exchange Changelog EventHandler provides the following public methods to access its current USN values:

### **public Entry getUsnValues ();**

Returns an Entry object with the following attributes:

- START\_USN
- END\_USN
- CURRENT\_USN\_CREATED
- CURRENT\_USN\_CHANGED

The value of each of the attributes is of type **java.lang.Integer** and represents the corresponding EventHandler's USN value.

### **public void setUsnValues (Entry usnEntry);**

Sets the EventHandler's current USN synchronization values to the values specified in the usnEntry parameter. The structure of the usnEntry parameter should be the same as the structure of the Entry returned by getUsnValues(). The values of the usnEntry attributes must be either **java.lang.Integer** or the string representations of the corresponding numbers.

**Note:** Be careful when changing the USN values at runtime. Specifying inconsistent values can result in improper synchronization.

## Configuration

The EventHandler needs the following parameters:

### **LDAP URL**

The LDAP URL of the Active Directory service you want to access. The LDAP URL has the form `ldap://hostname:port` or `ldap://server_IP_address:port`. For example, `ldap://localhost:389`



**Note:** The default LDAP port number is 389. When using SSL the default LDAP port number is 636.

#### **Login username**

The distinguished name used for authentication to the service. For example, **cn=administrator,ou=domain\_name,o=organization\_name**.

**Note:** If you use **Anonymous** authentication, you must leave this parameter blank.

#### **Login password**

The credentials (password).

**Note:** If you use **Anonymous** authentication, you must leave this parameter blank.

#### **Authentication Method**

The authentication method to be used. Possible values are:

- Anonymous (use no authentication)
- Simple (use weak authentication (cleartext password))

#### **Use SSL**

Specifies whether to use Secure Sockets Layer for LDAP communication with Exchange Server.

#### **LDAP Search Base**

The specified Exchange sub-tree which is polled for changes. For example, **cn=recipients,ou=domain\_name,o=organization\_name**.

#### **Persistent Parameter Name**

Specifies the name of the parameter that stores the current synchronization state in the User Property Store of the IBM Tivoli Directory Integrator. This must be a unique name for all parameters stored in one instance of the IBM Tivoli Directory Integrator User Property Store.

#### **Start At**

Specifies either **EOD** or **0**. **EOD** means report only changes that occur after the EventHandler is started. **0** means perform full synchronization, that is, report all objects available in Exchange Directory Service. This parameter is taken into account only when the parameter specified by the **Persistent Parameter Name** parameter is not found in the User Property Store.

#### **"Is-Deleted" Attribute visible**

Specifies whether the Exchange server exposes the **Is-Deleted** object attribute through LDAP.

**Note:** If the server does expose the **Is-Deleted** attribute, but **"Is-Deleted" Attribute visible** is set to **false**, then the EventHandler still works properly, but you can accelerate the EventHandler by setting **"Is-Deleted" Attribute visible** to **true**. If the server does not expose the **Is-Deleted** attribute, but **"Is-Deleted" Attribute visible** is set to **true**, then the EventHandler cannot distinguish between a modified object and a deleted object and reports all deletions as modify operations.

#### **Sleep Interval**

Specifies the number of seconds the EventHandler sleeps between successive polls for changes.

#### **Detailed Log**

Specifies whether detailed debug information is written to the log file.

#### **Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

## **See also**

"Migration of Changelog EventHandlers" on page 237.



---

## HTTP EventHandler

The HTTP EventHandler is a simple Web server that provides a simpler way to deal with HTTP connections than the TCP EventHandler. The HTTP EventHandler automatically parses the client request into an **event** object using the HTTP Parser. In addition the EventHandler implements HTTP basic authentication if you specify an authenticator Connector.

When dealing with events, the EventHandler forks new instances of itself, so the Prolog and Epilog are started once for each HTTP event received.

To provide simple Web server functionality, you need to provide the **http.body** and **http.content-type** attributes that the EventHandler returns as the response to a request. You can also add HTTP headers by setting any *http.\** attribute. For example, setting the value for **http.my-header** causes this EventHandler to generate a **my-header: value** in the response.

The **http.body** property can be set to any of the following

### Any string (java.lang.String)

The string is sent "as is" in the request.

### Any Input stream ( java.io.InputStream )

The input stream is buffered into memory to compute the *content-length* HTTP header. The input stream data is sent "as is" in the request.

### A Java file object (java.io.File)

The *content-length* is generated by getting the file size from the file object. Then the contents of the file is sent "as is" in the request.

## Example

The following example returns any file the client requests:

```
var base = event.getProperty("http.base");
if ( base == "/" )
    base = "/index.html";
// Construct the full path
path = "/home/httpd/documents" + base;

// Construct the Java file object
file = new java.io.File ( path );

// Set the response property
event.setProperty ( "http.body", file );
```

## Configuration

### HTTP Port

The TCP port on which this handler is listening.

### Auth Connector

The authenticator Connector. If you specify a Connector it must exist in your Connector library and be configured for Lookup. This EventHandler issues authentication requests to any client (for example, Web browser) that tries to access this service. When the client provides the username or password, the EventHandler calls the authenticator Connector's Lookup method providing the username and password attributes. Therefore, your authenticator Connector must be configured using a Link Criteria where you use the \$username and \$password. A typical link criteria might be:

```
username equals $username
password equals $password
```

If the search fails, the EventHandler denies the request and sends an authentication request back to the client. If the search succeeds, the request is granted and your code in the EventHandler is executed. You can access the username by retrieving the HTTP attribute or property **http.remote\_user**. You can access the entry returned by the authenticator Connector by retrieving the Property **auth.entry**, using code similar to the following:

```
var auth = event.getProperty("auth.entry");  
var fullName = auth.getString("FullName");
```

### Headers As Properties

If checked, all HTTP headers are accessible using the `getProperty` method of the event object. If not, all HTTP headers appear as attributes (for example, **getAttribute**).

### Use SSL

Check the checkbox if you want to use SSL.

**Note:** In order to use SSL, you must generate your own certificate in your keystore (with `keytool`). The client must then import this certificate.

### Comment

A comment for your own use.

### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## See also

"EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*,  
"HTTP Parser" on page 297.

---

## IBM Directory Server EventHandler

The IBM Directory Server EventHandler uses LDAP unsolicited event notifications to detect changes in an LDAP directory. To use the IBM Directory Server EventHandler your LDAP server must support LDAPv3 unsolicited notification events.

When the EventHandler starts, it connects to the LDAP server and retrieves all recent directory changes, which have happened while the EventHandler was offline, and registers for receiving unsolicited event notifications. When an event occurs in the LDAP directory, the EventHandler receives an unsolicited notification event and retrieves the next changelog entry. This changelog entry is accessible as the **event** entry object. The **event** entry object has the following attributes:

### **changenumber**

The change number as assigned by the supplier. This integer must increase as new entries are added, and always be unique within a given server.

This attribute is Required.

### **targetdn**

The distinguished name (DN) of the entry which was added, modified, or deleted; in the case of a **modrdn** operation, the **targetdn** gives the DN of the entry before it was modified.

This attribute is Required.

### **changetype**

The type of change (**add**, **delete**, **modify**, or **modrdn**).

This attribute is Required.

### **changes**

The changes that were made to the directory server. These changes are in LDIF format; available when **changetype** is either **add** or **modify**.

This attribute is Optional.

### **newrdn**

The new Relative Distinguished Name (RDN) of the entry. If the **changeType** is **modrdn**, or if the **changeType** attribute does not have the **modrdn** value, then there are no values contained in the **newrdn** attribute.

This attribute is Optional.

### **deleteoldrdn**

A flag which tells whether the old RDN of the entry must either be retained as a distinguished attribute of the entry or be deleted.

This attribute is Optional.

### **newsuperior**

If present, it gives the name of the entry which becomes the immediate superior of the existing entry.

This attribute is Optional.

### **changetime**

The time when the change was made.

This attribute is Required.

### **modifiersname**

The DN making the change.

This attribute is Optional.

An important feature of the IBM Directory Server EventHandler is that notifications are not lost when the EventHandler is not running or waiting for an action to complete, because each time it is invoked it retrieves the changes that it has missed while being offline, and iterate through them, simulating the reception of an event for every change.

**Note:** Even though the EventHandler will not miss any notifications as outlined above, some thought needs to be given as to how much work is performed to process each event. Starting an AssemblyLine to process a single change may not be a viable strategy in certain high volume scenarios. In such a case, it may be better to base your solution upon using an LDAP ChangeLog Connector.

## Configuration

### LDAP URL

The LDAP URL (`ldap://hostname:port`)

### Login username

The distinguished name used for authentication to the server (for example, `cn=root`).

**Note:** This distinguished name must have administrator privileges because the EventHandler must be able to read the changelog.

### Login password

The credentials (password).

### ChangeLog Search Base

The search base where the changelog is stored. The standard DN for this is `cn=changelog`.

### Search Base

The base of the directory tree branch about which you want to be notified. Specify a distinguished name. Some directories enable you to specify a blank string which defaults to whatever the server is configured to do. Other directory services require this to be a valid distinguished name in the directory.

### Search Scope

The scope of events which you want to be notified about. Can be one of subtree, level and base.

### ChangeNumber Filename

The name of the file where the last changenumber is stored. The file format is readable text. This file is updated after each event notification.

### InitialChangeNumber

If the file supplied in the **ChangeNumber Filename** parameter does not exist, the EventHandler retrieves the changelog entries, starting from **InitialChangeNumber**.

### Comment

A comment for your own use.

### Authentication Method

The authentication method. Possible values are:

- MD5-CRAM (use CRAM-MD5 (RFC-2195))
- SASL (use SASL)
- Anonymous (use no authentication)
- Simple (use weak authentication (cleartext password))

If not specified, the default (**Anonymous**) is used. If either the **Login username** or **Login password** parameter is blank, then **Anonymous** is used.

### Use SSL

Specifies whether to use SSL for communication with the LDAP server.

**Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**See also**

"EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*,

"LDAP EventHandler" on page 259,

"Migration of Changelog EventHandlers" on page 237.





---

## LDAP EventHandler

This EventHandler uses the LDAP event notification mechanism to detect changes in an LDAP directory. To use this EventHandler, your LDAP server must support Persistent Search. The only LDAP server tested with this EventHandler is the Netscape/iPlanet/SunONE directory server (see the 133 for more about iPlanet), but other LDAP servers may work as well.

**Note:** If you can base your change detection in your LDAP database upon reading a Changelog (using an appropriate Changelog Connector) instead of relying upon the events signalled by the LDAP database by means of the Persistent Search mechanism, your solution is much more robust. The Persistent Search mechanism is very ephemeral: you only see changes if you are actually listening while the changes occur. If the connection is down you miss them. A Changelog, on the other hand, is backed by mass storage, and given the right System Change Number you can always pick up processing from where you last stopped.

When the EventHandler starts, it connects to the LDAP server and specifies the selection criteria for event notifications. All DN's returned from the EventHandler are relative to the search base specified. To construct the full DN in a flexible way, you can append the search base to, for example, the new DN with the following code in a custom script

```
event.setProperty("ldap.newdn", event.getProperty("ldap.newdn") +  
    ", " + task.getParam("ldapSearchBase"));
```

When an event occurs in the LDAP directory, the EventHandler sets the **ldap.operation** property to one of the following values:

### **objAdded**

A new entry was added to the directory.

### **objRenamed**

An existing entry was renamed.

### **objModified**

An existing entry's attributes were modified.

### **objRemoved**

An existing entry was removed.

### **handleError**

An error was encountered.

Depending on the **ldap.operation**, the EventHandler sets the following properties:

## **Object Added (\_objAdded)**

### **ldap.newdn**

The new DN in case of a rename operation

### **ldap.newentry**

The new entry with changes applied

## **Object Rename (\_objRenamed)**

### **ldap.dn**

The old DN

### **ldap.newdn**

The new DN

## Object Modified (**\_objModified**)

### **ldap.dn**

The DN before the modify operation.

### **ldap.entry**

The contents of the LDAP entry before the modify operation. This functionality is only available for LDAP databases where a modification operation is done by first removing the object and then recreating it with the modified attributes.

### **ldap.newdn**

The DN after the modify operation.

### **ldap.newentry**

The contents of the LDAP entry after the modify operation.

## Object Removed (**\_objRemoved**)

### **ldap.dn**

The DN before the remove operation

### **ldap.entry**

The contents of the LDAP entry before the remove operation

The **ldap.entry** and **ldap.newentry** properties are instances of the Entry class so you can access these as you normally do with **conn** and **work** objects in the AssemblyLine as shown in the following example:

```
var old = event.getProperty ("ldap.entry");
task.logmsg ("Old common name = " + old.getString("cn") );
```

**Note:** One important aspect of the LDAP EventHandler is that you can lose important notifications when the EventHandler is not running. This EventHandler is best used when you want to trap changes in a directory but still can tolerate loss of information.

## Error Encountered (**\_handleError**)

### **ldap.error**

The java exception thrown by the EventHandler.

**Note:** iPlanet Directory 5.0 has changed the changelog to a proprietary format. Go to the following URL:

```
http://docs.ipplanet.com/docs/manuals/directory/51/html/ag/replicat\_new.htm#1
```

You must install the Retro ChangeLog Plug-in for accessing the change log. The following is an extract from the Change Log section of the iPlanet documentation:

"In iPlanet Directory Server 5.0, the format of the change log was modified. In earlier versions of Directory Server, the change log was accessible over LDAP. Now, however, it is intended only for internal use by the server. If you have applications that need to read the change log, you need to use the Retro Change Log Plug-in for backward compatibility. For more information, refer to the Retro Change Log Plug-In."

## Configuration

The EventHandler needs the following parameters:

### **LDAP URL**

The LDAP URL for the connection (*ldap://host:port*).

### **Login username**

The distinguished name used for authentication to the server.

**Login password**

The credentials (password).

**Search Base**

The search base to be used when iterating the directory. Specify a distinguished name. Some directories enable you to specify a blank string which defaults to whatever the server is configured to do. Other directory services require this to be a valid distinguished name in the directory.

**Search Filter**

The search filter to be used when iterating the directory.

**Search Scope**

This parameter is only used if the Connector is in Iterator mode. The possible values are:

**subtree**

Return entries on all levels from search base and below.

**onelevel**

Return entries that are immediately below searchbase only.

**Comment**

A comment for your own use.

**Authentication Method**

Type of LDAP authentication. Can be one of the following:

- Simple (using ldapUsername/ldapPassword). Treated as anonymous if username or password are not provided)
- MD5-CRAM
- SASL
- Anonymous (treated as Simple if username and password are supplied)

**Use SSL**

If this is checked, use secure sockets layer for communication with the LDAP server.

**Connector Flags**

Flags to enable specific behavior.

**deleteEmptyStrings** - This flag causes the Connector to remove attributes containing only an empty string as value before updating the directory. If you are using an LDAP version 3 server, use this flag, as the value of an attribute cannot be an empty string.

**Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**See also**

"EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*,  
"IBM Directory Server Changelog Connector" on page 97.



---

## LDAP Server EventHandler

The LDAP Server EventHandler accepts an LDAP connection request from an LDAP client. The LDAP Server EventHandler generates a copy of itself to take care of this connection until the connection is closed by the LDAP client. The LDAP Server EventHandler only terminates when the TCP connection is closed. Each LDAP message received on the connection drives one cycle of the LDAP Server EventHandler logic. The main thread returns to listening for similar LDAP requests from other LDAP clients. The LDAP operation in the message is parsed into the LDAP Server EventHandler entry object. The LDAP Server EventHandler code is executed, and the return message is built and sent back to the client. If it was an LDAP search command, the user will call the **add** method to build the data structure that is to be sent back to the client. The LDAP Server EventHandler goes back to listening for the next LDAP command on the existing connection.

The value of the LDAP operation is provided in the **LDAP.operation** attribute in the LDAP Server EventHandler **work** entry. Legal values are **SEARCH**, **BIND**, **UNBIND**, **COMPARE**, **ADD**, **DELETE**, **MODIFY**, and **MODIFYRDN**. The LDAP message provides a number of attributes for the specified LDAP operation. To facilitate scripting, the parser copies the LDAP message into the LDAP Server EventHandler **work** object.

### Scripting

The LDAP Server EventHandler must do work to determine the desired outcome of the LDAP message. The code can reside in the LDAP Server EventHandler, or the LDAP Server EventHandler can start an AssemblyLine to do the work. The basic LDAP operations (**SEARCH**, **BIND**, **UNBIND**, **COMPARE**, **ADD**, **DELETE**, **MODIFY**, and **MODIFYRDN**) are provided as values in the LDAP Server EventHandler scripting environment to facilitate scripting, for example, if **LDAP.operation** equals **BIND**. The user code sends search result entries to the client by calling the **add ( entry )** method in the LDAP Server EventHandler. The entry must be formatted with legal LDAP attribute names plus the special attribute **\$dn** (the distinguished name of the entry).

### Returning the LDAP message returned values

The user-provided code in the LDAP Server EventHandler responds to each request by setting the **ldap.status**, **ldap.matcheddn** and **ldap.errorMessage** entry attributes. **ldap.matcheddn** and **ldap.errorMessage** are optional.

At the end of the LDAP Server EventHandler execution cycle, the LDAP Server EventHandler formats and returns some of the attributes of the **work** entry. These are:

- **LDAP.status**
- **LDAP.errorMessage**

**Note:** Only string is supported. The **resultCode** is by default set to **0** (success). A **resultCode** indicating anything other than successful must be specifically set by the user.

### Error handling

The LDAP Server EventHandler terminates the connection and records an error if the received message does not conform to the LDAP v3 format

**Note:** The LDAP Server EventHandler does not perform any validation on the incoming attributes. Any operation or parameter value is therefore accepted.

### Configuration

The EventHandler needs the following parameters:

#### LDAP Port

The TCP port on which this EventHandler listens.

**Character Encoding**

Specify the character set here. The default is **UTF-8**.

**Binary Attributes**

A list of attributes that are treated as binary (a binary attribute is returned as a byte array, not a string). The format is one attribute name on each line.

**Note:** An AssemblyLine can have one list of binary attributes only. If you have several LDAP Connectors in an AssemblyLine, the last Connector must define the list of binary attributes for all the LDAP Connectors in this AssemblyLine (if you need to change this from the default).

**Comment**

A comment for your own use.

**Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Use SSL**

If checked the server will only accept SSL connections.

**Note:** Depending on your solution implementation, you may need to change the port number as well.

---

## Mailbox EventHandler

This EventHandler listens for changes in a mailbox. Depending on the protocol the handler either polls the mailbox periodically by reconnecting to the mailbox (POP3) or periodically issues idle messages on the connection (IMAP4).

### Configuration

This EventHandler needs the following parameters:

**Server Name**

The mail server hosting the mailbox.

**Protocol**

Specify POP3 or IMAP.

**Login Username**

The user name.

**Login Password**

The password for **Login Username**.

**Mail Folder**

The mail folder to monitor. For POP3 this can only be INBOX. For IMAP4 servers this can be any folder available on the server.

**Poll Interval (seconds)**

Number of seconds between each poll. Be aware that for POP3 this incurs a new connection each time.

**Auto-start Service**

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

### Objects/properties/attributes

The EventHandler sets the following event properties:

**event.originator**

The EventHandler object.

**mailbox.session**

The Java session object (javax.mail.Session).

**mailbox.store**

The message store object (javax.mail.Store).

**mailbox.folder**

The folder object (javax.mail.Folder).

**mailbox.message**

The message object (javax.mail.Message).

**mailbox.operation**

The operation related to mailbox.message. For pop3 connections only *existing* entries are reported. For imap connections this property contains the value *new* or *deleted*.

**mail.subject**

The subject header from the mail.message.

**mail.from**

The from header from the mail.message.

**mail.to**

The first recipient in the mail.message.

**Examples**

Go to the *root\_directory/examples/event\_handler\_mailbox* directory of your IBM Tivoli Directory Integrator installation.

**See also**

"EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.



---

## SNMP EventHandler

SNMP is a standard wire-level protocol used to query and set published attributes in remote systems. Typically, it is used by a monitoring console to configure and get status information from a wide range of SNMP-compliant systems.

**Note:** This implementation of the SNMP EventHandler supports protocols up to version 2.

The SNMP EventHandler receives UDP packages on a specified port, and returns an appropriately formatted response to the originator. The implementation is non-blocking by default, meaning the SNMP EventHandler spawns a copy of itself to perform the work while the main thread returns to listen for further packets (the main thread can be set to blocking as well).

Setting the community string enables the SNMP EventHandler to ignore incoming SNMP requests that do not contain this specific string. Leaving the community string blank results in all SNMP packets arriving in the SNMP EventHandler.

The value of the SNMP operation is provided in the **SNMP.operation** attribute in the SNMP EventHandler **work** entry. Legal values are **GET**, **GETNEXT**, **SET** and **TRAP**. A single SNMP message can request an operation on multiple OIDs (OID is an address into a MIB structure, indicating a specific variable or attribute to be read or modified in the target system). A GET can contain a list of OIDs, while a SET can also include the corresponding values to be set for those variables in the target system. However, most SNMP deployments use only one OID per SNMP message.

To facilitate scripting, the parser copies the OID table into two multi-valued attributes in the SNMP EventHandler **work** object: **SNMP.OID**, containing the desired OID, and **SNMP.OIDvalue**, which contains the corresponding value. **OIDValue** contains **java.lang.Integer** or **java.lang.String** values. After parsing, the SNMP EventHandler **work** object contains the following:

- The community-string in **SNMP.community**
- The originating IP Address in **SNMP.remoteIP**
- The SNMP sequencing number in **SNMP.requestId**
- The attributes **SNMP.errorcode** (value set to 2) and **SNMP.errorindex** (value set to 0)

TRAP messages contain an additional set of values:

- **SNMP.enterprise** – OID for object-generating trap
- **SNMP.agentAddress** – address of object-generating trap
- **SNMP.specificTrap**, **SNMP.genericTrap** – has value when **specificTrap = 6**
- **SNMP.timeTicks** – time since last initialization of object-generating trap

## Scripting the desired action

The SNMP EventHandler must do work to determine the desired outcome of the SNMP message. The code can reside in the SNMP EventHandler, or the SNMP EventHandler can start an AssemblyLine to get the work done.

The basic SNMP operations (**GET**, **GETNEXT**, **SET** and **TRAP**) are provided as values in the SNMP EventHandler scripting environment to facilitate scripting, for example, if **SNMP.operation** equals **GET**. By modifying the **SNMP.OID** and **SNMP.OIDvalue** attributes, you can build content that is sent back in the return message. The return error code is manipulated by setting the value of the SNMP EventHandler **SNMP.errorcode** attribute and **SNMP.errorindex** (the entry in the OID table that contains the error).

## Error handling

SNMP supports return error codes that are part of the **GET-RESPOND** return message. Messages that do not conform to the SNMP format are not processed by the SNMP EventHandler, but control is given to the Epilog, where a user can add customized code:

- The default error code is **2**, indicating that no work has been done. An error code **0** indicating success must be specifically set by the user.
- Only standard SNMP-compliant error codes can be set by the user. The SNMP EventHandler overwrites an error code with the value **5** (interpreted as other error) if the value is outside the supported range before turning the message to the originator.

## Returning the SNMP packet returned values

The SNMP EventHandler formats and returns some of the attributes of the **work** entry. These are:

- **SNMP.OID**
- **SNMP.OIDValue**

**Note:** Only **string**, **integer** and **NULL** are supported. **java.lang.String** is mapped to **OctetString** and **java.lang.Integer** is mapped to **integer**.

- **SNMP.errorcode**

**Note:** The default value is **2**. If the user tries to set **SNMP.errorcode** to something outside the range **0-5**, **SNMP.errorcode** is set to **5** before being returned.

- **SNMP.errorindex**

**Note:** Set to the (zero-based) index in the OID table of the OID value that caused the error.

**Note:** According to the SNMP protocol, only one error can be reported. In case of multiple errors, **SNMP.errorindex** must be the lowest index indicating an error. The user is responsible to set this value correctly.

## Configuration

This EventHandler needs the following parameters:

### UDP Port

The SNMP default UDP port for get/set operations is 161, but is configurable. TRAPs are usually received on port 162.

### Verify Community

If set, discard all messages not matching this community string. If blank, enable all community strings.

### Multi threaded

Check to create a new thread for each event.

### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

### Detailed Log

If this field is checked, additional log messages are generated.

---

## TCP Port EventHandler

This EventHandler waits for incoming TCP connections on a specified port and spawns a new thread to handle the incoming request. When the new thread has started, the original EventHandler goes back to listening mode. When the newly created thread has completed, the thread stops and the TCP connection is closed.

This EventHandler is forking, so the Prolog and Epilog are started once for each HTTP event received.

**Note:** The TCP Port EventHandler is deprecated for release 6.1.1 of IBM Tivoli Directory Integrator, and will be removed in a future release. Build your solution using the TCP Server Connector instead.

## Configuration

### TCP Port

The TCP port on which to listen for incoming connections.

### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Objects/properties/attributes

The EventHandler sets the following event properties:

### **event.originator**

The EventHandler object

### **event.inputstream**

TCP socket input stream

### **event.outputstream**

TCP socket output stream

### **tcp.remoteIP**

Remote IP address (dot notation)

### **tcp.remotePort**

Remote TCP port number

### **tcp.remoteHost**

Remote hostname

### **tcp.localIP**

Local IP address - dot notation

### **tcp.localPort**

Local TCP port number

### **tcp.localHost**

Local hostname

### **tcp.socket**

TCP Socket object (java.net.Socket)

## Examples

Go to the *root\_directory/examples/event\_handler\_tcp* directory of your IBM Tivoli Directory Integrator installation.

## See also

"EventHandler" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.

---

## Generic thread (primitive EventHandler)

The generic thread is started at startup and continues to run as long as the script runs. The script can call the `task.sleep(milliseconds)` to periodically perform its work.

### Configuration

The port listener needs the following parameters:

#### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

#### Detailed Log

Specifies whether more detailed log information is written to the log file.

**Script** The script to run.

### See also

“Mailbox EventHandler” on page 265.



---

## Timer EventHandler (primitive EventHandler)

The timer waits for a specified time, when it starts a script or starts an AssemblyLine. The script must be provided by the administrator or user.

### Configuration

This EventHandler needs the following parameters:

#### Auto-start Service

If this field is checked, this EventHandler is started when IBM Tivoli Directory Integrator is started.

#### Schedule

This parameter decides when the EventHandler is run. The format is as follows:

<month> <day> <weekday> <hour> <minute>

The fields have numeric values:

- Month = 0 – 11 (January . . . December)
- Day = 1 – 31
- Weekday = 1 – 7 (Sunday . . . Saturday)
- Hour = 0 – 23
- Minute = 0 – 59

Fields are separated by white space. Enter "\*" to specify any value. You can specify multiple values for any field, separated by commas, but the values must be in ascending order.

When the current time matches all the fields in the schedule, the specified AssemblyLine is run. For example:

- \* \* 5 22 0 - Run every Thursday at 22:00 hours
- \* 3 \* 22 0 - Run every 3rd of each month at 22:00 hours

#### Notes:

1. The month field has values from 0 to 11, while day and weekday values begin at 1.
2. A common source of confusion is specifying both a day and a weekday. Both attributes must match, meaning that this event does not occur often.

#### Run AssemblyLine

The AssemblyLine to start.

#### Detailed Log

If this parameter is checked, more detailed log messages are generated.

**Script** If specified, the script must contain a function called **ontimer**. This function is called with no parameters whenever the time specified by the schedule parameter is reached, and then the AssemblyLine is started. The schedule of the EventHandler can be modified through the **timer** object. You reconfigure the timer by setting the schedule parameter from the **ontimer** function. For example:

```
function ontimer()
{
timer.setParam ("schedule", "* * * 22 0");
}
```

### Examples

Go to the *root\_directory/examples/event\_handler\_timer* directory of your IBM Tivoli Directory Integrator installation.





---

## z/OS LDAP Changelog EventHandler

The z/OS LDAP Changelog EventHandler iterates through the change records in the z/OS LDAP server (RACF accessed through its LDAP interface). This EventHandler is very similar to the IBM Directory Server EventHandler (see “IBM Directory Server EventHandler” on page 255). The difference is that this EventHandler polls the changelog instead of using Unsolicited Event Notification.

**Note:** The z/OS LDAP Changelog EventHandler does not currently support Unsolicited Event Notification.

The z/OS LDAP server creates change records when certain events happen in its LDAP Directory (**add**, **modify**, **delete**, and so forth). This EventHandler is used to iterate through those change records and initiate AssemblyLines as configured by the user.

Use this EventHandler as you might use the IBM Directory Server EventHandler. The z/OS LDAP Changelog EventHandler can be used just as effectively with the IBM Directory Server instead of the existing IBM Directory Server EventHandler.

### Configuration

The EventHandler needs the following parameters:

#### LDAP URL

The URL to reach the z/OS LDAP server. This URL is in the format: `ldap://hostname.domain:port`

#### Login username

The DN to authenticate to the LDAP server.

#### Login password

The password to authenticate to the LDAP server (for **Login username**).

#### ChangeLog Search Base

The suffix used for changelog. In the case of z/OS, it is always **cn=changelog** (**cn=changelog** is the default).

#### Search Base

The part of the directory tree that you are interested in changing. For example, if search base is **o=ibm,c=us**, the EventHandler responds to all changes in the **o=ibm,c=us** tree, but not those in **o=ms,c=us**.

#### Search Scope

The scope to use in conjunction with search base (the default is subtree). See previous example (**Search Base**). If scope was set to **baseObject**, changes to the given object only are triggered.

#### ChangeNumber Filename

The file to store the last processed change number in (this is a plain text file).

#### InitialChangeNumber

If **ChangeNumber Filename** does not exist, this number is used as the starting point for the changelog processing. If **ChangeNumber Filename** exists, this field is ignored.

#### PollInterval

The time (in seconds) that the EventHandler sleeps between successive polls to the changelog.

#### Comment

Write any comments you want.

#### Authentication Method

The type of authentication method to use for the LDAP connection.

#### Use SSL

Initiates SSL to the LDAP server (be sure to change port in **LDAP URL**).

### Auto-start Service

Check this checkbox if you want this EventHandler to start automatically when the server starts.

### Detailed Log

Turns on debug logging in the EventHandler.

## Polling logic

Because the z/OS LDAP server does not currently support Event Notification, a polling mechanism is used to check for new entries in the changelog.

When the EventHandler starts, it attempts to read the last processed change number from the file specified in the configuration. If this file does not exist, the **InitialChangeNumber** as specified in the **Config ...** panel is used.

A root DSE search is done to retrieve the **lastchangenumber** attribute. If the current **changenumber** (from file or **Config ...**) is less than the **lastchangenumber**, then the EventHandler uses an LDAP Connector to request the next sequential **changenumber** from z/OS LDAP.

If the entry described in that changelog entry fits within the search boundaries, the event is dispatched and the **changenumber** is incremented. If the entry does not fit the search boundary, or the entry does not exist, the **changenumber** is incremented and the entry is ignored.

This comparison against the **lastchangenumber** is continued until the **changenumber** is equal to the **lastchangenumber**. When this condition is true, it means that the last **changenumber** in the system and the EventHandler goes to sleep for the **PollInterval** as specified in the **Config ...** panel. After this interval has passed, the root DSE is searched again for **lastchangenumber** and the cycle is repeated.

If at any time the **lastchangenumber** attribute is equal to 0, meaning that the changelog is empty, the EventHandler sleeps for the **PollInterval**.

---

## See also

“Migration of Changelog EventHandlers” on page 237.

---

## Chapter 4. Parsers

Parsers are used in conjunction with a transport Connector to interpret or generate the content that travels over the Connector's byte stream.

When the bytestream you are trying to parse is not in harmony with the chosen Parser, you get a `sun.io.MalformedURLException` error. For example, the error message can show up when using the **Schema** tab to browse a file.

---

### Base Parsers

- "CSV Parser" on page 279
- "DSML Parser" on page 281
- "DSMLv2 Parser" on page 283
- "Fixed Parser" on page 295
- "HTTP Parser" on page 297
- "LDIF Parser" on page 301
- "Line Reader Parser" on page 303
- "Script Parser" on page 305
- "Simple Parser" on page 309
- "SOAP Parser" on page 311
- "XML Parser" on page 313
- "XML SAX Parser" on page 317
- "XSL based XML parser" on page 319

---

### Character Encoding conversion

Java2 uses Unicode as its internal Character Encoding. When you work with strings and characters in AssemblyLines and Connectors, they are always assumed to be in Unicode. Most Connectors provide some means of Character Encoding conversion. When you read from text files on the local system, Java2 has already established a default Character Encoding conversion that is dependent on the platform you are running.

The TDI Server has the `-n` command line option, which specifies the character set of Config files it will use when writing new ones; it also embeds this character set designator in the file so that it can correctly interpret the file when reading it back in later.

However, occasionally you read or write data from or to text files in which information is encoded in different Character Encodings (this could happen if you are reading a file created on a machine running a different operating system). The Connectors that require a Parser usually accept a `characterSet` parameter in the Parser configuration. If set, this parameter must be set to one of the accepted conversion tables found in the Java2 runtime, as governed by the IANA Charset Registry. If this parameter is not set, most Parsers use the local character set. Some Parsers might have specific default character sets. See information about individual Parsers in this chapter.

### Availability

Please refer to the IANA Charset Registry (<http://www.iana.org/assignments/character-sets>).

A common character set on Windows computers is CP850; for i5/OS a common value is IBM037.



---

## CSV Parser

The Comma Separated Values (CSV) Parser reads and writes data in a CSV format.

**Note:** In the Config Editor, the parameters are set in the **Parser** tab of the File Connector. If you want to use TAB as a Field Separator you need to specify `\t`, but when supplying Field Names you must use the actual tab character between field names.

On output, multi-valued attributes only deliver their first value.

## Configuration

The Parser has the following parameters:

### Field Separator

Specifies the character used to separate each column. If not specified, the parser attempts to guess when reading, and uses a comma when writing. You can use backslash ( `\` ) as the escape character to specify non-printable characters. For example, ( `\t` ) denotes the TAB character.

### Field Names

Specifies the name for each column the parser must read or write. If not specified, the parser reads the first line and uses the value as field names. You can use the Field Separator between the field names, or specify each name on a separate line.

### Enable Quoting

On write, when this parameter is set to **true**, the field is output with quotes around it under the same conditions as in previous versions, however, quotes inside a quoted field are now doubled.

**Note:** If **Enable Quoting** is set to **false**, the field is output as is, which can cause problems.

When reading, quotes around the field are stripped if this parameter is set to **true**, and the parser is able to read quoted attributes containing the column separator. If this parameter is set to **false**, the parser returns unexpected values when the input contains fields delimited by quotes.

### Write Header

The default value for this parameter is **true**. If **Write Header** is set, the first line output by the parser contains all the field names separated by the column separator.

### Log long lines

Define a maximum number of bytes for a line. Linenumbers of lines longer than this maximum number are logged.

### Character Encoding

Character Encoding conversion. Also see “Character Encoding conversion” on page 277.

### Detailed Log

If this field is checked, additional log messages are generated.



---

## DSML Parser

The DSML Parser reads and writes XML documents. The Parser silently ignores schema entries.

### Configuration

The Parser has the following parameters:

#### DN Attribute

The attribute used for the distinguished name DSML attribute (**\$dn**).

#### DSML prefix

Prefix used on XML elements to indicate that they belong to the DSML namespace. Default is **dsml**.

#### DSML namespace URI

The URI which identifies this namespace. Default is <http://www.dsml.org/DSML>.

#### Omit XML Declaration

If checked, the XML declaration is omitted in the output stream.

#### Document Validation

If checked, this parser requests a DTD/Schema-validating parser.

#### Namespace Aware

If checked, this parser requests a namespace-aware parser.

#### Character Encoding

Character Encoding conversion.

#### Detailed Log

If this parameter is checked, more detailed log messages are generated.

### Examples

The following example shows how you can generate DSML documents dynamically:

```
var dsml = system.getParser ( "ibmdi.DSML" );
var entry = system.newEntry();
entry.setAttribute ( "$dn", "uid=johnd,o=doe.com" );
entry.setAttribute ( "mail", "john@doe.com" );
entry.setAttribute ( "uid", "johnd" );
entry.setAttribute ( "objectclass", "top" );
entry.addAttributeValue ( "objectclass", "person" );
dsml.setOutputStream ( new java.io.StringWriter() );
// Uncomment if you dont want the "<?xml version= ...." header
// dsml.setOmitXMLDeclaration ( true );
dsml.initParser();
dsml.writeEntry ( entry );
dsml.closeParser();

var result = dsml.getXML();
task.logmsg ( result );
```

The following example shows how you can read a DSML document using script:

```
var dsml = system.getParser ( "ibmdi.DSML" );
dsml.setInputStream ( new java.io.FileInputStream("dirdata.dsml") );
dsml.initParser ();

var entry = dsml.readEntry();
while ( entry != null ) {
    task.dumpEntry ( entry );
    entry = dsml.readEntry();
}
```

## See also

"XML Parser" on page 313,  
"SOAP Parser" on page 311,  
"DSMLv2 Parser" on page 283.



---

## DSMLv2 Parser

The Directory Services Markup Language v1.0 (DSMLv1) enables the representation of directory structural information as an XML document. DSMLv2 goes further, providing a method for expressing directory queries and updates (and the results of these operations) as XML documents. DSMLv2 documents can be used in a variety of ways. IBM Tivoli Directory Integrator provides a Parser that can parse and create DSMLv2 request and response messages.

An example can be found in the examples directory (*<installation directory>\examples\event\_handler\_dsmlv2\_http\DSML\_EH\_Test.xml*).

The DSMLv2 Parser is initialized with a DSMLv2 batch request or DSMLv2 batch response. Individual calls to read or write Entries will result in parsing or creation of individual DSML requests or responses (as parts of the batch request or response).

The Parser supports Delta tagging at the Entry level and the Attribute level. See also “Multiple Attribute modifications” on page 290.

### Modes

The DSMLv2 Parser operates either in Server or in Client mode:

- In Server mode the Parser reads/parses DSMLv2 requests and write/creates DSMLv2 responses
- In Client mode the Parser reads/parses DSMLv2 responses and writes/creates DSMLv2 requests.

### Operations

The DSMLv2 Parser supports **Modify, Add, Delete, Search, ModifyDN, Compare, Auth** and **Extended** operations.

**Attention:** The following TDI 6.0 DSMLv2 Parser custom helper objects from the ITIM DSML library are no longer supported:

- dsml.request – for all request operations.
- dsml.response – for all response operations.

If you have configurations using either of these Attributes, you must edit the configurations to remove any reference to these Attributes. The data available through the raw request and response objects in older versions are not available through the other Attributes delivered by the DSMLv2 Parser and DSMLv2 EventHandler.

### Modify Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Modify Requests:

Table 21.

| Attribute      | Value  |
|----------------|--|
| dsml.operation | set to "modifyRequest"   |
| dsml.base      | holds the "dn" XML attribute of the DSML "modifyRequest" element |
| \$dn           | holds the "dn" XML attribute of the DSML "modifyRequest" element |

Additionally, for each modification item: a TDI attribute named as the "name" XML attribute of the DSML "modification" element, with the values specified for the "modification" DSML element and TDI attribute's operation set as the "operation" XML attribute of the DSML "modification" element.

### Modify Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Modify Responses:

Table 22.

| Attribute        | Value   |
|------------------|---|
| dsml.operation   | modifyResponse  |
| \$dn             | holds the "matchedDN" XML attribute of the DSML "modifyResponse" element  |
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response  |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral    | holds a vector containing all referral URIs of the DSML "addResponse" element   |

## Search Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Search Requests:

Table 23.

| Attribute         | Value   |
|-------------------|---|
| dsml.operation    | set to "searchRequest"  |
| \$dn              | holds the "matchedDN" XML attribute of the DSML "compareResponse" element   |
| dsml.base         | holds the "dn" XML attribute of the DSML "searchRequest" element  |
| dsml.scope        | holds the value of the "scope" attribute of the DSML "searchRequest" element  |
| dsml.filter       | the LDAP filter that corresponds to the "filter" element of the DSML request  |
| dsml.attributes   | the value of this attribute is a Vector whose elements hold the names of the attributes listed in the "attributes" element of the DSML request. |
| dsml.derefAliases | holds the value of the "derefAliases" attribute of the DSML "searchRequest" element   |
| dsml.sizeLimit    | holds the value of the "sizeLimit" attribute of the DSML "searchRequest" element  |
| dsml.timeLimit    | holds the value of the "timeLimit" attribute of the DSML "searchRequest" element  |
| dsml.typesOnly    | holds the value of the "typesOnly" attribute of the DSML "searchRequest" element  |

## Search Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Search Responses:

Table 24.

| Attribute      | Value   |
|----------------|---|
| dsml.operation | set to "searchResponse"   |
| \$dn           | holds the "matchedDN" XML attribute of the DSML "searchResultDone" element of the DSML response |

Table 24. (continued)

| Attribute        | Value  |
|------------------|--|
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| resultEntries    | a multi-valued attribute, each of its values is a TDI Entry whose attributes correspond to the "attr" elements of the corresponding "searchResultEntry" element.   |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response   |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |

## Add Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Add Requests:

Table 25.

| Attribute      | Value   |
|----------------|---|
| dsml.operation | set to "addRequest"   |
| dsml.base      | holds the "dn" XML attribute of the DSML "addRequest" element |
| \$dn           | holds the "dn" XML attribute of the DSML "addRequest" element |

Additionally, for each DSML attr element: a TDI Attribute named as the "name" XML attribute of the DSML "attr" element and as values specified for the "attr" DSML element.

## Add Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Add Responses:

Table 26.

| Attribute        | Value  |
|------------------|--|
| dsml.operation   | set to "addResponse"   |
| "\$dn            | holds the "matchedDN" XML attribute of the DSML "addResponse" element  |
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response   |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral    | holds a vector containing all referral URIs of the DSML "addResponse" element  |

## Delete Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Delete Requests:

Table 27.

| Attribute      | Value   |
|----------------|---|
| dsml.operation | set to "deleteRequest"  |
| dsml.base      | holds the "dn" XML attribute of the DSML "delRequest" element |
| \$dn           | holds the "dn" XML attribute of the DSML "delRequest" element |

## Delete Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Delete Responses:

Table 28.

| Attribute        | Value  |
|------------------|--|
| dsml.operation   | set to "deleteResponse"  |
| \$dn             | holds the "matchedDN" XML attribute of the DSML "delRequest" element   |
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response   |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral    | holds a vector containing all referral URIs of the DSML "addResponse" element  |

## ModifyDN Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for ModifyDN Requests:

Table 29.

| Attribute         | Value   |
|-------------------|---|
| dsml.operation    | set to "modDnRequest"   |
| dsml.base         | holds the "dn" XML attribute of the DSML "modDNRequest" element           |
| \$dn              | holds the "dn" XML attribute of the DSML "modDNRequest" element           |
| newrdn            | holds the "newrdn" XML attribute of the DSML "modDNRequest" element       |
| dsml.newSuperior  | holds the "newSuperior" XML attribute of the DSML "modDNRequest" element  |
| dsml.deleteOldRDN | holds the "deleteoldrdn" XML attribute of the DSML "modDNRequest" element |

## ModifyDN Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for ModifyDN Responses:

Table 30.

| Attribute        | Value  |
|------------------|--|
| dsml.operation   | set to "modDnResponse"   |
| \$dn             | holds the "matchedDN" XML attribute of the DSML "modDNResponse" element  |
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response   |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral    | holds a vector containing all referral URIs of the DSML "addResponse" element  |

## Compare Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Compare Requests:

Table 31.

| Attribute          | Value   |
|--------------------|---|
| dsml.operation     | set to "compareRequest"   |
| dsml.base          | holds the "dn" XML attribute of the DSML "compareRequest" element             |
| \$dn               | holds the "dn" XML attribute of the DSML "compareRequest" element             |
| dsml.compare_name  | holds the "name" XML attribute of the "assertion" element of the DSML request |
| dsml.compare_value | holds the value of the "assertion" element of the DSML request                |

## Compare Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Compare Responses:

Table 32.

| Attribute           | Value   |
|---------------------|---|
| dsml.operation      | set to "compareResponse"  |
| \$dn                | holds the "matchedDN" XML attribute of the DSML "compareResponse" element   |
| dsml.compare_result | either "true" or "false" depending on whether the compare found match or not. When the Parser is used to create a DSML response, this attribute is required and depending on its value the Parser sets the right result code value. |
| dsml.resultcode     | holds the "code" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.resultdescr    | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.error          | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response  |

Table 32. (continued)

| Attribute      | Value  |
|----------------|--|
| dsml.exception | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral  | holds a vector containing all referral URIs of the DSML "addResponse" element  |

## Auth Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Auth Requests:

Table 33.

| Attribute      | Value   |
|----------------|---|
| dsml.operation | set to "authRequest"  |
| dsml.principal | holds the "principal" XML attribute of the DSML "authRequest" element |

## Auth Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Auth Responses:

Table 34.

| Attribute        | Value  |
|------------------|--|
| dsml.operation   | set to "authResponse"  |
| \$dn             | holds the "matchedDN" XML attribute of the DSML "authResponse" element   |
| dsml.resultcode  | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.error       | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response.  |
| dsml.exception   | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral    | holds a vector containing all referral URIs of the DSML "authResponse" element   |

## Extended Request

Entries with the following structure are parsed (on read) and created (on write) by the parser for Extended Requests:

Table 35.

| Attribute                  | Value  |
|----------------------------|--|
| dsml.operation             | set to "extendedRequest"   |
| dsml.extended.requestname  | holds the "requestName" XML attribute of the DSML "extendedRequest" element  |
| dsml.extended.requestvalue | holds the "requestValue" XML attribute of the DSML "extendedRequest" element |

## Extended Response

Entries with the following structure are parsed (on read) and created (on write) by the parser for Extended Response:

Table 36.

| Attribute         | Value  |
|-------------------|--|
| dsml.operation    | set to "extendedResponse"  |
| \$dn              | holds the "matchedDN" XML attribute of the DSML "extendedResponse" element   |
| dsml.resultcode   | holds the "code" XML attribute of the "resultCode" XML element of the DSML response  |
| dsml.resultdescr  | holds the "descr" XML attribute of the "resultCode" XML element of the DSML response   |
| dsml.error        | the presence of this attribute indicates an error condition and holds the value of the "errorMessage" XML element of the DSML response   |
| dsml.exception    | holds a javax.naming.NamingException object that is used to automatically fill in the "code" and "descr" XML attributes of the "resultCode" XML element of the DSML response; if this attribute is specified, any values set to the "dsml.resultcode" and "dsml.resultdescr" Entry Attributes are ignored and replaced with data retrieved through the exception object. |
| dsml.referral     | holds a vector containing all referral URIs of the DSML "extendedResponse" element   |
| dsml.responseName | holds the "responseName" XML attribute of the DSML "extendedResponse" element  |
| dsml.response     | holds byte array containing string which represents the response from an "extendedResponse" operation  |

## Binary and non-String Attributes

When parsing DSML messages, attributes tagged as binary by the **Binary Attributes** Parser parameter are Base64 decoded, that is, the string value from the DSML message is Base64 decoded to Java byte array.

When creating DSML messages, all Attributes whose value is Java byte array are Base64 encoded to String before being written in the DSML message.

If when creating a DSML message an Attribute is passed whose value's type is neither String nor Java byte array, the value is converted to String by calling the object's "toString()" method and this String value is written in the DSML message.

## Optional Attributes

The following optional attributes, when present, are parsed (on read) and created (on write) by the parser for all DSMLv2 Requests and Responses:

Table 37.

| Attribute      | Value  |
|----------------|--|
| dsml.requestID | corresponds to the DSMLv2 "requestID" attribute.   |
| dsml.controls  | holds an array of raw "com.ibm.dsml2.parser.Control" objects and corresponds to the "control" DSMLv2 elements. |

## Setting result code and result description

When setting the "dsml.resultcode" Attribute for DSML Response messages, allowed types are: java.lang.Integer and java.lang.String containing an integer value as string. This value corresponds to the integer "code" XML attribute of the "resultCode" DSML element and it is required by the DSMLv2 specification.

You can optionally set the "dsml.resultdescr" Attribute for DSML Response messages. This value corresponds to the "descr" XML attribute of the "resultCode" DSML element. It is not required by the DSMLv2 specification. When you assign a value to this attribute it is placed in the DSML response as is – no validation of the value (which is an enumerated string is done) and no check is performed whether this value corresponds to the mandatory integer "dsml.resultcode" Attribute.

The "code" and "descr" XML attributes of the "resultCode" DSML element can also be set through the "dsml.exception" Entry Attribute for DSML Response messages. This attribute can only accept javax.naming.NamingException objects. When "dsml.exception" attribute is set, the "code" and "descr" XML attributes of the "resultCode" DSML element are overwritten with new values extracted from the exception object. For example when the "dsml.exception" attribute is set to a javax.naming.AuthenticationException object, the "code" attribute will be set to the LDAP code of "49" and the "descr" attribute will be set to the LDAP description "inappropriateAuthentication".

## Multiple Attribute modifications

The DSMLv2 Parser (and LDIF Parser) does not support multiple modifications over a single Attribute – the values from a modification are accumulated in the Attribute and the operation from the last modification is set as the operation tag for the Attribute. Therefore, the Parsers need to merge the modifications in a TDI Entry in such way that the resulting Attribute modification be equivalent to the modifications for that Attribute in the modify operation. This can be achieved by using Attribute.ATTRIBUTE\_MOD – a TDI-specific tagging at the Attribute level and by using AttributeValue level tagging - AttributeValue.AV\_ADD, AttributeValue.AV\_DELETE.

The following data flow rules will be used when accumulating modifications in a TDI Attribute object:

- On modification "Add" – the value(s) will be added with AttributeValue.AV\_ADD to the Attribute; also the Attribute will be tagged as Attribute.ATTRIBUTE\_MOD unless it is already tagged as Attribute.ATTRIBUTE\_REPLACE
- If the Attribute is already tagged with Attribute.ATTRIBUTE\_REPLACE in a previous modification this tag will not be changed
- On modification "Delete" with value(s) – the value(s) will be added with AttributeValue.AV\_DELETE to the Attribute; also the Attribute will be tagged as Attribute.ATTRIBUTE\_MOD unless it is already tagged as Attribute.ATTRIBUTE\_REPLACE; if the Attribute is tagged as Attribute.ATTRIBUTE\_REPLACE for each value in the "Delete" modification the value will be removed from the Attribute if that value is present in the Attribute
- On modification "Delete" without values – the Attribute values from previous modifications will be cleared and the Attribute will be tagged as Attribute.ATTRIBUTE\_REPLACE
- On modification "Replace" – the Attribute values from previous modifications will be cleared and the new ones will be added; also the Attribute will be tagged as Attribute.ATTRIBUTE\_REPLACE.

## Configuration

The Parser needs the following parameters:

### Character Encoding

Specifies the XML character encoding; for example, UTF-8 or ASCII.

**Mode** Specifies whether the Parser operates in Server or in Client mode – possible values are "Server" and "Client". In "Server" mode requests are read and responses are written. In "Client" mode requests are written and responses are read.



## Binary Attributes

Specifies a comma delimited list of attributes that will be treated by the Parser as binary attributes.

The following attributes are specified as binary by default (but you can change this list):

- photo
- personalSignature
- audio
- jpegPhoto
- javaSerializedData
- thumbnailPhoto
- thumbnailLogo
- userPassword
- userCertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair
- x500UniqueIdentifier
- objectGUID
- objectSid

## On Error

A BatchRequest element can contain the XML-attribute `onError`, which determines how the server responds to failures while processing request elements. The valid values are: `exit` and `resume`. The default value is `exit`.

## Processing

Sets the value of the "processing" DSML attribute for Batch Requests.

## Response Order

Influences how the server orders individual responses within the BatchResponse. The values of this parameter are `sequential` and `unordered`. The default value is `sequential`. If the Response Order value is set to `sequential`, the server must return a BatchResponse in which the individual responses maintain a positional correspondence with the individual requests.

## Omit XML Declaration

Determines whether XML declaration omitting is enabled or disabled. By default, this parameter is disabled.

## Indent Output

If checked, the output will be indented according to the depth of the statement lines. This is cosmetic only; it has no bearing upon the semantic content of the output file.

## Soap Binding

When turned on, the parser processed and creates SOAP DSML message. Otherwise the DSML messages are not wrapped in SOAP.

## Detailed Log

If checked, more detailed log messages will be generated.

## Examples

### Parsing a DSMLv2 AddRequest in Server mode

If the DSMLv2 Parser is configured to run in "server" (read) mode and is passed the following DSMLv2 request:

```

<batchRequest onError="exit" processing="sequential"
  responseOrder="sequential" xmlns="urn:oasis:names:tc:DSML:2:0:core"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <addRequest requestID = "3" dn="cn=chavdar kovachev,o=ibm,c=us">
    <attr name="objectclass">
      <value>person</value>
    </attr>
    <attr name="telephoneNumber">
      <value>555</value>
    </attr>
    <attr name="sn">
      <value>kovachev</value>
    </attr>
    <attr name="cn">
      <value>chavdar kovachev</value>
    </attr>
  </addRequest>
</batchRequest>

```

it will generate an Entry object with the following Attributes:

- sn: 'kovachev'
- \$dn: 'cn=chavdar kovachev,o=ibm,c=us'
- telephoneNumber: '555'
- objectclass: 'person'
- dsml.operation: 'addRequest'
- dsml.requestID: '3'
- cn: 'chavdar kovachev'
- dsml.base: 'cn=chavdar kovachev,o=ibm,c=us'

## Creating a DSMLv2 SearchRequest in Client mode

If the DSMLv2 Parser is configured to run in "client" (write) mode and is passed an Entry with the following Attributes:

- dsml.derefAliases: 'neverDerefAliases'
- dsml.sizeLimit: '0'
- dsml.operation: 'searchRequest'
- dsml.timeLimit: '0'
- dsml.typesOnly: 'false'
- dsml.requestID: '7'
- dsml.attributes: '[cn, sn]'
- dsml.scope: 'wholeSubtree'
- dsml.base: 'o=ibm,c=us'
- dsml.filter: '(sn=\*)'

it will generate the following DSMLv2 request:

```

<?xml version="1.0" encoding="UTF-8"?>
<batchRequest onError="exit" processing="sequential"
  responseOrder="sequential" xmlns="urn:oasis:names:tc:DSML:2:0:core"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">

  <searchRequest requestID="7" derefAliases="neverDerefAliases"
    dn="o=ibm,c=us" scope="wholeSubtree" sizeLimit="0"
    timeLimit="0" typesOnly="false">
    <filter>
      <present name="sn"/>
    </filter>
  </searchRequest>
</batchRequest>

```

```
        <attribute name="cn"/>
        <attribute name="sn"/>
    </attributes>
</searchRequest>
</batchRequest>
```



---

## Fixed Parser

The Fixed Parser reads and writes fixed length text records.

### Configuration

The Parser has the following parameters:

#### Column Description

This multi-line parameter specifies each field name, the offset and length. For example:

```
field1, 1, 12  
field2, 13, 4  
field3, 17, 3
```

#### Trim values

Trim leading or trailing spaces for input fields.

#### Character Encoding

Character Encoding conversion.

#### Detailed Log

If this field is checked, additional log messages are generated.



---

## HTTP Parser

The HTTP Parser interprets a byte stream according to the HTTP specification. This Parser is used by the HTTP Client Connector and by the HTTP Server Connector.

### Configuration

The Parser has the following parameters:

#### Headers As Properties

If set, the header values are **get as Properties** and **set as Properties**. If not set, the header values are **read as attributes** and **returned as attributes**.

#### Client Mode

If set, the parser operates in client mode. If not set, the parser operates in server mode.

#### Character Encoding

Character Encoding conversion.

#### Detailed Log

If this parameter is checked, more detailed log messages are generated.

### Attributes or properties

When constructing a page, depending on the value of **Headers As Properties**, the Parser uses these attributes or properties, where relevant, to construct the header. When reading a page, the Parser parses the header to fill in these attributes or properties where possible.

#### http.method

The HTTP method when sending this information in client mode (default is **GET**). This attribute or property is returned in server mode. See <http://www.w3.org/Protocols/HTTP/Methods.html> for more information about HTTP methods.

#### http.url

The URL to use. This attribute or property is mandatory in client mode.

#### http.content-type

The content type for the returned **http.body** (if any). If this is set to **application/x-www-form-urlencoded**, the **http.body** is also parsed for more headers. The default value when writing (when **http.body** contains something), is **text/plain**.

#### http.responseCode

The HTTP response code as an Integer object. Read in client mode.

#### http.responseMsg

The HTTP response message as a String object. Read in client mode.

#### http.content-encoding

The encoding of the returned **http.body** (if any)

#### http.content-length

The number of bytes in **http.body**. This attribute or property is returned when reading, and ignored when writing. It is recomputed by the Parser.

#### http.body

When reading, depending of the content-type of the data, this object is an instance of `java.lang.StringBuffer`, a `char[]` or a `byte[]` that contains the returned body. When the content is a `StringBuffer`, you can use code such as the following:

```
var body = conn.getObject ("http.body");
task.logmsg ("Returned text: " + body.toString() );
```

See "Using binary values in scripting" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for information about handling a `char[]` or `byte[]`. When writing, **http.body** must contain either an instance of `java.io.File`, in which case that file is used as the body, or some text that is used as the body.

#### **http.text-body**

When reading, if the **http.content-type** starts with the sequence **text/**, the Connector assumes the body is textual data and reads the **http.body** stream object into this attribute.

#### **http.redirect**

When this attribute or property has a value, and the user is writing and in server mode, redirect message pointing to the value of this attribute or property is sent.

#### **http.status**

Used when writing in server mode. The default is **OK**. Some possible values are:

- **OK** or **200 OK**- Returns a **200 OK** response.
- **FORBIDDEN** or **401 Forbidden**- Attempts to authenticate using the **http.auth-realm** attribute or property.
- **NOT FOUND** or **404 File Not Found** - Returns a **404 File Not Found** response.

#### **http.auth-realm**

Used when requesting additional authentication. The default value is **IBM-Directory-Integrator**.

#### **http.authorization**

Contains the authorization read in server mode. It is probably easier to use **http.remote\_user** and **http.remote\_pass**.

#### **http.remote\_user**

The username returned when reading in server mode, or the username to use when writing in client mode.

#### **http.remote\_pass**

The password returned when reading in server mode, or the password to use when writing in client mode.

#### **http.base**

The base URL. Returned when reading in server mode.

#### **http.qs.\***

Parts of the query string when reading in server mode. The key is the part of the name after **http.qs**.

The value is contained in the attribute or property.

**http.\*** All other attributes or properties beginning with **http**. are used to generate a header line when writing. When reading, headers are put into attributes or properties with a name beginning with **http.**, and continuing with the name of the header.

## **Character sets/Encoding**

### **Character set when reading**

The default character encoding when reading is **iso-8859-1**. This encoding is overridden by the **Character Encoding** parameter in the config pane for this Connector; and this `characterSet` parameter is overridden in turn by a header of the type "Content-type: text/plain; charset=iso-8859-1". For optimum performance and compatibility, this header should be present.

### **Character set when sending**

The default character encoding when reading is **iso-8859-1**. This encoding is overridden by the **Character Encoding** parameter in the config pane for this Connector. When sending a text message, the Entry to



send should contain an attribute with the name "http.content-type", having a text value of the form "Content-type: text/plain; charset=iso-8859-1". The defaults will be used only if this attribute is not present .

If the http.body attribute is a java.io.File object, that file will be sent as is, no character conversion will be performed

## **See also**

"HTTP Client Connector" on page 83,  
"HTTP Server Connector" on page 91.



---

## LDIF Parser

The LDIF Parser reads and writes LDIF style data. The LDIF Parser is usually used to do file exchange with an LDAP directory.

The LDIF Parser correctly parses and writes MIME BASE64 encoded strings: it tries to perform BASE64 encoding if necessary. One such situation is where there are trailing spaces after attribute values: To make sure another LDIF Parser gets the space, it encodes the attribute as BASE64.

**Note:** A conforming LDIF file must always have **Character Encoding** set to UTF-8. The **Character Encoding** parameter is also applied when encoding or decoding BASE64 encoded strings.

BASE64 encoding looks like garbled text if you do not know how to decode it.

This Parser handles/provides tags compatible with Delta Tagging at the Entry level, the Attribute level and the Attribute Value level. Delta tagging at the Attribute level is handled as in the DSMLv2 Parser, see “Multiple Attribute modifications” on page 290.

## Configuration

The Parser has the following parameters:

### DN Attribute Name

The attribute name to use.

### Version Number

Displays a version attribute in the beginning of the output if checked. This parameter is **On** by default.

**Note:** LDIF parser can now suppress the LDIF version number by using the **Version Number** parameter.

### Binary Attributes

If you need to specify additional attributes to be treated as binary (a binary attribute is returned as a byte array, not a string), specify them in this parameter. By default, the following attributes are treated as binary:

- photo
- personalSignature
- audio
- jpegPhoto
- javaSerializedData
- thumbnailPhoto
- thumbnailLogo
- userPassword
- userCertificate
- authorityRevocationList
- certificateRevocationList
- crossCertificatePair
- x500UniqueIdentifier
- objectGUID
- objectSid

### Character Encoding

Character Encoding conversion.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**See also**

<http://www.ietf.org/rfc/rfc2849.txt>

---

## Line Reader Parser

The Line Reader Parser reads single lines of data. The line read is returned in a single attribute. There is also an attribute named **linenumber** that contains the line number, starting with **1**.

**Note:** Use the Line Reader Parser if you want to copy a text file only. If you want to copy a binary file, see the FTP Object “Example” on page 437 for an example of how not to copy a binary file.

The Line Reader Parser is useful when reading text files only.

## Configuration

The Parser has the following parameters:

### Attribute Name

Specifies the name of the attribute that contains the line. Default is **line**.

### Character Encoding

Character Encoding conversion.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.



---

## Script Parser

The Script Parser enables you to write your own Parser using JavaScript.

To operate, a Script Parser must implement a few functions. The functions do not use parameters. Passing data between the hosting Connector and the script is done by using predefined objects. One of these predefined objects is the **result** object which is used to communicate status information. Upon entry into either function, the status field is set to **normal** which causes the hosting Parser to continue calls. Signaling end-of-input or errors is done by setting the status and message fields in this object. The **entry** object is populated on calls to **writeEntry** and is expected to be populated in the **readEntry** function. When reading entries you have the **inp** BufferedReader object available for reading character data from a stream. When writing entries you have the **out** BufferedWriter object available for writing character data to a stream.

You can add your own parameters to the configuration and obtain these by using the **Parser** object.

## Objects

The following objects are the only ones accessible to the script Parser:

### The result object

#### setStatus

code

- 0 - End of Input
- 1 - Status OK
- 2 - Error

#### setMessage

text

### The entry object

#### addAttributeValue (name, value)

Adds a value to an attribute.

#### getAttribute (name)

Returns the named attribute.

A complete list of available methods, including parameters and return values, can be found in the Javadocs (*root\_directory/docs/api/com/ibm/di*).

### The inp object

**read()** Returns next character from stream.

#### readLine()

Returns next CRLF-stopped line from the input stream.

### The out object

#### write (str)

Writes a string to the output stream.

#### writeln (str)

Writes a string followed by CRLF to the output stream.

### The Parser object

#### getParam(str)

Returns the parameter value associated with parameter name **str**

**setParam(str, value)**

Sets the parameter **str** to value **value**

**logmsg(str)**

Writes the parameter **str** in the log file

A complete list of methods can be found in the installation package.

**The Connector object**

For more information, see the Javadocs material included in the installation package.

**Functions (methods)**

The Parser should supply the following functions, where relevant for the intended usage in IBM Tivoli Directory Integrator:

**readEntry()**

Read the next logical entry from the input stream and populate the **entry** object. This function is not required for Parsers called in `add_only` situations only.

**writeEntry()**

Write the contents of the **entry** object to the output stream. This function is not required for Parsers that are only used for reading.

**closeParser ( )**

The `closeParser` function, if implemented, will be called when `Connector.close` is called. For example:

```
function closeParser ( )
{
  task.logmsg("CLOSE CALLED.");
}
```

**flush()**

The `flush` function will be called if the Parser's `flush` is called via the `connector.getParser( ).flush( )` method. Implementing these methods in effect overrides the Parser's methods. For example:

```
function flush ( )
{
  task.logmsg("FLUSH CALLED.");
}
```

**Configuration**

The Parser has the following parameters:

**Script Language**

Choose an available script language from the list.

**External Files**

If you want to include external script files at runtime, specify them here, one file on each line. These files are run before your script.

**Include Global Scripts**

Include scripts from the Script Library.

**Character Encoding**

Character Encoding conversion.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

**Script** The user-defined script to run.



**Note:** When you use a Script Connector or Parser, the script is copied from the Library where it resides and into your configuration file. This has the advantage that you can customize the script, but with the disadvantage that new versions are not known to your AssemblyLine.

To work around this disadvantage, remove the old Script Parser from the AssemblyLine and re-introduce it. Remember to copy over code from your hooks.

## Example

Go to the *root\_directory/examples/script\_parser* directory of your IBM Tivoli Directory Integrator installation.

## See also

"Script Connector" on page 201,

"Scripted FC" on page 345

"JavaScript Parser" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.



---

## Simple Parser

The Simple Parser reads and writes entries. The format is lines with *attributename:value* pairs, where *attributename* is the name of the attribute, and *value* is the value.

Multi-valued attributes use multiple lines. Lines with a single period mark the end of an entry. `\r` and `\n` in the *value* is an encoding of CR and LF.

## Configuration

The Parser has the following parameters:

### Character Encoding

Character Encoding conversion.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.



---

## SOAP Parser

The SOAP Parser reads and writes SOAP XML documents. The Parser converts SOAP XML documents to or from entry objects in a simple, straightforward fashion. When writing the XML document, the Parser uses attributes from the entry to build the document. The **SOAP\_CALL** attribute is expected to contain the value for the SOAP call. Similarly, when reading, this attribute is set to reflect the first tag following the **SOAP-ENV:Body** tag. Then, for each attribute in the entry, a tag with that name and value is created. When reading the document, each tag under the **SOAP\_CALL** tag translates to an attribute in the entry object.

**Note:** When working with the WebServices EventHandler and Connector, you must avoid starting attribute names with special characters (such as [0-9] [ - ' ( ) + , . / = ? ; ! \* # @ \$ % ] ). Also, you must avoid having attribute names that include special characters (such as [ ' ( ) + , / = ? ; ! \* # @ \$ % ] ). This is because WebServices builds on SOAP, which is XML. XML does not accept \$ as in tags.

The following examples show an entry and a SOAP XML document as they are read or written.

### Example Entry

```
*** Begin Entry Dump
SOAP_CALL: 'updateLDAP'
mail: ('john@doe.com')
uid: 'johnd'
*** End Entry Dump
```

### Example SOAP document

```
<SOAP-ENV:Envelope
  xmlns:SOAP-ENV="(http://schemas.xmlsoap.org/soap/envelope/)"
  xmlns:xsi="(http://www.w3.org/1999/XMLSchema-instance)"
  xmlns:xsd="http://www.w3.org/1999/XMLSchema">
<SOAP-ENV:Body>
<ns1:updateLDAP xmlns:ns1="" SOAP-ENV:encodingStyle=
  "http://schemas.xmlsoap.org/soap/encoding/">
<uid xsi:type="xsd:string">johnd</uid>
<mail xsi:type="xsd:string">john@doe.com</mail>
</ns1:updateLDAP>
</SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

## Configuration

The Parser has the following parameters:

### Omit XML Declaration

Omit the XML declaration header in the output stream.

### Document Validation

Request a DTD/XSchema-validating XML parser.

### Namespace Aware

Request a namespace-aware XML parser.

### Character Encoding

Character Encoding conversion.

### Detailed Log

If this parameter is checked, more detailed log messages are generated.

## Parser-specific calls

You can access the SOAP Parser from your script by dynamically loading the Parser and calling the methods to read or write SOAP documents. The following example shows how to generate the XML document from an entry:

```
var e = system.newEntry();
e.setAttribute ("soap_call", "updateLDAP");
e.setAttribute ("uid", "johnd");
e.setAttribute ("mail", "(john@doe.com)");

// Retrieve the XML document as a string
var soap = system.getParser ("ibmdi.SOAP");
soap.initParser();
var soapxml = soap.getXML ( e );

task.logmsg ( "SOAP XML Document" );
task.logmsg ( soapxml );

// Write to a file
var soap = system.getParser("ibmdi.SOAP");
soap.setOutputStream ( new java.io.FileOutputStream("mysoap.xml") );
soap.writeEntry ( e );
soap.close();

// Read from file
soap.setInputStream ( new java.io.FileInputStream ("mysoap.xml") );
var entry = soap.readEntry();

// Read from string (from soapxml generated above)
var entry = soap.parseRequest( soapxml );
task.dumpEntry ( entry );
```

## Examples

Go to the *root\_directory/examples/soap* directory of your IBM Tivoli Directory Integrator installation.

---

## XML Parser

The XML Parser reads and writes XML documents. This Parser uses the Apache Xerces and Xalan libraries. The Parser gives access to XML document through a script object called **xmldom**. The **xmldom** object is an instance of the `org.w3c.dom.Document` interface. Refer to <http://java.sun.com/xml/jaxp-1.0.1/docs/api/index.html> for a complete description of this interface.

You can also use the XPathAPI (<http://xml.apache.org/xalan-j/apidocs/index.html> and Access Java Classes in your Scripts) to search and select nodes from the XML document. **selectNodeList**, a convenience method in the **system** object, can be used to select a subset from the XML document.

When the Connector is initialized, the XML Parser tries to perform Document Type Definition (DTD) verification if a **DTD** tag is present.

Use the Connector's override functions to interpret or generate the XML document yourself. Create the necessary script in either the **Override GetNext** or **GetNext Successful** in your AssemblyLine's hook definitions. If you do not override, the Parser reads or writes a very simple XML document that mimics the entry object model. The default Parser only permits you to read or write XML files two levels deep. It will also read multi-valued attributes, although only one of the multi-value attributes will be shown when browsing the data in the Schema tab.

Note that certain methods, such as `setAttribute` are available in both the IBM Tivoli Directory Integrator **entry** and the objects returned by **xmldom.createElement**. These functions have the same name or signature. Do not confuse the **xmldom** objects with the IBM Tivoli Directory Integrator objects.

### Notes:

1. If you read large (greater than 4MB) or write large (greater than 14MB) XML files, your Java VM may run out of memory. Refer to "Increasing the memory available to the Virtual Machine" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for a solution to this. Alternatively, use the "XML SAX Parser" on page 317.
2. The Parser silently ignores empty entries.
3. When reading a CDATA attribute, no blank space is trimmed from the value. However, blank space is trimmed from attributes that are not CDATA.
4. Certain characters, such as \$, are illegal in XML tags. Avoid these characters in your attribute names when using the XML Parser because these characters might create illegal XML.
5. When reading from an LDAP directory or an LDIF file, the distinguished name (DN) is typically returned in an attribute named \$dn. If you map this attribute without changing the name into an XML file, it fails because \$dn is not a legal tag in an XML document. If you do explicit mapping, you must change "\$dn" to "dn" (or something without a special character) in your output Connector. If you do implicit mapping, for example, \* or **Automatically map all attributes** checked in the **AssemblyLine Settings** (through the **Config . . .** tab of the AssemblyLine), you can configure the XML Parser to translate the distinguished name (for example, \$dn) to a different name. For example, you can add something like this in the **Before GetNext** Hook:

```
conn.setAttribute("dn", work.getAttribute("$dn"));
conn.removeAttribute("$dn");
```
6. The implementation of XML used in IBM Tivoli Directory Integrator uses the DOM model, which means it is memory based. The whole tree must be contained in memory for it to be valid. This is not a problem in regards to Connectors utilizing the XML Parser in Iterator mode, except possibly for the fact that you could run out of memory if the input file is large. During normal operation as well as restart the Parser reads the whole tree into memory but still skips to the correct entry if so instructed by the Checkpoint/Restart framework at restart.

## Configuration

The Parser has the following parameters:

**Root Tag**

The root tag (output).

**Entry Tag**

The entry tag for entries (output).

**Value Tag**

The value tag for entry attributes (output).

**Character Encoding**

Character Encoding conversion.

**Omit XML Declaration**

If checked, the XML declaration is omitted in the output stream.

**Document Validation**

If checked, this parser requests a DTD/Schema-validating parser.

**Namespace Aware**

If checked, this parser requests a namespace-aware parser.

**Indent Output**

If this field is checked, then the output is indented.

**Note:** If this text is to be processed by a program (and not meant for human interpretation) you most likely will want to deselect this parameter. This way, no unnecessary spaces or newlines will be inserted in the output.

**Detailed Log**

If this parameter is checked, more detailed log messages are generated.

## Character Encoding in the XML Parser

The default and recommended Character Encoding to use when deploying the XML Parser is UTF-8. This will preserve data integrity of your XML data in most cases. When you are forced to use a different encoding, the Parser will handle the various encodings in the following way:

- When reading a file, the encoding specified in the XML header of the file is used. If no encoding is specified there, then the encoding specified in the parser config is used. If still no encoding is specified, then UTF-8 is used.
- On output, the Parser will write an XML header specifying the character encoding. This will be the encoding specified in the Parser config. If nothing is specified there, UTF-8 will be used.

## Examples

**Override Add hook:**

```
var root = xmldom.getDocumentElement();
var entry = xmldom.createElement ("entry");
var names = work.getAttributeNames();

for ( i = 0; i < names.length; i++ ) {
  xmlNode = xmldom.createElement ("attribute");
  xmlNode.setAttribute ( "name", names[i] );
  xmlNode.appendChild ( xmldom.createTextNode ( work.getString(
    names[i] ) ) );
  entry.appendChild ( xmlNode );
}
root.appendChild ( entry );
```

**After Selection hook:**

```
//
// Set up variables for "override getNext" hook
//
```



```

var root = xmldom.getDocumentElement();
var list = system.selectNodeList ( root, "//Entry" );
var counter = 0;

```

### Override GetNext hook

```

//
// Note that the Iterator hooks are NOT called when we override the
// getNext function
// Initialization done in After Select Entries hook

var nxt = list.item ( counter );

if ( nxt != null ) {
    var ch = nxt.getFirstChild();
    while ( ch != null ) {
        var child = ch.getFirstChild();
        while (child != null ) {
            // Use the grandchild's value if it exist, to be able to
            // read multivalued attributes
            grandchild = child.getFirstChild();
            if (grandchild != null)
                nodeValue = grandchild.getNodeValue();
            else nodeValue = child.getNodeValue();
            // Ignore strings containing newlines, they are just fillers
            if (nodeValue != null && nodeValue.indexOf('\n')
                == -1) {
                work.addAttributeValue ( ch.getNodeName(), nodeValue );
            }
            child = child.getNextSibling();
        }
        ch = ch.getNextSibling();
    }

    result.setStatus (1); // Not end of input yet
    counter++;
} else {
    result.setStatus (0); // Signal end of input
}

```

The previous example parses files containing entries that look like the following:

```

<DocRoot>
  <Entry>
    <firstName>John</firstName>
    <lastName>Doe</lastName>
    <title>Engineer</title>
  </Entry>
  <Entry>
    <firstName>Al</firstName>
    <lastName">Bundy</lastName>
    <title">Shoe salesman</title>
  </Entry>
</DocRoot>

```

Suppose instead that the input looks like the following:

```

<DocRoot>
  <Entry>
    <field name="firstName">John</field>
    <field name="lastName">Doe</field>
    <field name="title">Engineer</field>
  </Entry>
  <Entry>
    <field name="firstName">Al</field>

```

```

    <field name="lastName">Bundy</field>
    <field name="title">Shoe salesman</field>
  </Entry>
</DocRoot>

```

Here the attribute names can be retrieved from attributes of the field node, and this code is used in the **Override GetNext** Hook:

```

var nxt = list.item ( counter );

if ( nxt != null ) {
  var ch = nxt.getFirstChild();
  while ( ch != null ) {
    if(String(ch.getNodeName()) == "field") {
      attrName = ch.getAttributes().item(0).getNodeValue();
      nodeValue = ch.getFirstChild().getNodeValue();
      work.addAttributeValue ( attrName, nodeValue );
    }
    ch = ch.getNextSibling();
  }

  result.setStatus (1); // Not end of input yet
  counter++;
} else {
  result.setStatus (0); // Signal end of input
}

```

This example package demonstrates how the base XML Parser functionality can be extended to read XML more than two levels deep, by using the **Override GetNext** and **Override Add** hooks.

## Additional Examples

Go to the *root\_directory/examples/xmlparser* directory of your IBM Tivoli Directory Integrator.

## See also

“XML SAX Parser” on page 317,  
 “XSL based XML parser” on page 319,  
 “SOAP Parser” on page 311,  
 “DSML Parser” on page 281.

---

## XML SAX Parser

The XML SAX Parser is based on the Apache Xerces library. It is used for reading large sized XML documents that the DOM based XML parser won't be able to handle because of memory constraints. It extracts data enclosed within the 'Group tag' supplied in the configuration and creates an Entry with the attributes present in the data. You can specify multiple group tags by separating each tag name with a comma. This will cause the SAX parser to break on any the tags specified. When specifying multiple group tags the SAX parser will use a first-in-win approach where the group tag that was first encountered will be tag that closes the group. As an example, if you have A and B as group tags and the document has a structure where B is a child of A, then A will be the tag closing the entry (as A is found before B and thus takes precedence).

Once a group tag has been found, then any nested occurrence of group tags will have no effect on the current Entry.

If no group tags have been defined, the entire XML document will be returned as a single Entry.

The entry attribute name is composed of surrounding tag names with "@" as the separator. For example, consider the following XML file -

```
<?xml version="1.0" encoding="UTF-8"?>
<DocRoot>
  <Entry>
    <Company>
      <Name incorporated="yes">IBM Corporation</Name>
      <Country>USA</Country>
    </Company>
  </Entry>
  <Entry>
    <Company>
      <Name incorporated="no">Smith Brothers</Name>
      <Country>USA</Country>
    </Company>
  </Entry>
</DocRoot>
```

Using "Entry" as the GroupTag, the above XML document would yield two entries as follows -

### Entry 1

```
Attribute name: DocRoot@Entry@Company@Name
Attribute value: IBM Corporation
Attribute name: DocRoot@Entry@Company@Name#incorporated
Attribute value: yes
Attribute name:DocRoot@Entry@Company@Country
Attribute value: USA
```

### Entry 2

```
Attribute name: DocRoot@Entry@Company@Name#incorporated
Attribute value: Smith Brothers
Attribute name: DocRoot@Entry@Company@Name#incorporated
Attribute value: no
Attribute name:DocRoot@Entry@Company@Country
Attribute value: USA
```

The attribute name may be shortened by specifying a 'Remove Prefix' value in the configuration. For example, a 'Remove Prefix' value of "DocRoot@Entry@Company" in the above example will result in the Entry containing attributes like -

```
Attribute name: Name
Attribute value: IBM Corporation
Attribute name: Name#incorporated
```

Attribute value: yes  
Attribute name: Country  
Attribute value: USA  
...

When the Connector is initialized, the XML Parser tries to perform Document Type Definition (DTD) verification if a DTD tag is present. The parser will read multi-valued attributes, although only one of the multi-value attributes will be shown when browsing the data in the Schema tab.

If the XML file has nested entry tags, all Entry tags enclosed within the outermost Entry tag, will be treated as normal XML tags. For example,

```
<entry>
  <entry>
    <company>IBM</company>
  </entry>
</entry>
```

Here the entry will contain the following attribute:

attribute name: entry@entry@company  
attribute value: IBM

## Configuration

### Group Tag

XML Group tag name(s) that encloses entries. Specify multiple tags by separating each tag name with a comma; or use the root tag if this parameter is not specified (and the entire XML document will be returned as a single Entry).

### Remove prefix

Specify the prefix to remove from the attribute names.

### Ignore attributes

Asks the parser to ignore attributes of the group tag and its children.

### Character Encoding

The character set to observe when reading; the default is UTF-8.

### Document Validation

Checking this field, requests the validation of the file on basis of the DTD/XSchema used.

### Namespace Aware

Checking this field, requests a namespace aware XML parser.

### Read Timeout

The time in seconds, after which the parser stops if no data is received.

### Detailed Log

If this field is checked, additional log messages are generated.

## See also

“XML Parser” on page 313,

“XSL based XML parser” on page 319.

---

## XSL based XML parser

### Introduction

The XSL based XML DOM Parser enables TDI to parse XML documents in any format using the XSL supplied by the user, into attribute value pairs, stored in the entry object. The XSL based parser is required to facilitate reading of any kind of XML format. Particularly, when the user needs only a specific chunk of the XML he can write an XSL for picking the required chunk. The parser will create an in-memory parse tree to represent the input XML and the TDI internal format. The XSL transforms the DOM Document generated from input XML, and produces an output DOM for the TDI internal format. It uses the javax transformation libraries to carry out transformations.

### Configuration

The XSL based DOM XML Parser provides the following parameters:

#### Use input XSL file

Check box to indicate whether to use input XSL file or use the XSL keyed in (in the *Input XSL* field)

#### Input XSL File Name

The input XSL file that contains template matching rules for transforming user XML to TDI internal format

#### Input XSL

Editable area to allow the user to key in or paste the entire input XSL.

#### Use output XSL file

Check box to indicate whether to use output XSL file or use the XSL keyed in (in the *Output XSL* field).

#### Output XSL File Name

The output XSL file that has template matching rules for transforming TDI internal format back to user XML

#### Output XSL

Editable area to allow the user to key in or paste the entire output XSL.

#### Character Encoding

The character encoding to use when reading or writing; the default is UTF-8.

#### Omit XML Declaration

If checked, omit XML declaration header in output stream.

#### Document validation

if checked, request a DTD/XSchema validating XML parser.

#### Namespace aware

If checked, request a namespace aware XML parser.

#### Indent Output

If checked, causes the output to be neatly indented, improving human readability. If your output is going to be processed by another program, this option is best left off.

#### Detailed log

Specifies whether detailed debug information is written to the log.

### Using the Parser

The parser can be used with the Filesystem Connector in *Iterator* or *AddOnly* mode. The XSL based DOM XML parser requires the user to specify:

- The input XSL file (when used in a Filesystem Connector in *Iterator* mode): to transform XML to TDI internal format.

- The output XSL file (when used in a Filesystem connector in AddOnly mode): to transform TDI internal format back to the original format.

In an XSL transformation, an XSLT processor reads both an XML document and an XSLT style sheet. Based on the instructions the processor finds in the XSLT style sheet, it outputs a new XML document or fragment thereof. The parser will do the basic validation of the XSL files for authenticity. The parser also has optional Document and namespace validation of the file supplied by the Connector. The parser can be used in conjunction with the filesystem connector. The parser will support reading as well as writing, in the sense that XML files can be read and written to in a format specified by the respective XSL. The following optional validations are provided:

- Document validation
- Namespace aware

## TDI Internal Format

```
<DocRoot>
<Entry>
  <attribute_name>
    <value_tag>attribute_value</value_tag>
    <value_tag>attribute_value</value_tag>
    <value_tag>attribute_value</value_tag>
  </ attribute_name>
  <attribute_name>
    <value_tag>attribute_value</value_tag>
  </ attribute_name>
  -
  -
  -
</Entry>
<Entry>
  -
  -
  -
</Entry>
-
</DocRoot>
```

## Example

### Input XML: birds.XML

```
<?XML version="1.0" encoding="UTF-8"?>
<Class>
  <Order Name="TINAMIFORMES">
    <Family Name="TINAMIDAE">
      <Species Scientific_Name="Tinamus major"> Great Tinamou.</Species>
      <Species Scientific_Name="Nothocercus">Highland Tinamou.</Species>
      <Species Scientific_Name="Crypturellus soui">Little Tinamou.</Species>
      <Species Scientific_Name="Crypturellus cinnamomeus">Thicket Tinamou.</Species>
      <Species Scientific_Name="Crypturellus boucardi">Slaty-breasted Tinamou.</Species>
      <Species Scientific_Name="Crypturellus kerriae">Choco Tinamou.</Species>
    </Family>
  </Order>
  <Order Name="GAVIIFORMES">
    <Family Name="GAVIIDAE">
      <Species Scientific_Name="Gavia stellata">Red-throated Loon.</Species>
      <Species Scientific_Name="Gavia arctica">Arctic Loon.</Species>
      <Species Scientific_Name="Gavia pacifica">Pacific Loon.</Species>
      <Species Scientific_Name="Gavia immer">Common Loon.</Species>
      <Species Scientific_Name="Gavia adamsii">Yellow-billed Loon.</Species>
    </Family>
  </Order>
</Class>
```

### Input XSL: birds.XSL

```
<?XML version="1.0" ?>
<XSL:stylesheet xmlns:XSL="http://www.w3.org/1999/XSL/Transform" version="1.0">
  <XSL:output method="XML" indent="yes" />
<XSL:template match="Class">
  <DocRoot>
    <XSL:for-each select="Order">
      <XSL:variable name="order"><XSL:value-of select="@Name" />
      </XSL:variable>
      <XSL:for-each select="Family">
        <Entry>
          <Attribute name="Order">
            <Value><XSL:value-of select="$order" /></Value>
          </Attribute>
          <Attribute name="Family">
            <Value><XSL:value-of select="@Name" /></Value>
          </Attribute>
          <Attribute name="Species">
            <XSL:for-each select="Species">
              <Value><XSL:value-of select="." /></Value>
            </XSL:for-each>
          </Attribute>
        </Entry>
      </XSL:for-each>
    </XSL:for-each>
  </DocRoot>
</XSL:template>
</XSL:stylesheet>
```

birds.xml transforms birds.xml to TDI internal format from entry object with attribute value pairs, can be formed.

### See also

“XML Parser” on page 313

The XML Bible (the chapter on XSL)

<http://www.ibiblio.org/xml/books/bible2/chapters/ch17.html>

W3C Document Object Model

<http://www.w3.org/DOM/>

Effective XML processing with DOM and XPath in Java

<http://www-106.ibm.com/developerworks/XML/library/x-domjava/>

XSL Transformation using Xalan and Java

<http://www.perfectxml.com/vip1.asp>





---

## User-defined parsers

In addition to the parsers already provided with the installation of IBM Tivoli Directory Integrator, you can write your own parsers and add them to the system.

One example of a user-defined parser, capable of parsing Regular Expressions, is provided in the Examples directory. Go to the *root\_directory/examples/regexp\_parser* directory of your IBM Tivoli Directory Integrator installation. This particular example was written in Java.

Another example of a user-defined parser can be found in *root\_directory/examples/script\_parser*, which shows how to write a parser using scripting. See "JavaScript Parser" in the *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for a further explanation of this example.



---

## Chapter 5. Function Components

Function Components (FC) are, besides of Connectors, EventHandlers and Parsers, another type of building block that make up the IBM Tivoli Directory Integrator. Function Components are similar in scope to a Connector, with the difference that the latter are datasource specific whereas a Function Component is not. Rather, it is an AssemblyLine Component that facilitates wrapping of custom logic and external methods, and may present a user friendly "connector-like" user interface in the Configuration Editor (CE).

Also, a Function Component is modeless; that is, in order to configure a Function Component in your AssemblyLine you don't have to specify in which mode it is supposed to operate. It will do its work in the `perform()` method whenever it is called by the AssemblyLine.

Many of the components described below provide the means to build a complete (both client-side and server-side) web service solution in the modular TDI web service architecture.

The Function Components provided with the IBM Tivoli Directory Integrator 6.1.1 are:

- "AssemblyLine FC" on page 339
- "Axis EasyInvoke Soap WS FC" on page 367
- "Axis Java To Soap FC" on page 355
- "Axis Soap To Java FC" on page 365
- "Castor Java to XML FC" on page 327
- "Castor XML to Java FC" on page 329
- "CBE Generator Function Component" on page 347
- "Complex Types Generator FC" on page 371
- "Function Component For SAP R/3" on page 385
- "InvokeSoap WS FC" on page 361
- "Java Class Function Component" on page 341
- "Memory Queue FC" on page 353
- "Parser FC" on page 343
- "Remote Command Line FC" on page 373
- "Scripted FC" on page 345
- "SendEMail Function Component" on page 351
- "WrapSoap FC" on page 359
- "XMLToSDO FC" on page 331
- "SDOToXML FC" on page 335
- "z/OS TSO/E Command Line FC" on page 377



---

## Castor Java to XML FC

Processing complex and custom data types is often a requirement for various XML solutions, for example Web Services.

The existence of a self-contained Java-to-XML and XML-to-Java binding functionality in the IBM Tivoli Directory Integrator provides the ability to process complex/custom data types independently of a Web Service toolkit. In particular this means that there is an option to deal with possible binding limitations of various Web Service toolkits.

## Castor Overview

Castor is an open source data binding framework providing access to the data defined in an XML document through an object data model.

Castor can marshal almost any "bean-like" Java object to and from XML. The process of marshalling/unmarshalling can use Castor's default introspection model (an implementation based on Java reflection where Castor decides how to marshal and unmarshal data), but this process can also be controlled and customized by the use of Castor XML Mapping Files that define mapping rules.

From an IBM Tivoli Directory Integrator perspective, you can create XML Mapping Files and specify how custom data is mapped to and from XML.

With Castor you can process an XML document not specially designed for Castor by skipping parts of the XML you are not interested in. A limitation here is that Castor cannot skip an XML node and process a node belonging to the subtree of the skipped node. This limitation is a serious inconvenience when you want to extract random parts of a big and complex XML document (cases which might be expected in the real world) – that is why the IBM Tivoli Directory Integrator Castor Function Components provide the ability to specify certain parts of the XML through XPath queries.

The CastorJavaToXML Function Component uses Castor 0.9.5.4. Documentation and information for the Castor library can be obtained from the Castor project web site: <http://www.castor.org/>

## Configuration

### Parameters

#### Castor Mapping File

An XML Mapping File (as defined by the Castor syntax) that defines how Java or *Entry* objects are serialized into XML.

The mapping file as specified by this parameter should always include the mapping rules defined in the "*TDI\_installation\_directory*/jars/functions/di\_castor\_mapping.xml" file. This means that either you must specify "*jars/functions/di\_castor\_mapping.xml*" as value of this parameter or make sure that the mapping file specified contains these rules (for example by using Castor's "include" clause to include "*di\_castor\_mapping.xml*" rules in another mapping file).

#### XML Root Element

The name of the root element of the generated XML; if left empty the root element is named "Entry".

#### Use Attribute Names

If this is checked, the names of the Attributes are used as XML element names, otherwise the XML elements are named as specified in the Mapping File. This parameter is only taken into account in Entry mode.

#### Return XML as

This drop-down list specifies the return type - only taken into account when the input object is not an object of type *Entry*. Valid values are **String** and **DOMElement**.

### Detailed Log

Check to generate additional log messages.

### Comment

Your own comments go here.

## Using the FC

The CastorJavaToXML Function Component creates an XML document from a Java object or an *Entry* object.

This Function Component can operate both with *Entry* objects and with custom Java objects.

When the Function Component is passed an *Entry* object on input, it will return an *Entry* object. This mode of operation is called **Entry** mode.

When passed a Java object which is not an *Entry* object, the Function Component will serialize the object passed using Castor serialization and this will be the result XML. This mode of operation is called **non-Entry** mode.

### Entry mode

- In **Entry** mode each Attribute of the *Entry* passed on input is marshalled and placed under the root of the resulting XML element.
- If the **Return XML as** parameter is set to **DOMelement** the resulting *Entry* contains one attribute named "*xmlDOMElement*" and its value is the marshaled XML element as a "*org.w3c.dom.Element*" object.
- If the **Return XML as** parameter is set to **String** the resulting *Entry* contains one attribute named "*xmlString*" and its value is the serialized XML element as a "*java.lang.String*" object.

### Non-Entry mode

- If the **Return XML as** parameter is set to **DOMelement** the resulting XML element is returned as a "*org.w3c.dom.Element*" object.
- If the **Return XML as** parameter is set to **String** the XML element is returned as a "*java.lang.String*" object.

---

## Castor XML to Java FC

The CastorXMLtoJava Function Component is the mirror-image counterpart to the “Castor Java to XML FC” on page 327, and the same section on “Castor Overview” on page 327 applies.

Specifically, the CastorXMLtoJava FC creates an *Entry* or a general Java object from an XML document, and it provides the option to get data from certain parts of the XML tree when deserializing the XML document.

In addition to the Castor mapping mechanism which specifies how to build a Java object (possibly of a custom Java class) from an XML node/subtree, this Function Component provides its own logic to specify how to populate Entry Attributes from an XML document. By using XPath queries you can specify which parts of the XML document will be passed to the Castor APIs for deserializing.

This approach both provides ease of use in the IBM Tivoli Directory Integrator context and gives more power when processing custom XML documents, for example XML documents generated by other systems. Through the XPath queries you are able to specify which parts of the XML you are interested in (and get them directly into Entry Attributes) and which are irrelevant for your process and should not be processed. In addition, the writing of the Castor XML Mapping Files is facilitated since you will only have to write mapping rules for the parts of the XML document you are interested in and not for the whole XML document.

The CastorXMLtoJava Function Component uses Castor 0.9.5.4. Documentation and information for the Castor library can be obtained from the Castor project web site: <http://www.castor.org/>

## Configuration

### Parameters

#### Castor Mapping File

An XML Mapping File (as defined by the Castor syntax) that defines how XML is mapped to Java objects

The mapping file as specified by this parameter should always include the mapping rules defined in the “*TDI\_installation\_directory*/jars/functions/di\_castor\_mapping.xml” file. This means that either you must specify “jars/functions/di\_castor\_mapping.xml” as value of this parameter or make sure that the mapping file specified contains these rules (for example by using Castor’s “include” clause to include “di\_castor\_mapping.xml” rules in another mapping file).

#### Attribute Specification

Each line specifies a single Attribute in the format: <AttributeName>,<XPath query>[,<type>] . This parameter is only taken into account when the Function Component is used in Entry mode. Within each line,

##### <AttributeName>

specifies the name of the Entry Attribute;

##### <XPath query>

specifies which part(s) of the XML to unmarshal and assign as value to this Attribute.

##### <type>

must be used whenever the type of the Attribute is not a complex Java class, but one of the following basic data types: *string*, *date*, *boolean*, *integer*, *long*, *double*, *float*, *big-decimal*, *byte*, *short*, *character*, *strings* (array of strings), *chars* (array of chars), *bytes* (array of bytes). In these cases the user must specify the type, because of a limitation in Castor – Castor cannot handle these types when they map to standalone objects (instead of being members of other objects) and so the Function Component needs to know the type and take special actions to make Castor produce the correct object.

### XML Input as

This drop-down list specifies whether the Function Component will accept the input XML data in the form of a **DOMElement** object or as a **String**.

### Detailed Log

Check to generate additional log messages.

### Comment

Your own comments go here.

## Using the FC

The CastorXMLToJava Function Component creates an *Entry* or a general Java object from an XML document, and can operate both with Entry objects and with custom Java objects.

When the Function Component is passed an Entry object on input, it will return an Entry object. This mode of operation is called **Entry** mode.

When the Function Component is passed an object that is not an Entry on input (**String** or a **DOMElement**) it returns the raw Java object as it is unmarshalled by Castor. This mode of operation is called non-Entry mode.

### Entry mode

- If the **XML Input as** parameter specifies **DOMElement**, the Function Component will expect on input an Entry with an Attribute named "*xmlDOMElement*" with value of type "*org.w3c.dom.Element*".
- If the **XML Input as** parameter specifies **String**, an Entry with an Attribute named "*xmlString*" and value of type "*java.lang.String*" is expected on input.
- The output generated is an *Entry* whose Attributes are the unmarshalled XML elements as specified by the **Attribute Specification** parameter and the mapping file.

### Non-Entry mode

- If the **XML Input as** parameter specifies **DOMElement**, the Function Component will expect on input a "*org.w3c.dom.Element*" object.
- If the **XML Input as** parameter specifies **String**, a "*java.lang.String*" object is expected on input.



---

## XMLToSDO FC

The EMF XMLToSDO Function Component converts an XML document to SDO objects connected in a tree-like structure resembling the XML structure.

For each XML element an XML Attribute Data Object is created. TDI Entry Attributes are then created for some of the Data Objects. The name of the Entry Attribute consists of the names of the ancestor elements of the element the TDI Attribute represents. Subsequent XML element names are separated by the “@” character. When an XML attribute is represented, the name of the XML attribute is appended to the name of the XML element using the “#” symbol as a separator.

All Attribute names start with the “DocRoot” text which represents the XML root. There are two types of Entry Attribute values:

- The standard Java wrapper when the XML element/attribute value is a primitive type (java.lang.String, java.lang.Integer, java.lang.Boolean, etc.)
- A Service Data Object when the XML element is a complex XML structure. This will be an object of type org.eclipse.emf.ecore.sdo.EDataObject.

XML elements that have a common parent element are called siblings. Sibling elements with the same name are grouped in a multi-valued TDI Attribute Entry.

**Note:** Attributes are not created for XML elements with an ancestor element that has a sibling with the same name. Those can only be accessed through the multi-valued Attribute representing the siblings.

### Example

This example illustrates how the following XML file is processed by the EMF XMLToSDO Function Component:

```
<?xml version="1.0">
<database name="Persons">
  <description>This is a sample database</description>
  <person>
    <name>Ivan</name>
    <age>21</age>
  </person>
  <person>
    <name>George</name>
    <age>32</age>
  </person>
</database>
```

When the EMF XMLToSDO Function Component processes the example XML File, an entry with the following Attributes is created:

- DocRoot – a Service Data Object representing the XML root
- DocRoot@database - a Service Data Object representing the “database” XML element
- DocRoot@database#name – a java.lang.String object representing the “name” XML attribute of the “database” XML element.
- DocRoot@database@description - a java.lang.String representing the “description” XML element (which is a child of the “database” XML element).
- DocRoot@database@person – multi-value attribute whose values are Service Data Objects representing the individual “person” XML elements.

“DocRoot@database@person@name” is not a valid TDI Attribute in this case because more than one person XML element exists in the XML document at the same level.

The EMF XMLToSDO Function Component provides an option to use namespace prefixing. Namespace prefixing option specifies that all XML element names part of the Entry Attribute name will be prefixed with the corresponding namespace; for example: "DocRoot@namespace1:database@namespace2:person".

## Configuration

### **xsdFile**

Specifies the location of the XML Schema (XSD) File. The XML Schema File is used in the process of reading the XML document, in the generation of an EMF Ecore Model and in the Discover Schema functionality. This parameter is required.

The extension of the XML Schema File specified must be ".xsd".

### **useNamespaces**

Specifies whether XML elements and attributes namespaces will be set in the generated Entry Attribute names. When this parameter is checked XML elements and attributes will be prefixed either with a prefix defined in the "namespaceMap" parameter or with the namespace URI if no prefix is defined in "namespaceMap".

This parameter also specifies whether the Discover Schema functionality will use XML namespaces to prefix the Entry Attribute names.

### **namespaceMap**

Defines a mapping between namespace prefixes and namespace URIs. Each pair is specified on a new line. The prefix is delimited from the URI with an equal sign, for example "ibm=http://www.ibm.com". Preceding and trailing white space for both the prefix and the URI is ignored.

This parameter is only taken into account if the "useNamespaces" parameter is set to true.

### **inputXMLType**

Specifies the type of the input XML document. It can be a java.lang.String object or org.w3c.dom.Element object.

**debug** Turns on debug messages.

## Migration

The EMF XMLToSDO and SDOToXML Function Components are not compatible with the TDI 6.0 Castor Function Components. Any solution which uses the Castor Function Components needs to be re-implemented in order to work with the EMF XMLToSDO and EMF SDOToXML Function Components. The Castor XML To Java Function Component supports a mapping file. This mapping file can be used to specify how a complex custom XML is to be parsed and converted to a complex custom Java object. This feature is not supported by the EMF XMLToSDO Function Component. By following the next broad guidelines, a TDI 6.0 configuration can be re-implemented to work with the EMF XMLToSDO Function Component:

1. Insert the EMF XMLToSDO Function Component into an AssemblyLine.
2. Set its parameters accordingly.
3. Insert a Script Component into the AssemblyLine right after the EMF XMLToSDO Function Component.
4. Write Javascript code in this Script Component, which extracts the desired data from the SDO DataObject returned by the EMF XMLToSDO Function Component and populates the custom Java Object needed.

The Castor XML To Java Function Component used to support a mechanism which allowed a specific portion of the XML to be mapped to Entry Attributes. The EMF XMLToSDO Function Component does not support this feature. The EMF XMLToSDO Function Component always parses and maps the entire XML to Entry Attribute. By using the Input Attribute Map of the EMF XMLToSDO Function Component, however, only the desired Attributes can be mapped thus emulating the behavior of the Castor XML To Java Function Component.

The Castor Java To XML Function Component used to support a mapping file, which could be used to specify how to serialize a complex Java object into XML (element/attribute names, etc.). The EMF SDOToXML Function Component serializes into XML based on an XML Schema file, that is, the names of elements/attributes, etc. are specified in the XML Schema file specified as a Function Component parameter.



---

## SDOToXML FC

The EMF SDOToXML Function Component converts Service Data Objects to XML. This component uses an XML Schema definition to build an Ecore model.

The Function Component receives an Entry whose Attributes represent an XML document. The types of the Entry Attribute values are either Java classes representing primitive types or Service Data Objects (`org.eclipse.emf.ecore.sdo.EDataObject`) representing complex XML elements.

The Entry Attribute names describe the XML hierarchy in exactly the same manner as the EMF XMLToSDO Function Component constructs Attribute names. All Attribute names start with “DocRoot” which represents the XML root. Subsequent elements down the XML hierarchy are separated with the “@” character. If the TDI Entry Attribute represents an XML attribute the “#” character is used to separate the name of the XML attribute from the name of the XML element containing this attribute.

It is possible that the TDI Entry passed contains only Entry Attributes corresponding to the real data. For example, the Entry may contain an Attribute “DocRoot@database@person” without containing an Attribute “DocRoot@database” – the EMF SDOToXML Function Component will automatically create the “database” XML element in the XML document it builds. The EMF SDOToXML Function Component uses the XML Schema to track and create all XML elements that are ancestors of the specified XML element or attribute.

It might happen that the Entry contains Attributes specifying XML elements that are contained in other XML elements specified by Entry Attributes, for example the Entry contains both “DocRoot@database@person” and “DocRoot@database” Attributes. In this case the Attributes are processed starting from the one that is closest to the root, continuing with the one closest to it and so on – the last one will be the most specific XML element that is contained in all the other. This order of processing provides the option to change specific details in a bigger XML context.

For example, if you want to change just the “DocRoot@database@person” element but you want to leave the other parts of the “DocRoot@database” element untouched, you might read the XML document with the EMF XMLToSDO Function Component, map the “DocRoot@database” attribute and provide it to the EMF SDOToXML Function Component as is. Then you will also provide the “DocRoot@database@person” Attribute that contains the specific updates you want to make on the “person” XML element(s). The EMF SDOToXML Function Component will first process the “DocRoot@database” applying all the content to the resulting XML and it will then override the “person” child of the “database” element with whatever is provided in the “DocRoot@database@person” Entry Attribute.

In case a multi-valued Attribute is provided together with an Attribute specifying a child or other successor of that element, the function Component will signal an error (throw exception) because it cannot be determined to which of the sibling XML elements, this successor applies. For example, if “DocRoot@database@person” is provided and contains two values (thus specifying two XML “person” elements at the same level) and also “DocRoot@database@person@name” is provided, the Function Component would not know to which “person” element of the two existing this “name” element applies to. The names of the elements in the Entry Attribute can be XML namespace prefixed.

The names of the elements are prefixed with the namespace URI or with the prefixes defined in the “namespaceMap” parameter.

For example, in order to construct the following XML document:

```
<?xml version="1.0"?>
<database xmlns="www.ibm.com" xmlns:tmp="www.tmp.com" name="employees">
  <person>
```

```
<name>Ivan</name>
<tmp:age>21</tmp:age>
<person>
</database>
```

the following TDI Entry can be passed to the EMF SDOToXML Function Component:

- DocRoot@ibm:database#ibm:name
- DocRoot@ibm:database@ibm:person@ibm:name
- DocRoot@ibm:database@ibm:person@www.tmp.com:age

The namespace prefixes used assume that the “namespaceMap” parameter contains the “ibm” prefix set to “www.ibm.com” and no namespace prefix is defined for “www.tmp.com” (that is why it is used directly in the Attribute name). More details on the “namespaceMap” parameter can be found in section “Configuration”.

## Configuration

### xsdFile

The parameter specifies the location of the XML Schema File. The XML Schema File is used in the process of generating the XML document and in the Discover Schema functionality. This parameter is required. The extension of the XML Schema File specified must be “.xsd”.

### useNamespaces

Specifies whether the Discover Schema functionality will use XML namespaces to prefix the Entry Attribute names. When this parameter is checked XML elements and attributes will be prefixed either with a prefix defined in the “namespaceMap” parameter or with the namespace URI if no prefix is defined in “namespaceMap”.

### namespaceMap

Defines a mapping between namespace prefixes and namespace URIs. Each pair is specified on a new line. The prefix is delimited from the URI with an equal sign, for example “ibm=http://www.ibm.com”. Preceding and trailing white space for both the prefix and the URI is ignored.

### returnXMLType

Specifies the type of the XML document that will be returned by the Function Component. It can be a java.lang.String object or an org.w3c.dom.Element object.

**debug** Turns on debug messages.

## Using the FC

### Migration

The EMF XMLToSDO and SDOToXML Function Components are not compatible with the TDI 6.0 Castor Function Components. That is why any solution which uses the Castor Function Components needs to be re-implemented in order to work with the EMF XMLToSDO and EMF SDOToXML Function Components. The Castor XML To Java Function Component used to support a mapping file. This mapping file could be used to specify how a complex custom XML is to be parsed and converted to a complex custom Java object. This feature is not supported by the EMF XMLToSDO Function Component. However by following the next broad guidelines such a TDI 6.0 configuration can be re-implemented to work with the EMF XMLToSDO Function Component:

1. Insert the EMF XMLToSDO Function Component into an AssemblyLine.
2. Set its parameters accordingly.
3. Insert a Script Component into the AssemblyLine right after the EMF XMLToSDO Function Component.

4. Write Javascript code in this Script Component, which extracts the desired data from the SDO DataObject returned by the EMF XMLToSDO Function Component and populates the custom Java Object needed.

The Castor XML To Java Function Component used to support a mechanism which allowed a specific portion of the XML to be mapped to Entry Attributes. The EMF XMLToSDO Function Component does not support this feature. The EMF XMLToSDO Function Component always parses and maps the entire XML to Entry Attribute. By using the Input Attribute Map of the EMF XMLToSDO Function Component, however, only the desired Attributes can be mapped thus emulating the behavior of the Castor XML To Java Function Component.

The Castor Java To XML Function Component used to support a mapping file, which could be used to specify how to serialize a complex Java object into XML (element/attribute names, etc.). The EMF SDOToXML Function Component serializes into XML based on an XML Schema file, that is, the names of elements/attributes, etc. are specified in the XML Schema file specified as a Function Component parameter.





---

## AssemblyLine FC

The AssemblyLine FC wraps the calling of another AssemblyLine into a Component, with some controls on how the other AssemblyLine is executed and what to do with a possible result.

### Configuration

#### AssemblyLine

A drop-down list of pre-defined AssemblyLines that could be the target of this FC.

**Server** The TDI Server on which the AssemblyLine should be run. Use "Local" or blank for internal server or *hostname[:port]* for remote server.

#### Config Instance

Specify the config instance when using a remote server.

#### Execution Mode

A drop-down list of three possible modes:

##### Run and wait for result

Result can be picked up as described in the JavaDocs for this FC; this typically involves calling the FC with an empty Entry object. The returned Entry object contains the reference to the target AL in its "value" attribute.

##### Run in background

This starts the AssemblyLine asynchronously, and does not wait for any results.

##### Manual (cycle mode)

#### Detailed Log

When checked, generates additional log messages.

#### Comment

Your own comments go here.

## Using the FC

This FC provides a handler object for calling and managing AssemblyLines on either the local or a remote Server.

You configure this FC by choosing the AL to call, the Server on which this AL is defined and should run on (blank or "local" indicating that the AL runs on this Server which is running the FC), as well as the Config Instance that the AL belongs to. Again, a blank parameter value means that this AL is in the same Config Instance as the one containing the FC itself.

You also choose the Execution Mode (see "AL Cycle Mode" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide* for more information). Although there are three Execution Modes (Run and wait for completion, Run in background and Manual cycle mode), the first two options are the standard methods of starting an AL from script with or without calling the AL `join()` method.

These first two modes cause the target AL to run on its own (stand alone) in its own thread. The third mode, cycle mode, means that the target AL is controlled by the FC which will execute it one cycle at a time for each time the FC is invoked. When the FC runs an AssemblyLine in stand-alone mode, the FC keeps a reference to the target AL – just like you get when you call `main.startAL()`. The FC can also return the status of the running/terminated ALs. You obtain this status by calling the FC's `perform()` method with a null or empty Entry parameter. The returned Entry object contains the reference to the target AL in an attribute called "value". If you pass a null value to the FC, the return value is the actual reference to the target AL (again, like making a `main.startAL()` call).

You can also call the FC with specific string command values to obtain info about the target AL:

|                   |   |
|-------------------|---|
| perform("target") | returns the object reference of the target AL.  |
| perform("active") | returns either "active", "aborted" or "terminated" depending on the target AL status.         |
| perform("error")  | returns the java.lang.Exception object when the status is "aborted".                          |
| perform("result") | returns the current result Entry object.  |
| perform("stop")   | tries to terminate an active target AL, and will throw an error if the call does not succeed. |

Note that if you have specified the "Run and wait for completion" Execution Mode, then each call to perform() starts the target AL and returns the complete status for the execution (e.g. reference to the target as well as status and error object). In this case, the initialize() method does NOT start the target AL as it does in all other cases. When the FC is called in this mode with an Entry object, the Entry object can contain one or more of the above keywords in an attribute called command (as described in the list above, and concatenated in a comma-separated list). The returned Entry object is then populated with the same values as described above. So, rather than calling perform() several times with each desired command, you can create an Entry with all keywords as attributes in the Entry object and get away with one call to perform():

```
var e = system.newEntry();
e.setAttribute("command", "target, status");
// In this example, fc references a Function Interface.
// If this was an AL Function instead, then fc.callreply(e)
// would be done.
var res = fc.perform(e);
task.logmsg("The status is: " + res.getString("status"));
```

When the FC runs an AL in manual mode, each call with an Entry object causes one cycle to be executed in the target AL. The returned Entry object is the work entry result at the end of the cycle. When the target AL has completed, a null entry is returned. If the cycle execution causes an error, then that error is re-thrown by the FC (so you should use a try-catch block in your script).

Note that the Quick Discovery button in the FC Input and Output Map tabs will try the following methods for determining the schema of the AL to be called:

1. If the AL has a defined schema (AL Call/Return tab), then this will be used.
2. Otherwise the FC examines the Input and Output maps of all Connectors in the AL to be called in order to "guess" its schema.

---

## Java Class Function Component

IBM Tivoli Directory Integrator 6.1.1 (TDI) allows you to use Java objects in your script code to perform specific operations not provided directly by TDI. Because calling methods of Java objects when the Java object must be constructed and parameters mapped to proper classes can be difficult, the Java class Function Component makes using Java objects in your scripts easier. The Java Class Function Component allows you to choose a Java class and method through the Config Editor and performs the conversion and mapping of parameters to the method.

### Schema

The schema for the Java Class Function Component is dynamic and reflects the chosen Java class and method. The Function Component also performs dynamic conversion of parameters to match the signature of the target Java class/method.

### Parameter Conversion

Parameter conversion is performed for the most common types. However, it is beyond the scope of this FC to provide conversion for all potential Java class objects. For unsupported objects you must explicitly create these before invoking the Java Class Function Component. Below is a table of objects that the Java Class Function Component will recognize for parameter conversions.

*Table 38.*

| Parameter type | Notes   |
|----------------|---|
| Integer        | Both object and primitive type                                    |
| Long           | Both object and primitive type                                    |
| Double         | Both object and primitive type                                    |
| Float          | Both object and primitive type                                    |
| Short          | Both object and primitive type                                    |
| Byte           | Both object and primitive type                                    |
| Character      | Both object and primitive type                                    |
| Boolean        | Both object and primitive type                                    |
| Date           | Only conversion from default date format as defined by DateFormat |
| String         |   |

In addition to these types, the Java Class Function Component will also attempt conversion into primitive arrays and `java.util.Collection` objects.

### Configuration

The Java Class Function Component uses the following parameters:

#### JAR/Class File

This parameter specifies the file in which the Java class is found.

#### Java class

Specifies the fully qualified name of the Java class. This parameter is required.

#### Method

Specifies the method to call in the Java class.



---

## Parser FC

The Parser FC wraps a Parser into an AssemblyLine Component, such that it can be inserted anywhere in the AssemblyLine data flow.

Multiple instances of Parser FCs could aid in decoding two or more layers of protocol.

## Configuration

### Content Parser

A drop-down list of pre-defined parsers that interpret or generate data stream records.

### Operation Mode

Operation mode of the Parser: Read an Entry from parser, Write an Entry to parser (returning result)

### Returns result as String

Check to have the function return a String object instead of a *Bytearray* object

### Detailed Log

When checked, generates additional log messages.

### Comment

Your own comments go here.

## Using the FC

This FC allows you to select a Parser and then set its mode to either input (**Read**) or output (**Write**).

In **Read** mode, you must provide an attribute (in the Output Map) called "*value*" which is either a string, a File, a Reader or a java.io.InputStream object to be used as input for the Parser. The FC will return an *Entry* object (conn) with the parsed attributes, which are then available for your Input Map.

In **Write** mode the FC takes an Entry with the attributes passed in by the Output Map and applies the Parser to that Entry, providing the return bytestream in the Attribute named "*value*". This Attribute is a java.lang.String if you select the **Return result as String** checkbox in the Config tab; otherwise it is a *bytearray*.



---

## Scripted FC

Like Connectors, EventHandlers and Parsers, IBM Tivoli Directory Integrator allows you to fully program a Function Component using scripting. This is done by means of the template that the Scripted FC provides.

## Configuration

Configuration is relatively simple as all logic is in the Script pane.

### Detailed Log

When checked, generates additional log messages.

### Comment

Your own comments go here.

## Using the FC

The bulk of the FC is in the script pane; in here, you must provide the logic that make up the FC.

To aid in programming, you are provided with stub functions as a reminder of the functions required to make a valid FC. These are:

### **initialize (fc,obj)**

This function is called during the initialization phase of the AssemblyLine this FC is part of. The *obj* parameter is the parameter block as described by your FCs Config dialog.

### **terminate (fc)**

This function is called during the termination phase of the AssemblyLine this FC is part of. Here is where you would release resources, etc.

### **perform (fc,obj)**

This is the function that performs the actual work, and is called by the AssemblyLine at the point you positioned the FC. The *obj* parameter is the parameter block as described by your FCs Config dialog.

### **getUI (fc)**

This function implements/overrides the standard `getUI()` method, and can be used to configure the FC's operational parameters. This function is optional.

These correspond to the three main Function Interface methods. Each method is passed an initial Function Component parameter, which is the AL FC wrapper, giving your script access to settings like the Attribute Maps etc.

## See also

"Script Connector" on page 201,

"Script Parser" on page 305,

"JavaScript Connector" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.





---

## CBE Generator Function Component

The CBE Generator Function Component allows you to generate Common Base Event (CBE) event objects which can be written to CBE logs or issued to an IBM Common Event Infrastructure (CEI) server.

### Common Base Event (CBE)

Common Base Event (CBE) facilitates effective intercommunication among disparate enterprise components that support logging, management, problem determination, autonomic computing, and e-business functions.

An event encapsulates message data sent as the result of an occurrence of a situation. Events exchanged between and among applications in complex information technology systems allow these various facets of the system to interoperate, communicate and coordinate their activities. Fundamental aspects of enterprise management and e-business communications, such as performance monitoring, security and reliability, as well as fundamental portions of e-business communications, such as order tracking, are grounded in the viability and fidelity of these events.

The Common Base Event is defined as a new standard for enterprise management and business applications events. The Common Base Event definition ensures completeness of the data by providing properties to publish general information whenever a situation occurs. This general information provided by the Common Base Event is called the 3-tuple.

The following elements constitute the 3-tuple:

- The identification of the component that is reporting the situation
- The identification of the component that is affected by the situation (which may be the same as the component reporting the situation)
- The situation itself

### The Common Event Infrastructure (CEI)

The Common Event Infrastructure (CEI) is IBM's implementation of a consistent, unified set of APIs and infrastructure for the creation, transmission, persistence and distribution of a wide range of business, system and network CBE formatted events. CEI is based upon the Autonomic Computing Division's CBE specification, which defines a standard format for event information, which devices and software use to keep track of transactions and other activity.

### CBE FC Configuration

The CBE Generator Function Component uses the following parameters:

#### Logger's Name

The name of the logger. This is an optional attribute and if you not define it defaults to LocalHostIP .

#### Debug

Turns on debug messages. This parameter is globally defined for all TDI components.

### Input and Output Map Attributes

The CBE specification has a complex structure. To enable you to define the attributes, a dotted notation for the attributes is supported in the attribute map for some of the components. To know more about these attributes and their suggested values please refer to the Autonomic Computing Toolkit Developer's Guide at: [http://www-128.ibm.com/developerworks/autonomic/books/fpy0mst.htm#ToC\\_91](http://www-128.ibm.com/developerworks/autonomic/books/fpy0mst.htm#ToC_91).

Table 39. Input map attributes

| Attribute Name | Attribute Type  |
|----------------|---|
| Event          | org.eclipse.hyades.logging.events.cbe.CommonBaseEvent |
| eventXml       | String  |

Table 40. Output map attributes

| Attribute Name                             | Attribute Type | Description   |
|--|----------------|---|
| CreationTime                               | String         | The time the event was created. Default value will be the time when the event object is created in the CBEGeneratorFC.  |
| GlobalInstanceId                           | String         | Primary Identifier of event. A unique id will be generated if not passed by user.   |
| Message                                    | String         | Optional property   |
| Severity                                   | Integer        | Optional property. Value ranges from 0 – 70   |
| ExtensionName                              | String         | Optional property.  |
| SequenceNumber                             | Integer        | Optional property   |
| RepeatCount                                | Integer        | Optional property.  |
| ElapsedTime                                | Integer        | Optional property if RepeatCount is not set.  |
| Priority                                   | Integer        | Optional property. Values range from 0 – 100.   |
| <i>situation.</i>                          |                | <i>This notation defines properties of the situation object.</i>  |
| situation.CategoryName                     | String         | Describes the type of Situation. Defined Values are <ul style="list-style-type: none"> <li>• StartSituation</li> <li>• StopSituation</li> <li>• ConnectSituation</li> <li>• ConfigureSituation</li> <li>• RequestSituation</li> <li>• FeatureSituation</li> <li>• DependencySituation</li> <li>• CreateSituationDestroy</li> <li>• SituationReportSituation</li> <li>• AvailableSituation</li> <li>• OtherSituation</li> </ul> This is a required property. |
| situation.reasoningScope                   |                | Describes scope of the situation. This is a required property.  |
| availableSituation.operationDisposition    | String         | Required if CategoryName is AvailableSituation  |
| availableSituation.processingDisposition   | String         | Required if CategoryName is AvailableSituation  |
| availableSituation.availabilityDisposition | String         | Required if CategoryName is AvailableSituation  |
| configureSituation.successDisposition      | String         | Required if CategoryName is ConfigureSituation  |
| connectSituation.successDisposition        | String         | Required if CategoryName is ConnectSituation  |
| connectSituation.situationDisposition      | String         | Required if CategoryName is ConnectSituation  |
| createSituation.successDisposition         | String         | Required if CategoryName is CreateSituation   |
| dependencySituation.dependencyDisposition  | String         | Required if CategoryName is DependencySituation   |
| destroySituation.successDisposition        | String         | Required if CategoryName is DestroySituation  |

Table 40. Output map attributes (continued)

| Attribute Name                      | Attribute Type | Description  |
|-------------------------------------|----------------|--|
| featureSituation.featureDisposition | String         | Required if CategoryName is FeatureSituation   |
| reportSituation.reportCategory      | String         | Required if CategoryName is ReportSituation  |
| requestSituation.successDisposition | String         | Required if CategoryName is RequestSituation   |
| requestSituation.situationQualifier | String         | Required if CategoryName is RequestSituation   |
| startSituation.successDisposition   | String         | Required if CategoryName is StartSituation   |
| startSituation.situationQualifier   | String         | Required if CategoryName is StartSituation   |
| stopSituation.successDisposition    | String         | Required if CategoryName is StopSituation  |
| stopSituation.situationQualifier    | String         | Required if CategoryName is StopSituation  |
| otherSituation.any                  | String         | Required if CategoryName is OtherSituation   |
| <b>SCI.</b>                         |                | <i>This notation describes the source component identification. These are required properties for a CommonBaseEvent.</i>         |
| SCI.location                        | String         |  |
| SCI.locationType                    | String         |  |
| SCI.executionEnvironment            | String         |  |
| SCI.component                       | String         |  |
| SCI.subcomponent                    | String         |  |
| SCI.componentIdType                 | String         |  |
| SCI.componentType                   | String         |  |
| <b>RCI.</b>                         |                | <i>This notation describes component identification information for the reporter component. This is not a required property.</i> |
| RCI.location                        | String         |  |
| RCI.locationType                    | String         |  |
| RCI.executionEnvironment            | String         |  |
| RCI.component                       | String         |  |
| RCI.subcomponent                    | String         |  |
| RCI.componentIdType                 | String         |  |
| RCI.componentType                   | String         |  |
| <b>X.</b>                           |                | <i>This notation describes an ExtendedDataElement (EDE). This is not a required property.</i>                                    |
| X.attributeName                     | String         | Creates EDE with name attribute Name and value defined by user   |
| X.attributeName.childAttributeName  | String         | Creates EDE with name attribute Name and child element with name childAttributeName  |

## Function Component API

The CBEGenerator FC exposes the following methods (also see the Javadocs for this component):

**public String convertCBEventToXML (CommonBaseEvent event) throws Exception**

This method will convert a CommonBaseEvent object to a XML string object. This XML will also be available by default in the eventXml attribute of the Input Map.

### **public String getCBELogXML (CommonBaseEvent event, boolean isCompleteXML)**

This method is a wrapper over the `org.eclipse.hyades.logging.java.CommonBaseEventLogRecord` class's `externalizeCanonicalXmlDocString()` and `externalizeCanonicalXmlString()` API. This method can be used for obtaining a CBE Log XML. Whether the XML string returned is a complete XML document or just an XML fragment is decided by the `isCompleteXML` flag.

For more details see: <http://download.eclipse.org/tptp/4.2.0/javadoc/Platform/public/org/eclipse/hyades/logging/java/CommonBaseEventLogRecord.html>

Also see "Generating a CBE Log XML."

### **public static String mapCbeToEntry (CommonBaseEvent cbe, Entry entry)**

This static method maps the fields of a Common Base Event object into the attributes of a TDI Entry. The process is the reverse of what the CBE Generator FC's 'perform' method does. All attributes in the resulting Entry are of type `java.lang.String`.

This method is accessible through Javascript in TDI.

## **Generating a CBE Log XML**

In one of the scripts (after event generation from CBE Generator), a call to the `getCBELogXML()` API (exposed in the `CBEGeneratorFC`) can be made, and the newly created *event* object can be passed. The resulting output string will be an XML fragment which adheres to the Hyades CBE Logging format. The string received from the `getCBELogXML()` API can be (for example) set back into the work entry by calling the `work.setAttribute()` API.

```
var cbe = work.getObject("event");
var xmlString = com.ibm.di.fc.cbe.CBEGeneratorFC.getCBELogXml(cbe, false);
work.setAttribute("logXML",xmlString);
```

Then, using the File System connector with a `LineReader` parser, you can write this new attribute (containing the CBE Log XML) to any log file.

## **See also**

- Autonomic Computing Toolkit (includes specification of the Common Base Event)
- Common Base Event best practices: Getting it right the first time. Highlights of the "Best Practices for the Common Base Event and Common Event Infrastructure" manual
- Common Base Event Best Practices Guide
- An example of generating Common Base Events with TDI in `examples/cbe_demo`

---

## SendEmail Function Component

The SendEmail Function Component uses the JavaMail API to send e-mails. By connecting to an Simple Mail Transfer Protocol (SMTP) server, the SendEmail Function Component can send e-mails to multiple recipients and can optionally attach multiple files to e-mails. You can also attach multiple files with different Multipurpose Internet Mail Extensions (MIME) types.

**Note:** Many Web-based e-mail services provide access only to browsers with HTTP. These services cannot be accessed using the SendEmail Function Component.

### Configuration

The SendEmail Function Component uses the following parameters:

#### **smtpServerHost**

The parameter specifies the address of the SMTP server that sends mails. If this parameter is not set the smtpServer Entry Attribute should be mapped.

#### **smtpServerPort**

Specifies the port of the SMTP server that sends mails.

#### **username**

This parameter is the user name used for SMTP authentication. Do not enter a value for this parameter if the SMTP Server does not require a user name and password authentication.

#### **password**

This parameter is password used for SMTP authentication.

#### **useSSL**

This parameter uses Secure Sockets Layer (SSL) to communicate with the SMTP server.

**from** Specifies the content of the **From** field in the e-mail. If this parameter is not set, the from Entry Attribute should be mapped. The from parameter cannot contain spaces.

#### **recipients**

This parameter is a comma separated list of the recipients' addresses. If this parameter is not set, the recipients Entry Attribute should be mapped.

#### **subject**

Specifies the subject of the e-mail. This is a mandatory field; if absent, an exception is thrown.

#### **attachments**

This parameter allows you to attach any files(s) you want to include with your message. To set different a MIME type for individual attached files, add the MIME attachment type after file name. The MIME type and file name must be separated by the character >. For example:

```
SomeDocument.pdf>application/pdf
```

#### **contentType**

This parameter allows you to set the MIME content type of the e-mail's body. text/plain is the default value.

#### **encoding**

Specifies the MIME charset to use for encoded words and text parts. If left blank the default system charset is used. Supported encodings can be found at: <http://java.sun.com/j2se/1.5/docs/guide/intl/encoding.doc.html>.

#### **Debug**

Turns on debug messages. This parameter is globally defined for all TDI components



---

## Memory Queue FC

Aka. MemQueue FC. The Memory Queue FC encapsulates the functionality of the TDI Memory Buffer Pipe (as present in the API) and provides a GUI configuring it. The FC contains two parts: the raw FC and the Config Editor (GUI) component. The raw FC encapsulates the calls to the memory buffer pipe. The GUI provides a way for the user to configure the behavior of a memory buffer pipe. The FC either returns a reference to the Memory Buffer Pipe object or reads/writes to it.

**Note:** The Memory Queue FC is deprecated in this release. It is much easier and also recommended to use the “Memory Queue Connector” on page 149 or directly use “The system object” on page 439 to create a new pipe, add data to the pipe and put data into the pipe. APIs for all these functionalities have been exposed in the System Object.

## Configuration

### Instance name

Name of the TDI instance on which to create the Memory Buffer Pipe. The current instance is assumed if this is blank (default).

### Pipe name

Name of the Memory Buffer Pipe to be created.

### Watermark

The Watermark parameter is either:

- With **Paging Off** (next parameter), it is the maximum queue size. When this size is reached, the **Blocking Add Parameter** determines if the read waits or fails since the queue is full.
- With **Paging On**, it is the threshold at which objects are persisted to the System Store. Note that the Page Size determines when pages are actually written, so the Watermark should be a multiple of the Page Size.

### Enable paging using System Store

Check this to let the Memory Buffer Queue use the System Store for paging.

### Page Size

Number of entries in one page.

### Database name

A JDBC URL of an external database to use.

### Username

Login username to the database used.

### Password

Login password to the database used.

### Table name

Table to use for paging.

### Blocking add operation

Check this option to block or fail (and always log that data is lost) while adding, if queue is full and no paging used.

### Detailed Log

Check for additional log messages.

## Using the FC

“The system object” on page 439 has a method called *getFunction(string name)* that returns an initialized instance of the FC. The returned object can be used to perform calls as in:

Using a simple call:

```
MemoryBufferQ pipe = system.getFunction("ibmdi.MemoryBufferPipeFC").perform(null);
```

Using the *Entry* call:

```
var inp = system.newEntry();  
inp.setAttribute ("test", "this is a sample entry");  
MemoryBufferQ pipe = system.getFunction("ibmdi. MemoryBufferPipeFC").perform(inp);
```

The Memory Buffer Queue FC returns a reference to a Memory Buffer Pipe for a null Entry object, performs a read operation on the Memory Buffer Pipe for the empty Entry object and a write operation on the Memory Buffer Queue for a non-empty Entry object.

The returned MemoryBufferQ object has two methods that can aid in managing the object: `purgeQueue()` and `deletePipe()`.

## See also

“Memory Queue Connector” on page 149

“System Queue Connector” on page 171



---

## Axis Java To Soap FC

The Axis Java-to-Soap Function Component (FC) is part of the TDI Web Services suite.

This component can be used both on the web service client and on the web service server side. This component receives an Entry or a Java object and produces the SOAP request (when on the client) or response (when on the server) message. It will provide the whole SOAP message, as well as separately the SOAP Header and the SOAP Body to facilitate processing and customization.

The component supports both RPC and Document style.

## Configuration

### Parameters

#### WSDL URL

The URL of the WSDL document describing the service

#### SOAP Operation

The name of the SOAP operation as described in the WSDL file

#### Return XML as

This drop-down list specifies whether the result is returned as a String or a DOM Element.

#### Complex Types

This parameter is optional; if specified, it should be a list of fully qualified Java class names (including the package name), where the different elements (Java classes) of this list are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

**Mode** A flag that indicates whether this FC should generate a SOAP **request** (when deployed on the client) or a SOAP **response** (when deployed on the server) message

#### Use Multi Refs

This parameter is taken into account only when RPC-style web services are used. When Document-style web services are used this parameter has no effect on the generated SOAP message.

If checked and the web service used is an RPC-style web service, the generated SOAP message will use multi-refs. If **not** checked and the web service used is an RPC-style web service, the generated SOAP message will not **use** multi-refs.

#### Operation Parameters

This parameter is a list of Attribute names, where different Attribute names are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

#### Detailed Log

When checked, generates additional log messages.

#### Comment

Your own comments go here.

### Function Component Input

*Entry* or *Java Object*. If anything else is passed, an Exception is thrown.

### Function Component Output

An Entry object with 3 attributes – one for the whole SOAP message, one for the SOAP Header and one for the SOAP Body. The SOAP message, Body and Header will be either XML strings or DOM objects, as specified by the **Return XML as** parameter.

## Using the FC

This Function Component (FC) serializes the Java representation of a SOAP message into the XML representation of that SOAP message.

- If this FC is passed (a) an *Entry* with a *"soapFault"* Attribute, whose value is an object of type `org.apache.axis.AxisFault`, or (b) a Java object of type `org.apache.axis.AxisFault`, then the FC generates a SOAP Fault message containing the information stored in the passed *AxisFault* object.
- If the value of the **Return XML as FC** parameter is **String** then the SOAP response message is stored in the *"xmlString"* Attribute, if an *Entry* was passed to the FC. However, If the value of the **Return XML as FC** parameter is **DOMELEMENT** then the generated SOAP message is stored in the *"xmlDOMELEMENT"* Attribute, if an *Entry* was passed to the FC. If a *Java Object* array (`Object[]`) was passed to this FC, then the return value of the FC is either a `java.lang.String` object (when the value of the **Return XML as FC** parameter is **String**) or an `org.w3c.dom.Element` object (when the value is **DOMELEMENT**).
- If the value of the *"soapFault"* Attribute passed in is not of type `org.apache.axis.AxisFault`, then an Exception is thrown.
- Each item from the value of the **Operation Parameters** FC parameter is the name of an Attribute, which must be present in the *Entry* passed to the FC. If any of these Attributes is missing, an Exception is thrown.
- If this FC is passed a *Java Object* array (`Object[]`) then it passes the SOAP operation each Java Object from this array in the order in which the Objects are stored in the array. If this FC is passed an *Entry*, then the order and values of the parameters passed to the SOAP operation are determined by the value of the **Operation Parameters** FC parameter.
- The order of the items from the value of the **Operation Parameters** FC parameter determines the order in which the Attribute values are passed as parameters to the SOAP operation.
- This FC is capable of generating (a) Document style SOAP messages, (b) RPC style SOAP messages and (c) SOAP Fault messages. The style of the message generated is determined by the WSDL specified by the **WSDL URL** FC parameter.
- The FC is capable of generating SOAP messages encoded using both "literal" encoding and SOAP Section 5 encoding. The encoding of the message generated is determined by the WSDL specified by the **WSDL URL** FC parameter.
- The parameter **Use Multi Refs** can mean different things, but is applicable only for RPC-style messages; when Document-style web services are used this parameter has no effect on the generated SOAP message. If checked and the web service used is an RPC-style web service, the generated SOAP message will use multi-refs. If **not** checked and the web service used is an RPC-style web service, the generated SOAP message will **not** use multi-refs.

**Note:** The presence of the **Use Multi Refs** parameter is a consequence of using the Axis library to implement this FC. Currently when the Axis `JavaToSoap` FC serializes an RPC-style message it uses XML hrefs/multi-refs in the generated SOAP, and this breaks the Axis C++ library. That is why an Axis `JavaToSoap` FC configuration parameter is present to allow you to switch hrefs/multi-refs on and off.

- This FC is capable of generating SOAP messages containing values of complex types which are defined in the `<types>` section of a WSDL document. In order to do that this FC requires that (1) the **Complex Types** FC parameter contains the names all Java classes that implement the complex types used as parameters to the SOAP operation and (2) these Java classes' class files are located in the Java class path of TDI.
- If this FC was passed an *Entry* object, then the FC stores the generated SOAP message Header and SOAP message Body (apart from the entire generated SOAP message) as Attributes in the returned *Entry*. If the value of the **Return XML as FC** parameter is **String** then the SOAP Header and Body are stored in the *"soapHeaderString"* and *"soapBodyString"* Attributes respectively as `java.lang.String` objects. If the value of the **Return XML as FC** parameter is **DOMELEMENT** then the SOAP Header and Body are stored in the *"soapHeaderDOMELEMENT"* and *"soapBodyDOMELEMENT"* Attributes respectively as `org.w3c.dom.Element` objects.

## Custom serializers/deserializers

Both AxisJavaToSoap and AxisSoapToJava Function Components provide methods for registering XML type to Java type mappings with custom serializers/deserializers (by default all complex types are serialized/deserialized by the Axis' org.apache.axis.encoding.ser.BeanSerializer/org.apache.axis.encoding.ser.BeanDeserializer).

```
/**
 * This method is analogous to the 'registerTypeMapping' method in org.apache.axis.client.Call.
 * It can be used for configuring serialization/deserialization of Java types, for which the
 * default serializer/deserializer (org.apache.axis.encoding.ser.BeanSerializer/
 * org.apache.axis.encoding.ser.BeanDeserializer) is not suitable.
 */
public void registerTypeMapping(Class javaType,
                               QName xmlType,
                               SerializerFactory serializerFactory,
                               DeserializerFactory deserializerFactory)
```

This method can be invoked on an FC in the "After Initialize" Prolog FC hook through JavaScript like this:

```
var myClass = java.lang.Class.forName("mypackage.MyClass");
var myQName = new javax.xml.namespace.QName("http://www.myserver.com", "MyClass");
var mySerializerFactory = new mypackage.MySerializerFactory();
var myDeserializerFactory = new mypackage.MyDeserializerFactory();

myFC.getFunction().registerTypeMapping(myClass, myQName, mySerializerFactory, myDeserializerFactory);
```

## See Also

"Axis Soap To Java FC" on page 365



---

## WrapSoap FC

The WrapSoap Function Component (FC) is part of the TDI Web Services suite.

This component is used to generate a complete SOAP message given the SOAP Body and optionally a SOAP Header.

Such a component is useful when the user customizes the content of the SOAP Body or creates it completely on his own (using Castor binding for example). This component will accept the contents of the SOAP Body and the SOAP Header and attributes for the SOAP Envelope, Header and Body XML elements (usually namespace declarations) and will create the complete SOAP message.

This is actually a helper FC that will save the user from error-prone processing of string or DOM objects to wrap his SOAP data into a complete SOAP message.

## Configuration

### Parameters

#### Input the SOAP Body and Header as

This drop-down specifies whether the SOAP Body and SOAP Header input values will be passed as String (that is, `java.lang.String`) or as DOM objects (`org.w3c.dom.Node`).

#### Return the SOAP message as

This drop-down specifies whether the complete SOAP message should be returned as a String or as a DOM object.

#### Header and Body tags present

Specifies whether the SOAP Body passed in an Attribute contains the `<Body>` tag and whether the SOAP Header passed in an Attribute contains the `<Header>` tag.

#### Attributes to add to the SOAP Envelope

Specifies the XML attributes and their values to include in the SOAP Envelope XML element.

#### Namespace declarations to add to the SOAP Envelope

Specifies Namespace declarations to add to the SOAP Envelope.

#### Attributes to add to the SOAP Body

Specifies the XML attributes and their values to include in the SOAP Body XML element.

#### Namespace declarations to add to the SOAP Body

Specifies Namespace declarations to add to the SOAP Body.

#### Attributes to add to the SOAP Header

Specifies the XML attributes and their values to include in the SOAP Header XML element.

#### Namespace declarations to add to the SOAP Header

Specifies Namespace declarations to add to the SOAP Header.

#### Detailed Log

Check to generate additional log messages.

#### Comment

Your own comments go here.

### Function Component Input

*Entry* object – it has one Attribute for the SOAP Header (optional) and one Attribute for the SOAP Body.

If anything else is passed an Exception is thrown.

## Function Component Output

An *Entry* object that contains the complete SOAP message.

## Using the FC

The type and format of the entries processed and returned by this FC are highly dependent on the specified parameters, as clarified below.

- If the **Input the SOAP Body and Header as FC** parameter is **String** then the SOAP Body is passed in the *"soapBodyString"* Attribute and the SOAP Header is passed in the *"soapHeaderString"* Attribute. If the **Input the SOAP Body and Header as FC** parameter is **DOMELEMENT** then the SOAP Body is passed in the *"soapBodyDOMELEMENT"* Attribute and the SOAP Header is passed in the *"soapHeaderDOMELEMENT"* Attribute.
- If the **Return the SOAP message as FC** parameter is **String** then the complete SOAP message is returned in the *"xmlString"* Attribute; however if it is specified as **DOMELEMENT** then the complete SOAP message is returned in the *"xmlDOMELEMENT"* Attribute.
- Each of the **Add attributes to...** parameters expects a list of XML attributes to be added to the target SOAP message element (envelope, header or body) tag in the created SOAP message. Each attribute-value pair is separated from the other attribute-value pairs by one of the following: a space, a comma, a semicolon, carriage return or a line feed. The attribute name in an attribute-value pair is separated from the attribute value by an equals sign "=".
- Each of the **Namespace declarations to add to...** parameters expects a list of XML namespace declarations to be added to the SOAP message element (envelope, header or body) tag in the created SOAP message. Each namespace prefix-value pair is separated from the other namespace prefix-value pairs by one of the following: a space, a comma, a semicolon, carriage return or a line feed. The namespace prefix in a prefix-value pair is separated from the namespace value by an equals sign "=".

---

# InvokeSoap WS FC

## Introduction

The Axis InvokeSoapWS Function Component (FC) is part of the TDI Web Services suite.

It is used to perform a web service call, given the input message for the call. It has no built-in SOAP parsing functionality and can be used with the “Axis Soap To Java FC” on page 365 and “Axis Java To Soap FC” on page 355 to provide a complete web service solution.

The InvokeSoapWS Function Component requires a complete SOAP request message. When called with a SOAP message the Function Component invokes the remote web service operation with this message. The Function Component returns the SOAP response message. The Function Component, however, does not perform any XML-Java binding (that is, the SOAP response message is not parsed) – the Function Component only returns the SOAP response message.

## Authentication

The InvokeSoapWS FC supports the HTTP basic authentication method. If username and password parameters are filled, then the “authorization” HTTP header field is set with the proper credentials (as specified in the HTTP specification for using HTTP basic authentication). Before sending the username and password, the FC encodes them. The encoding used is Base64 and is done internally by the InvokeSoapWS FC.

## Configuration

### Parameters

#### WSDL URL

The URL of the WSDL document describing the service. This parameter is required; otherwise an exception is thrown on initialization.

#### SOAP Operation

The name of the SOAP operation as described in the WSDL file. This parameter is required; otherwise an exception is thrown on initialization.

#### Provider URL

The URL of the web service provider; substitutes the value in the WSDL; this parameter is provided to allow for dynamic provider switching. If this parameter is **Empty** then the value from the WSDL is used.

#### Login username

The login username sent to the server, using HTTP Basic Authentication. If the server requires authorization it uses this value and the next (Login password) to authenticate the client. The encoding used is Base64 and is done internally by the InvokeSoapWS FC.

#### Login password

The login password sent to the server, using HTTP Basic Authentication. If the server requires authorization it uses this value and the previous (Login username) to authenticate the client.

#### Input the SOAP message as

This drop-down list specifies whether the SOAP request message will be passed to the FC as a string or as a DOM object. This is a required parameter.

#### Return the SOAP message as

This drop-down list specifies whether the SOAP response message should be returned as a string or as a DOM object. This is a required parameter. If the parameter is not specified or has an invalid value, an exception is thrown on initialization. Also, if the SOAP request message does

not conform to the format specified by the this parameter, an error will occur. However, it is ignored when invoking one-way web service operations (see "One-way web service operation support" on page 363.)

#### Detailed Log

When checked, will generate additional log messages.

#### Comment

Your own comments go here.

### Function Component Input

An *Entry*, a `java.lang.String` object, or an `org.w3c.dom.Element` object – contains the complete SOAP request message.

If anything else is passed, an Exception is thrown.

If an *Entry* is passed to the FC and if the value of the **Input the SOAP message as FC** parameter is **String** then the SOAP request message must be stored in the "*xmlString*" Attribute of that *Entry*. If an *Entry* is passed to the FC and if the value of the **Input the SOAP message as FC** parameter is **DOMElement** then the SOAP request message must be stored in the "*xmlDOMElement*" Attribute.

If a non-*Entry* object (either `String` or `Element`) is passed to the FC and if the value of the **Input the SOAP message as FC** parameter is **String** then the SOAP request message must be passed as a `java.lang.String` object. If a non-*Entry* object (either `String` or `Element`) is passed to the FC and if the value of the **Input the SOAP message as FC** parameter is **DOMElement** then the SOAP request message must be passed as an `org.w3c.dom.Element` object.

### Function Component Output

An *Entry* object with 3 attributes – one for the whole SOAP message, one for the SOAP Header and one for the SOAP Body. The SOAP message, Body and Header will be either XML strings or DOM objects, as specified by the **Return the SOAP message as** parameter. Refer to "Using the FC", next.

## Using the FC

This Function Component makes a web service call by sending a SOAP request message and receiving a SOAP response message.

- If an *Entry* was passed to the FC, then if the value of the *Return the SOAP message as FC* parameter is *String* then the SOAP response message is stored in the "*xmlString*" Attribute; however, If the value of the *Return the SOAP message as FC* parameter is *DOMElement* then the SOAP response message is stored in the "*xmlDOMElement*" Attribute.
- Additionally, if this FC was passed an *Entry* object, then the FC stores the SOAP response Header and SOAP response Body (apart from the entire SOAP response message) as Attributes in the returned *Entry*. If the value of the **Output the SOAP message as FC** parameter is **String** then the SOAP Header and Body are stored in the "*soapHeaderString*" and "*soapBodyString*" Attributes respectively as `java.lang.String` objects. If the value of the **Return the SOAP message as FC** parameter is **DOMElement** then the SOAP Header and Body are stored in the "*soapHeaderDOMElement*" and "*soapBodyDOMElement*" Attributes respectively as `org.w3c.dom.Element` objects.
- If a non-*Entry* object was passed to this FC, then the return value of the FC is either a `java.lang.String` object (when the value of the *Return the SOAP message as FC* parameter is *String*) or an `org.w3c.dom.Element` object (when the value is *DOMElement*).
- This FC is capable of sending and receiving SOAP messages encoded using both "literal" encoding and SOAP Section 5 encoding.
- This FC is capable of sending and receiving SOAP messages containing values of complex types which are defined in the <types> section of a WSDL document.



- This FC sets the *"soapAction"* HTTP Header for the SOAP request message to the value specified in the WSDL document (whose location is specified by the *WSDL URL* FC parameter) for the given SOAP operation (whose name is specified by the *SOAP Operation* FC parameter).
- This FC sends the SOAP request message over HTTP to the web service address specified in the *"WSDL URL"* parameter. If the *"WSDL URL"* parameter is missing or empty, the web service address specified in the WSDL document (whose location is specified by the *WSDL URL* FC parameter) for the given SOAP operation (whose name is specified by the *SOAP Operation* FC parameter) is used .
- This FC provides Username and Password parameters. If these parameters are provided, then the FC sets the basic authorization header and sends it to the server. It encodes the supplied username and password using encoding method base64; this is done inside the *InvokeSoapWS* FC

## One-way web service operation support

WSDL 1.1 has four transmission primitives that a web service endpoint can support:

### One-way

The endpoint receives a message.

### Request-response

The endpoint receives a message, and sends a correlated message.

### Solicit-response

The endpoint sends a message, and receives a correlated message.

### Notification

The endpoint sends a message.

WSDL refers to these transmission primitives as operations. (More information on the subject can be found on: [http://www.w3.org/TR/wsdl#\\_porttypes](http://www.w3.org/TR/wsdl#_porttypes).)

The *InvokeSoapWS* Function Component supports only **request-response** and **one-way** web service operations. During the initialization phase, the *InvokeSoapWS* FC reads the configured WSDL document and checks whether the specified SOAP operation is one-way. If the operation is not one-way, it is assumed to be request-response.

The following is a sample WSDL fragment, which describes a request-response operation:

```
<operation name="myRequestResponseOperation">
  <input message="myInputMessage"/>
  <output message="myOutputMessage"/>
</operation>
```

And the following sample WSDL fragment describes a one-way operation:

```
<operation name="myOneWayOperation">
  <input message="myInputMessage"/>
</operation>
```

**Note:** One-way web service operations do not involve a server response – the client sends a request message but the server is not supposed to reply back (not even with a fault message). That is why the *InvokeSoapWS* does not return a response when invoking a one-way SOAP operation: If the ‘perform’ method of the FC is passed an *Entry* argument (for example when the FC is executed as a part of an *AssemblyLine*), the FC returns an **empty Entry**. If the ‘perform’ method of the FC is passed a *java.lang.Object* (for example when the FC is executed by a script), the FC returns **null**.

## See also

“Axis EasyInvoke Soap WS FC” on page 367



---

## Axis Soap To Java FC

The Axis Soap-to-Java Function Component (FC) is part of the TDI Web Services suite.

This component can be used both on the web service client and on the web service server side. This FC uses Axis' mechanism for parsing SOAP response (when on the client) or SOAP request (when on the server) to Java objects - as a complementary component to the AxisJavaToSoap FC. It is given a SOAP response/request message and returns the parsed Java objects either as standalone Java object(s) or encapsulated in an Entry object.

This component supports both RPC and Document style.

## Configuration

### Parameters

#### WSDL URL

The URL of the WSDL document describing the service

#### SOAP Operation

The name of the SOAP operation as described in the WSDL file

#### Input the SOAP message as

This drop-down list specifies whether the SOAP message is specified as a string or as a DOM object.

#### Complex Types

This parameter is optional; if specified, it should be a list of fully qualified Java class names (including the package name), where the different elements (Java classes) of this list are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

**Mode** This required parameter takes either a value of **Request** or **Response**. The value of Specifies whether this FC will parse SOAP request or SOAP response messages.

#### Detailed Log

If checked, will generate additional log messages.

#### Comment

Your own comments go here.

### Function Component Input

*Entry* or *Java Object* representing the complete SOAP message.

If anything else is passed, an Exception is thrown.

### Function Component Output

An *Entry* or a *Java Object* containing the Java representation of the SOAP request/response.

## Using the FC

This Function Component parses a SOAP message and turns it into a Java Object.

- If this FC is passed a SOAP Fault message to parse, this FC returns a Java object of type `org.apache.axis.AxisFault`.
- In case this FC returns an `org.apache.axis.AxisFault` object, the FC stores this object in the `"soapFault"` Attribute if an *Entry* is passed to the FC; and if a *java.lang.Object* was passed then this FC returns the `org.apache.axis.AxisFault` object.
- If the value of the **Input the SOAP message as** FC parameter is **String** then the SOAP message to parse is read from the `"xmlString"` Attribute as a `java.lang.String`, provided an *Entry* is passed to the

FC. If the value of the **Input the SOAP message as** FC parameter is **DOMELEMENT** then the SOAP message to parse is read from the "*xmlDOMELEMENT*" Attribute as an `org.w3c.dom.Element` object, provided an *Entry* is passed to the FC.

- If a *Java Object* is passed to this FC, then the SOAP message to parse is assumed to be the value of the passed Java Object as either a `java.lang.String` object (when the value of the **Input the SOAP message as** FC parameter is **String**) or as an `org.w3c.dom.Element` object (when the value of the **Input the SOAP message as** FC parameter is **DOMELEMENT**).
- This FC is capable of parsing (a) Document style SOAP messages, (b) RPC style SOAP messages and (c) SOAP Fault messages.
- This FC is capable of parsing SOAP messages encoded using both "literal" encoding and SOAP Section 5 encoding.
- This FC is capable of parsing SOAP messages containing values of complex types which are defined in the <types> section of a WSDL document. In order to do that this FC requires that (1) the **Complex Types** FC parameter contains the names all Java classes that implement the complex types used in the SOAP message and (2) these Java classes' class files are located in the Java class path of TDI.
- If an *Entry* is passed to this FC and the message parsed is not a SOAP Fault message, then this FC returns the output parameters in *Entry* Attributes, whose names match the names of the SOAP Operation output parameters.

### See Also

"Custom serializers/deserializers" on page 357

"Axis Java To Soap FC" on page 355

---

## Axis EasyInvoke Soap WS FC

The Axis EasyInvokeSoapWS Function Component (FC) is part of the TDI Web Services suite.

This is a "simplified" web service invocation component: it is a stand-alone FC with its own Config screen, but internally instantiates, configures and uses the following three FCs: AxisJavaToSoap, InvokeSoapWS and AxisSoapToJava.

The functionality provided is the same as if you chain and configure these three FCs in an AssemblyLine. When using this FC you lose the possibility to hook custom processing, that is, you are tied to the processing and binding provided by Axis, but you gain simplicity of setup and use.

### Authentication

The AxisEasyInvokeSoapWS FC uses `org.apache.axis.client.Call`'s authentication mechanism. When username and password parameters of the FC are specified, then they are set to be used by the Call object. This information is sent to the server and if it requires authentication it takes this two parameters for username and password.

### Configuration

#### Parameters

##### WSDL URL

The URL of the WSDL document describing the service. This parameter is required; otherwise an exception is thrown on initialization.

##### SOAP Operation

The name of the SOAP operation as described in the WSDL file. This parameter is required; otherwise an exception is thrown on initialization.

##### Login username

The login username sent to the server, using HTTP Basic authentication. If the server requires authorization it uses this value and the next (Login password) to authenticate the client. The encoding used is Base64 and is done internally by the InvokeSoapWS FC.

##### Login password

The login password sent to the server. If the server requires authorization it uses this value and the previous (Login username) to authenticate the client.

##### Input the SOAP message as

This drop-down list specifies whether the SOAP request message will be passed to the FC as a string or as a DOM object. This parameter is required. If the parameter is not specified or has an invalid value, an exception is thrown on initialization. Also, if the SOAP request message does not conform to the format specified by the this parameter, an error will occur.

##### Complex Types

This parameter is optional; if specified, it should be a list of fully qualified Java class names (including the package name), where the different elements (Java classes) of this list are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

##### Operation Parameters

The list of ordered SOAP operation parameter names. This parameter is required if the SOAP operation has any parameters and the FC is passed an *Entry*; if the SOAP operation has no parameters and the FC is passed an *Entry* then this parameter must be empty. If no *Entry* is passed, the content of the parameter is not relevant.

- If specified, the parameter must contain a list of Attribute names, where different Attribute names are separated by one or more of the following: a comma, a semicolon, a space, a carriage return or a new line.

- Each item from this list is a name of an Attribute, which must be present in the *Entry* passed to the FC. If one of these Attributes is missing, an Exception is thrown.
- The order of the items from the list determines the order in which the Attribute values are passed as parameters to the SOAP operation.

### Detailed Log

Checking this box causes additional log messages to be generated.

### Comment

Your own comments go here.

## Security and Authentication

The AxisEasyInvokeSoapWS FC uses the org.apache.axis.client.Call's authentication mechanism. When the username and password parameters of the FC are filled, then they are set to be used by the Call object. This information is sent to the server and if it requires authentication it takes this two parameters for username and password.

## Function Component Input

*Entry* or a *Java object* representing the web service input data. If anything else is passed, an Exception is thrown.

## Function Component Output

*Entry* or a *Java object* representing the web service output data.

## Using the FC

This Function Component (FC) provides a relatively simple way of invoking SOAP over HTTP web services.

This is how the communication flows:

Web service client <-> AxisEasyInvokeSoapWS FC <-> org.apache.axis.client.Call <-> Web service

The following usability notes apply:

- If this FC is passed a *Java Object* array (*Object[]*) then it passes to the SOAP operation each Java Object from this array in the order in which the Objects are stored in the array. If this FC is passed an *Entry*, then the order and values of the parameters passed to the SOAP operation are determined by the value of the SOAP Operation FC parameter.
- This FC is capable of generating and parsing Document-style SOAP messages and RPC-style SOAP messages as well as parsing SOAP Fault messages. The style of the message generated is determined by the WSDL specified by the WSDL URL FC parameter.
- The FC is capable of generating and parsing SOAP messages encoded using both "literal" encoding and SOAP Section 5 encoding. The encoding of the message generated is determined by the WSDL specified by the WSDL URL FC parameter.
- This FC is capable of generating and parsing SOAP messages containing values of complex types which are defined in the <types> section of a WSDL document. In order to do that this FC requires that (1) the Complex Types FC parameter contains the names all Java classes that implement the complex types used as parameters to the SOAP operation and (2) these Java classes' class files are located in the Java class path of TDI.
- If an *Entry* is passed to this FC and the SOAP response message returned by the server is not a SOAP Fault message and there is a single output parameter of the SOAP Operation, then this FC returns the parameter in the "return" Attribute. (Due to Axis 1.1 specifics, if a SOAP operation has a single output parameter, this parameter is considered the return value of the operation. And if a SOAP operation has several output parameters, its return type is considered to be void.)

- If an *Entry* is passed to this FC and the SOAP response message returned by the server is not a SOAP Fault message and there are several output parameters of the SOAP Operation, then this FC returns the output parameters in *Entry Attributes*, whose names match the names of the SOAP Operation output parameters.
- If an *Object[]* with the input parameters of the SOAP operation is passed to this FC and the SOAP response message returned by the server is not a SOAP Fault message, the result is of type *Object[]*, where the first element is the return value of the SOAP operation (null if the operation is void) and the rest are the output parameters of the operation.
- This FC provides username and password parameters. If these parameters are specified, then the FC sets basic authorization header and sends it to the server. It encodes the supplied username and password. The used encoding method is base64 and is done inside the *InvokeSoapWS FC*.

*Object[]* -> *AxisEasyInvokeSoapWS FC* -> *Object[]*

or

*Entry* -> *AxisEasyInvokeSoapWS FC* -> *Entry*

## See also

“*InvokeSoap WS FC*” on page 361





---

## Complex Types Generator FC

The Complex Types Generator Function Component is part of the TDI Web Services suite.

This Function Component is used for generating a JAR file, which contains the Java class files implementing the complex data types defined in a schema either internal to or referenced by a WSDL. This JAR file can then be used by the other Web Service FCs in order to serialize and parse SOAP messages containing these complex data types.

Please note that this FC is not supposed to be "run" as part of an AssemblyLine for example. Here is the way this FC is supposed to be used:

1. Place it in an AssemblyLine
2. Fill in its parameters
3. Click the "Generate complex types" button to create the JAR file.

After the desired JAR file has been created the FC can be either disabled or deleted altogether from the AssemblyLine – the FC does not provide any runtime functionality whatsoever.

## Configuration

### Parameters

#### WSDL URL

The value of this parameter must be either a valid URL string or a file system path (either absolute or relative) specifying the location of a WSDL file.

#### WSDL2Java Options

The value of this parameter is a command-line-like list of options for the Axis WSDL2Java utility. The FC passes this list of options to the WSDL2Java utility when generating Java source files from WSDL. These options can be used to alter the default behavior of the WSDL2Java utility.

#### JAR file name

The value of this parameter must be the name of the JAR file (either absolute or relative) to be created.

#### JDK Path

The path to a Java Development Kit installation. If left empty the utility assumes that the Java compiler "javac" and the "jar" tools are on the system executable path.

**Note:** The implementation of this FC requires a minimum version 1.4 of the JDK.

#### Generate Java Source Files

If this box is checked (which is the default), then the FC utility generates Java source files from the specified WSDL. If unchecked, then the FC utility skips the generation of Java source files and only performs the compilation and the JAR creation. Setting this parameter to false (that is, unchecked) is useful when you want to write the implementation of the complex types yourself or you want to modify auto-generated Java source files (setting this parameter to true will overwrite any manually edited/written Java source files).

## Function Component Input and Output

You run the FC JAR creation utility by pressing the "Generate complex types" button.

- The Java **source** files are output and then read from "<installation\_folder>/temp/ComplexTypesJavaFiles". If this folder does not exist it is automatically created.
- The Java class files are output and then read from "<installation\_folder>/temp/ComplexTypesClassFiles". If this folder does not exist it is automatically created.

**Note:** Before creating any output files (Java source or class files, the JAR file) the previously generated files are deleted.

## Troubleshooting

If the ComplexTypesGenerator FC displays an error message box and you need further information about the error that has occurred do the following:

1. Change the log level of the *log4j.logger.com.ibm.di.admin* logger in "*<installation\_directory>/log4j.properties*" to DEBUG. For example change the line *log4j.logger.com.ibm.di.admin=WARN* to *log4j.logger.com.ibm.di.admin=DEBUG*.
2. Restart the Config Editor.
3. Run the ComplexTypesGen utility again.

---

## Remote Command Line FC

The Remote Command Line Function Component (Remote CLFC) enables command line system calls to be executed on remote machines. The design and implementation uses the RXA toolkit v2.2 to connect to remote machines, execute the commands and return the results. The returned output can then be parsed to be consumed one value at a time and detect any problems with the executed command.

The Remote CLFC has the ability to connect to remote machines using any of the following protocols: RSH, REXEC, SSH, AS400 or Windows. You can select which of the protocols will be used, however, if left to the default value of 'ANY', the FC will attempt to connect to the remote machine using each of the available protocols one-by-one until a successful connection is made.

You will need to provide information about the remote machine including hostname, username and password. . If the connection is being made using the SSH protocol then you have the option of providing a keystore name and passphrase instead of using a password for authentication.

**Note:** SSH Connections are typically associated with Linux/UNIX and z/OS hosts. However, by installing Cygwin and the Cygwin openssh package on the Windows target machine the SSH protocol can be used with those targets as well. In addition, z/OS targets can be reached using the SSH protocol also.

## Configuration

### Target Machine Hostname

The hostname (address) of the target machine.

### Remote User

The name of a user with Administrative privileges on the target machine.

### Password

The password for the user (specified as **Remote User**) on the target machine. This parameter may be optional in the case of SSH connections using a keystore, as well as for RSH connections.

### Keystore Path

Full path to the file containing the keystore. This parameter is optional, and only used for SSH connections.

### Passphrase

The passphrase that protects your private key, in the keystore specified by the **Keystore Path** parameter above.

### Connection Protocol

Select from 'ANY', 'SSH', 'RSH', 'RExec', 'AS400' and 'WIN'. This designates what protocol to use when connecting to the remote machine. See "Using the FC" on page 375 for more details.

**Port** The port to use to connect to the target machine.

### Command

The command that is to be executed on the target machine. This is overridden if an input attribute 'command.line' has been provided.

### Stdin source file (local)

The path to the file on the local system that is to be used as standard input to the command specified. This parameter is optional.

### Stdin destination directory (remote)

The path to an existing destination directory on the target where you want the standard input file, designated by **Stdin source file (local)**, to be copied. If a value for **Stdin source file (local)** has been provided, but no value for the destination then a random temporary directory will be created on the remote machine. Note that the file is copied temporarily; once the command has finished execution, the copy on the remote machine is deleted.

### Timeout (ms)

The desired CPU timeout period in milliseconds. If the operation does not complete within the specified duration then the operation is cancelled. This parameter is optional. An unspecified or 0 (zero) value indicates Unlimited, that is, no computational time limit.

**Note:** The timeout is a measure of the CPU clock time of the Remote CLFC process, not a measure of the actual time elapsed since process initiation. Commands that are not computationally intensive will not timeout in the specified time if they have not reached their computational time limit.

### Enable SSL for AS400?

This parameter governs whether an SSL connection is enforced on the AS400 (i5/OS) connection. If checked an SSL connection will be attempted to the AS400 target (SSL must be installed and configured on the AS400 target system). The default is unchecked.

### AS400 Proxy Server Name

This parameter defines an AS400 proxy server if so required.

### Run AS400 Program?

An optional Remote CLFC parameter that defines the type of command execution to use for an AS400 (i5/OS) connection. AS400 programs have the extension .PGM. Arguments for these AS400 Programs can be specified using the Entry Attribute **command.args**.

The default value is unchecked.

### Enable RXA Internal Logging?

Enabling this will allow the RXA internal logger to generate log messages in the AssemblyLine log file.

### Detailed Log

Enabling this will generate debug log messages.

## Function Component Input

Some of the parameters configured in the Configuration screen of the Remote CLFC can be provided as Attributes mapped from the work Entry in the Input Map. When present and non-empty, they take precedence over the parameters in the Configuration screen:

### **command.line**

The command that is to be executed on the target machine.

### **command.args**

A multi-valued Attribute whose values each are command line arguments. Required when executing AS400 Programs.

### **command.args.delim**

This Attribute specifies the command/Program argument delimiter. If not specified the default is a single white space character.

### **stdin.source**

This attribute, of type `java.io.String`, represents the path to the file on the local machine that is to be used as standard input for the specified command.

### **stdin.destination**

This attribute, of type `java.io.String`, represents the path where the transferred file should be stored on the remote machine.

In other words, if an attribute called *command.line* is provided in the input entry object then any command that was entered in the Config Editor will be disregarded. This allows you to call the Remote CLFC repeatedly by other components in the AssemblyLine to perform different commands.

## Function Component Output

Once the Remote CLFC has executed the command specified by either the *command.line* attribute or the **Command** configuration parameter as discussed above, the FC makes the following attributes available for attribute mapping:

### **command.returnValue (int)**

The return code that resulted from executing the remote command.

### **command.error (String)**

The standard error message, if any, that was generated when the command was run.

### **command.out (String)**

The standard output message, if any, that was generated when the command was run.

## Using the FC

The Remote CLFC may be used within an AssemblyLine containing other TDI components such as Connectors and other Function Components. To function correctly, you must configure the Remote CLFC correctly using the Config Editor. When it is initialized it will establish a connection with the remote machine and then when its `perform()` method is called (normally when it is reached in the AssemblyLine it is part of), it will execute its command on the target.

Upon completion, the `perform()` method will return an Entry object containing the three output attributes described above: *command.returnValue*, *command.error* and *command.out*. These attributes will then be available to other TDI components further down in the AssemblyLine.

If you use the FC to perform a command that returns a list of messages in Standard Out such as a directory listing then the Remote CLFC would need to be used in conjunction with other TDI components, like a Parser, in order to extract the individual entries from the *command.out* String object and process them one at a time.

## Configuring the Target System

The target machines must satisfy the following requirements:

### Windows Targets

Using the **WIN** protocol: Windows XP targets must have Simple File Sharing disabled for Remote Execution and Access to work. Simple Networking forces all logins to authenticate as "guest". A guest login does not have the authorizations necessary for Remote Execution and Access to function.

To disable Simple File Sharing, you need to start Windows Explorer and click **Tools->Folder Options**. Select the **View** tab, scroll through the list of settings until you find **Use Simple File Sharing**. Remove the check mark next to **Use Simple File Sharing**, then click **Apply** and **OK**.

Windows XP includes a built-in firewall called the Internet Connection Firewall (ICF). By default, ICF is disabled on Windows XP systems, except on Windows XP Service Pack 2 where it is on by default. If either firewall is enabled on a Windows XP target, it will block attempted accesses by Remote Execution and Access. On Service Pack 2, you can select the File and Printer Sharing box in the Exceptions tab of the Windows Firewall configuration to allow access.

The target machine must have remote registry administration enabled (which is the default configuration) in order for Remote Execution and Access to run commands and execute scripts on the target machine.

The default hidden administrative disk shares (such as C\$, D\$, etc) are required for proper operation of Remote Execution and Access.

### Cygwin Targets

Using the **SSH** protocol: To use SSH logins to remote Windows computers, you must download Cygwin from <http://cygwin.com> and install it on each Windows machines that your application will target. Complete documentation for Cygwin is available at <http://cygwin.com>.

To use Remote Execution and Access applications on Cygwin targets, you will need to install up to two additional Cygwin packages that are not part of the default Cygwin installation. From <http://cygwin.com>, download and install openssh, which is in the *net* category of Cygwin packages. openssh contains the ssh daemon that is needed to support SSH logins on Cygwin targets. Another package, cygrunsrv, which is in the *admin* category of packages, provides the ability to run the ssh daemon as a Windows service. If you do not wish to run the ssh daemon as a service, this package is optional.

### UNIX and Linux Targets

Using SSH, RSH or REXEC protocols: The RXA toolkit this FC uses does not supply SSH code for UNIX machines. You must ensure SSH is installed and enabled on any target you want to access using SSH protocol. OpenSSH 3.71, or higher, contains security enhancements not available in earlier releases.

RXA cannot establish connections with any UNIX target that has all remote access protocols (rsh, rexec, or ssh) disabled.

In all UNIX environments except Solaris, the Bourne shell (sh) is used as the target shell in UNIX environments. On Solaris targets, the Korn shell (ksh) is used instead due to problems encountered with sh.

In order for RXA to communicate with Linux and other SSH targets using password authentication, you must edit the file `/etc/ssh/sshd_config` file on target machines and set: `PasswordAuthentication yes` (the default is 'no')

After changing this setting, stop and restart the SSH daemon using the following commands:

```
/etc/init.d/sshd stop  
/etc/init.d/sshd start
```

For further details on how to configure SSH between the local machine and the target, either using password authentication or a keystore, please refer to the relevant OpenSSH documentation at <http://www.openssh.com>.

### z/OS Targets

Using SSH and z/OS, VMS shell commands can be executed on mainframe zSeries systems. Commands executed using this type of connection are very Unix-like as they are run in the simulated Unix shell environment.

**Note:** The target TDI Server you run this on should be in ASCII mode as required by the underlying RXA libraries. Refer to "ASCII Mode" in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide* for more information.

### AS400 Targets

AS400 targets require the IBM Toolbox for Java (V5.2 recommended) to be installed along with a suitable JRE. The IBM Toolbox for Java is also required on the TDI server where the JAR files will be placed in the `<TDI_INSTALL>/jars/3rdParty/IBM` directory. The commands and programs themselves have to be located under the QSYS library on the iSeries system.

When enabling the AS400 SSL connection option, additional configuration is required for self signed certificates. In this case, the signing certificate must be added to the Java Security CA Certificate store (`<jre_directory>/lib/security/cacerts`). Further information can be found here: <http://access1.sun.com/techarticles/Keytool.html>.

## See also

"Command line Connector" on page 26,  
"z/OS TSO/E Command Line FC" on page 377.

---

## z/OS TSO/E Command Line FC

This Function Component addresses the need TDI to be able to issue privileged z/OS commands, including RACF, ACF2 and TopSecret commands.

### Configuration

#### Parameters

The z/OS environment requires a number of parameters for this FC to function properly.

##### Partner TP Name

Specifies the Partner TP Name as specified in the APPC TP Profile. This parameter is required.

##### Destination LU Name

Specifies the destination LU name as specified in the APPC configuration file. If NULL or empty the LU that is defined as default will be used.

##### Source LU Name

Specifies the source LU name as specified in the APPC configuration file. If NULL or empty the LU that is defined as default will be used.

##### APPC mode

Specifies the mode of the APPC conversation. If NULL or empty the default mode as specified in the source LU will be used.

##### User Name

The user under whose identity the conversation will be held.

If NULL or empty, `Security_Type` of the conversation is `ATB_SECURITY_SAME` and the identity under which the IBM Tivoli Directory Integrator is started is used with a default profile.

Otherwise, `Security_Type` of the conversation is `ATB_SECURITY_PROGRAM` and the TSO command will be executed under the identity of the user specified using the profile of that user.

##### User Password

The password of the user under whose identity the conversation will be held; only taken into account when the `User Name` parameter is specified.

If NULL or empty, the conversation will succeed only if the user specified is granted surrogate authorization on the system where the REXX script is deployed.

##### Detailed Log

When checked, generates additional log messages.

##### Comment

Your own comments go here.

### Using the FC

The z/OS TSO Command Line Function Component is able to execute TSO/E shell commands.

This component is only responsible for execution of the command it is passed – it will not construct shell commands and will not understand the business logic associated with the commands it is executing.

The Function Component is given the command line on input and returns the execution status and the output generated by the command. Architecturally this FC consists of a Java layer, a USS shared library and a REXX script component: The Java layer passes the command to the shared library, the shared library passes it to the REXX script through APPC and the REXX script executes the TSO/E command and passes back the result.

Specific business logic of a higher level can be built on top of this Function Component - for example a Connector that manages RACF users. This Connector could construct the correct RACF commands (that correspond to add, modify, etc.) and use internally the FC to execute them.

## Function Component Input

An *Entry* object with an Attribute named *command* whose value is the TSO/E command to be executed.

## Function Component Output

An *Entry* object with the following Attributes:

### **commandOutput**

Contains the output of the TSO/E command execution.

### **tsoCommandReturnCode**

Contains the return code of the TSO/E command.

### **appcReturnCode**

Contains the APPC return code.

## Authentication

The APPC conversation can be performed in two modes: **Security\_Same** and **Security\_Program**.

Whether the conversation will be held in the **Security\_Program** mode depends on whether the **User Name** Function Component parameter contains a non NULL value.

## Authorization

The REXX script is the component that actually executes the TSO command.

TDI will be allowed or disallowed to execute the TSO command depending on the privileges of the user id specified in the z/OS TSO Command Line Function Component configuration.

To minimize the chances that the REXX script ability to execute TSO commands is maliciously exploited, the following optional deployment strategy can be applied:

A specific dataset is created for the REXX script – this dataset will contain the REXX script only and no other members. In RACF the access to the dataset will be limited to only those users that we want to allow to execute that script. The same user(s) will then need to be specified in the z/OS TSO Command Line Function Component configuration.

Other options for restricting the access to the REXX script include limiting the access provided by APPC:

- The Logical Units from which conversation requests will be accepted can be restricted. If for example the REXX script is accessed from the local system, the TP Profile can be put in a LU that is inaccessible for remote calls.
- A limited number of users might be allowed to request a conversation with the TP associated with the REXX script. For example, special users might be created that can access the TP.

## Setting up the native part of the FC

Before using the TSO Command Line Function Component a REXX script must be deployed on a z/OS dataset and APPC configured accordingly:

The z/OS TSO Command Line Function Component contains a REXX script named "TDIEXEC" that executes a TSO/E command and returns the command output.

This REXX script has to be copied to a FB 80 z/OS dataset where it will be invoked from.

The z/OS TSO Command Line Function Component contains a JCL named "TDITP;jcl" that defines the TP Profile data for the REXX script.



You customize the JCL according to the z/OS system environment and execute it.

In detail, in order to deploy the FC you should:

1. Identify (or allocate) PDS datasets where the JCL and REXX script will reside. The JCL and the REXX script can reside in the same or in different datasets.

You can find the "TDITP;jcl" JCL and "TDIEXEC" REXX script in the "tso\_fc" subfolder of the IBM Tivoli Directory Integrator installation folder (only on z/OS).

2. Copy the REXX script and the JCL to the dataset.

For example, this can be done from the TSO shell or menu 6 of ISPF with the following commands:

```
OGGET '<TDI_root>/tso_fc/TDIEXEC' '<TDIEXEC_dataset>(TDIEXEC)'  
OGGET '<TDI_root>/tso_fc/TDITP.jcl' '<TDITP.jcl_dataset>(TDITP)'
```

3. Make sure APPC and ASCH (Transaction Scheduler) are started.

APPC could be started with the following system command:

```
s APPC,SUB=MSTR
```

ASCH could be started with the following system command:

```
s ASCH,SUB=MSTR
```

**Note:** If you want to execute the system commands from ISPF, go to "System Display and Search Facility", Menu "s" and prefix your command with "/", for example:

```
/s APPC,SUB=MSTR
```

4. Customize TDITP;jcl to reflect your environment.

To do so, follow the instructions within the TDITP;jcl JCL. Basically you need to specify the name of the dataset where the TDIEXEC REXX script resides, the APPC TP Profile dataset and the Transaction Scheduler class. The APPC configuration files will give you the necessary information for the APPC TP Profile dataset and the Transaction Scheduler class: by default the APPC and ASCH configuration files are located in the USER.PARMLIB dataset: APPCPM00 for APPC and ASCHPM00 for the Transaction Scheduler.

5. Submit the modified TDITP;jcl.

You can submit it from ISPF by typing "sub" in front of the name of the JCL.

## See also

"z/OS environment Support", in *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.



---

## Chapter 6. SAP R/3 Component Suite

---

### Who should read this chapter

IBM Tivoli Directory Integrator components are designed for network administrators who are responsible for maintaining user directories and other resources. This chapter assumes that you have practical experience installing and using both IBM Tivoli Directory Integrator and SAP R/3, and it describes the procedural steps that are required to achieve integration between IBM Tivoli Directory Integrator and SAP R/3.

This chapter assumes that both IBM Tivoli Directory Integrator and SAP R/3 are installed, configured and running on your network. No details are provided regarding the installation and configuration of these products, except where necessary to achieve integration.

---

### Component Suite Installation

This section describes the software requirements and installation steps for the IBM Tivoli Directory Integrator Component Suite for SAP R/3.

This chapter contains the following sub-sections:

- “Software Requirements”
- “Verifying the Component Suite for SAP R/3” on page 382
- “Checking the Version Numbers” on page 383
- “Uninstallation” on page 383

### Software Requirements

The IBM Tivoli Directory Integrator Component Suite for SAP R/3 is supported on the operating systems platforms that are common for IBM Tivoli Directory Integrator and SAP JCo 2.1.6. Please see the IBM Tivoli Directory Integrator Administrators Guide for supported operating system platforms supported by IBM Tivoli Directory Integrator and please see the SAP website for information about supported platforms for SAP JCo 2.1.6. SAP JCo has other prerequisites, please refer to the SAP Note 684106 for information about other prerequisites.

Installing IBM Tivoli Directory Integrator 6.1.1 also installs the Component Suite. However, to complete the install of the Component Suite, an additional component must be added on the target machine:

- SAP Java Connector (JCo) version 2.1.6

Licensed SAP R/3 customers can download the JCo from the SAP Website. You will require a valid SAP support login account and password, which can be obtained by request from SAP support. SAP R/3 6.20 or 6.40 must also be installed and running on a node within the network environment. TCP/IP network connectivity is required between the SAP R/3 instance and the machine hosting the IBM Tivoli Directory Integrator Component Suite for SAP R/3.

### Configuring the SAP Java Connector

Once downloaded and available on the machine designated to host IBM Tivoli Directory Integrator and the Component Suite for SAP R/3, the JCo can be installed and configured for IBM Tivoli Directory Integrator 6.1.1 as follows:

1. Unzip the JCo distribution package to a directory on the target machine. For example:  
/SapJco216
2. Open the `installation.html` file and follow the installation instructions for your Operating System. For example:

/SapJco216/docs/jco/installation.html

3. Add the following entries to your network service file:

- sapdpNN 32NN/tcp
- sapgwNN 33NN/tcp

- where *NN* is the SAP instance identifier of the SAP R/3 system to which the IBM Tivoli Directory Integrator Component Suite for SAP R/3 will connect.

4. Copy sapjco.jar from the SAP JCo package directory to the *TDI\_HOME*/jars folder.

5. **On Windows machines only**, copy librfc32.dll and sapjcorfc.dll to the *TDI\_HOME*/libs folder.

#### Notes:

1. The network service file can be found at %system\_root%\system32\drivers\etc\services on Windows 32, or /etc/services on UNIX.
2. Before using the IBM Tivoli Directory Integrator Component Suite for SAP R/3, ensure that the sapjco.jar is in the CLASSPATH, and that sapjcorfc.{dll/so} and librfc\*.{dll/so} are in the loadable library path.

## Verifying the Component Suite for SAP R/3

To verify the IBM Tivoli Directory Integrator 6.1.1 Component Suite for SAP R/3:

Table 41 below describes the files and locations installed by the system installer for IBM Tivoli Directory Integrator 6.1.1, with regards to the Components Suite.

Table 41. Installed locations for the IBM Tivoli Directory Integrator Component Suite for SAP R/3

| Filename                                    | Description                      |
|---|----------------------------------|
| TDI_SAPR3Connectors_UserGuide.doc           | <i>TDI_HOME</i> /doc             |
| SapR3BorConnector.jar                       | <i>TDI_HOME</i> /jars/connectors |
| SapR3UserConnector.jar                      | <i>TDI_HOME</i> /jars/connectors |
| SapR3RfcFC.jar                              | <i>TDI_HOME</i> /jars/functions  |
| index.html (Javadoc for all SAP Components) | <i>TDI_HOME</i> /docs/api/       |
| bapi_user_actgroups_assign.xml              | <i>TDI_HOME</i> /xml             |
| bapi_user_actgroups_delete.xml              | <i>TDI_HOME</i> /xml             |
| bapi_user_change.xml                        | <i>TDI_HOME</i> /xml             |
| bapi_user_create.xml                        | <i>TDI_HOME</i> /xml             |
| bapi_user_delete.xml                        | <i>TDI_HOME</i> /xml             |
| bapi_user_getdetail_postcall.xml            | <i>TDI_HOME</i> /xml             |
| bapi_user_getdetail_precall.xml             | <i>TDI_HOME</i> /xml             |
| bapi_user_getlist_postcall.xml              | <i>TDI_HOME</i> /xml             |
| bapi_user_getlist_precall.xml               | <i>TDI_HOME</i> /xml             |
| bapi_user_profiles_assign.xml               | <i>TDI_HOME</i> /xml             |
| bapi_user_profiles_delete.xml               | <i>TDI_HOME</i> /xml             |
| bapi_employee_dequeue.xml                   | <i>TDI_HOME</i> /xml             |
| bapi_employee_enqueue.xml                   | <i>TDI_HOME</i> /xml             |
| bapi_employee_getdata_postcall.xml          | <i>TDI_HOME</i> /xml             |
| bapi_employee_getdata_precall.xml           | <i>TDI_HOME</i> /xml             |
| bapi_persdata_change.xml                    | <i>TDI_HOME</i> /xml             |
| bapi_persdata_create.xml                    | <i>TDI_HOME</i> /xml             |

Table 41. Installed locations for the IBM Tivoli Directory Integrator Component Suite for SAP R/3 (continued)

| Filename                                  | Description          |
|---|----------------------|
| bapi_persdata_delete.xml                  | <i>TDI_HOME</i> /xml |
| bapi_persdata_getdetail_postcall.xml      | <i>TDI_HOME</i> /xml |
| bapi_persdata_getdetail_precall.xml       | <i>TDI_HOME</i> /xml |
| bapi_persdata_getdetailelist_postcall.xml | <i>TDI_HOME</i> /xml |
| bapi_persdata_getdetailelist_precall.xml  | <i>TDI_HOME</i> /xml |

## Checking the Version Numbers

To check the component software version numbers for this integration package:

1. Start IBM Tivoli Directory Integrator and click on **Help**
2. Select **About IBM Tivoli Directory Integrator Components**.
3. Version numbers are displayed for the following components:
  - **ibmdi.SapR3RfcFC**
  - **ibmdi.SapR3UserRegConnector**
  - **ibmdi.SapR3BorConnector**

## Uninstallation

To remove the IBM Tivoli Directory Integrator the Component Suite for SAP R/3 from the target system:

1. Stop IBM Tivoli Directory Integrator assembly lines that are currently running and using one of the IBM Tivoli Directory Integrator Components for SAP R/3.
2. Run the uninstall executable located at *TDI\_HOME*/uninstsap and follow the prompts.
3. Remove the following entries from your network service file (%system\_root%\system32\drivers\etc\services on Windows 32, /etc/services on UNIX):
  - sapdp*NN* 32*NN*/tcp
  - sapgw*NN* 33*NN*/tcp

- where *NN* is the SAP instance identifier of the SAP R/3 system to which the IBM Tivoli Directory Integrator Component Suite for SAP R/3 connects.
4. Remove the SAP JCo (*SAP\_JCO\_HOME*) directory that was created during the installation.
5. Remove the environment variable entries and additions that were created during installation as a result of following the instructions within *SAP\_JCO\_HOME*/docs/jco/installation.html.
6. Remove sapjco.jar from the *TDI\_HOME*/jars folder.
7. **On Windows machines only**, remove the librfc32.dll and sapjcorfc.dll files from the *TDI\_HOME*/libs folder.



---

## Function Component For SAP R/3

This chapter describes the IBM Tivoli Directory Integrator Function Component for SAP R/3.

This chapter includes the following sections:

- “Function Component Introduction”
- “Configuration”
- “Using the Function Component” on page 387

### Function Component Introduction

The Function Component for SAP R/3 6.20 and 6.40 uses SAP JCo 2.1.6 to invoke RFCs on the SAP R/3 System. The Function Component provides a means of calling an arbitrary RFC.

Figure 1 below illustrates the overview architecture of the RFC Function Component.

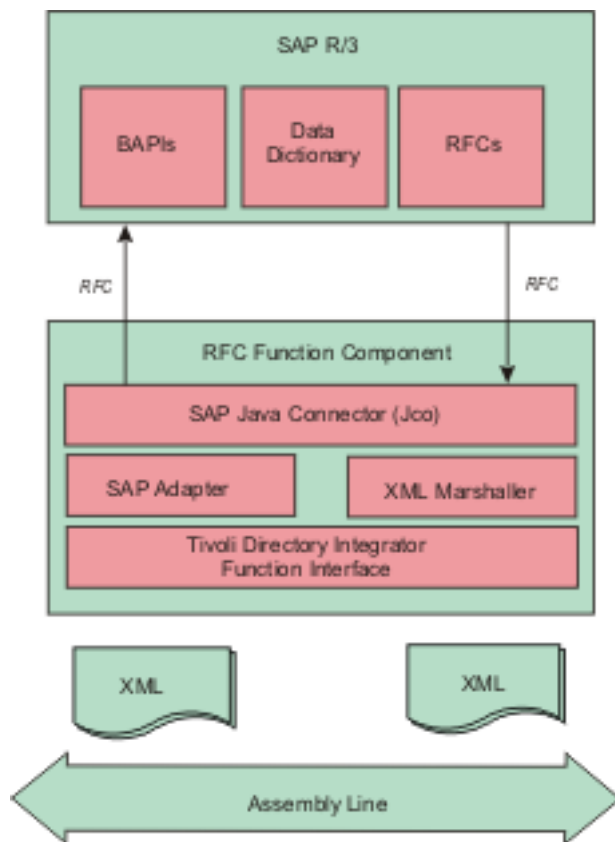


Figure 1. Overview architecture of the RFC Function Component

Before using the Function Component for SAP R/3, the SAP JCo must be downloaded and installed (for details, see “Software Requirements” on page 381).

### Configuration

If the Function Component for SAP R/3 is added directly into an assembly line, the following configuration parameters are available for client connections. The parameters are very similar to the logon parameters for the traditional SAP GUI. Runtime names are shown below in parentheses.

## Parameters

### R3 Client (**client**)

SAP R/3 Logon client for R/3 connection. For example, 100.

### R3 User (**user**)

SAP R/3 Logon user for R/3 connection.

### Password (**passwd**)

SAP R/3 Logon password for R/3 connection.

### R3 System Number (**sysnr**)

The SAP R/3 system number for R/3 connection. For example, 00.

### R3 Hostname (**ashost**)

SAP R/3 application server name for R/3 connection.

### Gateway host (**gwhost**)

Gateway host name for R/3 connection.

### RFC Trace (**trace**)

Set to one (1) to enable RFC API tracing. If enabled, the SAP RFC API will produce separate `rfc_nnnn.trc` files (where `nnnn` represents values assigned by the RFC API) in the working directory IBM Tivoli Directory Integrator. This option may be useful to help diagnose RFC invocation problems. It logs the activity and data between the Connector and SAP R/3. This should be set to zero (0) for production deployment.

Additional configuration parameters are available when using the Function Component programmatically. For more information on the additional parameters, see the `SapR3RfcFC` Java Doc in the distribution package.

## Function Component Input

The `perform()` method accepts an **Entry** object. If anything else is passed an Exception is thrown. The **Entry** object contains two attributes:

- **requestType**
- **request**

The Function Component supports three styles of invocation:

- XML Document,
- XML string, or
- multi-valued attribute.

The value of **requestType** should be set to one of the following, to indicate which style is to be used:

- `xmlDomDocument`
- `xmlString`
- `multiValuedAttributes`

The value of attribute **request** is a type of:

- `org.w3c.dom.Document` if **requesttype** is `xmlDomDocument`,
- `java.lang.String` if **requesttype** is `xmlString`, or
- `com.ibm.di.entry.Attribute` if **requesttype** is `multiValuedAttributes`.

The value of **request** represents the request data of an RFC as one of:

- XML String,
- DOM Document, or
- multi-valued Attribute (please refer to the Javadoc for some sample JavaScript using multi-values attribute invocation).



Any other value will result in an Exception being thrown.

**If request is of type `org.w3c.dom.Document`:**

Its associated value must be an `org.w3c.dom.Document` containing an XSchema that conforms to the specification for ABAP RFC XML serialization.

**If request is of type `java.lang.String`:**

Its associated value must be an XML string. A DOM parser will parse the string value. Its XSchema must also conform to the specification for Serialization of ABAP Data in XML.

**If request is a multi-valued attribute:**

The first value of attribute **request** must be of type `java.lang.String`, containing the name of the RFC, while the second value of the attribute **request** must be `com.ibm.di.entry.Attribute`, whose values contain additional attributes for the SAP RFC parameters as a series of nested and multi-valued attributes representing the names of the import and table parameters of the RFC. The names of the parameters must be encoded according to the rules for Serialization of ABAP Data in XML (names will not have characters that could result in badly-formed XML).

Here is an example of how to invoke the Function Component using the multi-valued attributes style:

```
var rfc = system.newAttribute("BAPI_SALESORDER_GETLIST");
var attr1 = system.newAttribute("CUSTOMER_NUMBER");
attr1.addValue("0000000016");
var attr2 = system.newAttribute("SALES_ORGANIZATION");
attr2.addValue("AU01");
rfc.addValue(attr1);
rfc.addValue(attr2);
var entry = system.newEntry();
var reqAttr = entry.newAttribute("request");
reqAttr.addValue(rfc);
entry.setAttribute("requestType", "multiValuedAttributes");
var result = fc.perform(entry);
```

**Note:** For SAP specifications, see the SAP Web site at <http://ifr.sap.com>.

## Function Component Output

The Function Component output is an **Entry** object with two attributes:

- **responseType**, indicating the response type,
- **response**, with the RFC response as either a DOM Document, an XML string or a nested multi-valued Attribute.

Attribute **responseType** will have a `java.lang.String` value corresponding to the input request type.

**If the Entry contains an attribute **responseType** with value *xmlDomDocument***

The value of attribute **response** is an `org.w3c.dom.Document` containing the RFC response.

**If the Entry contains an attribute **responseType** with value *xmlString***

The value of attribute **response** is an XML `java.lang.String` containing the RFC response.

**If the Entry contains an attribute **responseType** with value *multiValuedAttributes***

The value of attribute **response** is a nested and multi-valued attribute, where the first value is a `java.lang.String`, which has the name of the RFC that was invoked, and the second value contains the results of the RFC as a series of nested multi-valued attributes.

## Using the Function Component

The Function Component invokes the given RFC for a SAP R/3 system.

It can be placed in an assembly line or invoked directly from script. It is the callers' responsibility to check the returned Entry object for any errors that may have resulted from invoking the RFC.

As an example, the following code can be used to invoke an RFC from JavaScript:

```

var counter = 0;
var fc = system.getFunction("ibmdi.SapR3RfcFC");
var myentry;
var docResponse;

fc.setParam(fc.PARAM_CONFIG_CLIENT, "100");
fc.setParam(fc.PARAM_CONFIG_USER, "TIVOLI");
fc.setParam(fc.PARAM_CONFIG_PASSWORD, "*****");
fc.setParam(fc.PARAM_CONFIG_SYSNUMBER, "11");
fc.setParam(fc.PARAM_CONFIG_LANGUAGE, "E");
fc.setParam(fc.PARAM_CONFIG_APPLICATION_SERVER, "kimala");

fc.initialize(null);
var rfc = new java.lang.String("<BAPI_COMPANYCODE_GETLIST/>");
var myentry = system.newEntry();
var attr = myentry.newAttribute(fc.PARAM_INPUT_TYPE);
attr.addValue(fc.PARAM_VAL_STRING);

attr = myentry.newAttribute(fc.PARAM_INPUT);
attr.addValue(rfc);
var myresponse = fc.perform(myentry);

//system.dumpEntry(myresponse);
fc.terminate();

```

**Note:** Configuration parameters must be set before **initialize()** is called, and **terminate()** should be called to cleanup.

## Using the Command Line RFC Invoker

As a tool to assist in creating valid RFC XML requests, a command line utility has been provided. It can be invoked outside of the IBM Tivoli Directory Integrator environment and is able to read an XML file, which represents an RFC XML request to be executed against the SAP R/3 system.

To invoke the utility, add *TDI\_HOME/jars/functions/SapR3RfcFC.jar* to the CLASSPATH environment variable:

```

TDI_HOME/jvm/bin/java com.ibm.di.fc.sapr3rfc.RfcXmlInvoker -f
  [input XML file] -o [output XML file] -p
  [JCO Connection properties file]

```

### Notes:

1. These instructions assume that you have already completed the steps described in "Configuring the SAP Java Connector" on page 381. It is important that the *sapjco.jar* is in the CLASSPATH, and that *sapjcorfc.{dll/so}* and *librfc\*. {dll/so}* are in the loadable library path.
2. For AIX, the path to the Java executable is *TDI\_HOME/jvm/jre/bin/java.exe*

The contents of the JCO Properties file represent the R/3 client connection parameters for the R/3 system. An example of the values in the property file is shown below:

```

jco.client.client=R/3 CLIENT
jco.client.user=R/3 USER NAME
jco.client.passwd=R/3 USER PASSWORD
jco.client.sysnr=R/3 SYSTEM NUMBER
jco.client.ashost=R/3 APPLICATION SERVER HOSTNAME OR IP ADDRESS
jco.client.trace=RFC API TRACE: 1 = ON; 0 = OFF

```

---

## User Registry Connector for SAP R/3

The section describes the configuration and operation of the IBM Tivoli Directory Integrator User Registry Connector for SAP R/3.

This chapter contains the following sections:

- “Introduction”
- “Configuration” on page 390
- “Using the User Registry Connector for SAP R/3” on page 393

### Introduction

This component enables the provisioning and management of SAP R/3 user accounts to external applications (with respect to SAP R/3). The Connector uses the generic RFC invocation feature of the IBM Tivoli Directory Integrator Function Component for SAP R/3 (referred to hereafter as the RFC Function Component). The RFC Function Component enables the Connector to manage SAP user account attributes by executing RFC ABAP code as an external SAP R/3 client application.

The Connector supports an extendable generic framework for provisioning SAP R/3 user accounts and their associated attributes. This is achieved by defining an XML representation of user account information. This XML is then transformed via XSL style sheet transformations (XSLT) into RFC requests. The default functionality of the Connector does not require the deployment of custom RFC ABAP code onto the target R/3 instance.

The key features and benefits of the Connector are:

- Support for Create, Read, Update, and Delete (C.R.U.D) operations for SAP R/3 users.
- Modifiable behavior through XSL transformations for SAP R/3 RFC execution.
- Minimal compile time dependency between the Connector and SAP R/3. The Connector does not use any generated RFC proxy code. It relies on the RFC Function Component as a dynamic proxy.

The Connector supports the following IBM Tivoli Directory Integrator Connector modes:

- Add Only
- Update
- Delete
- Lookup
- Iterator

Figure 2 below illustrates the component design of the SAP R/3 User Registry.

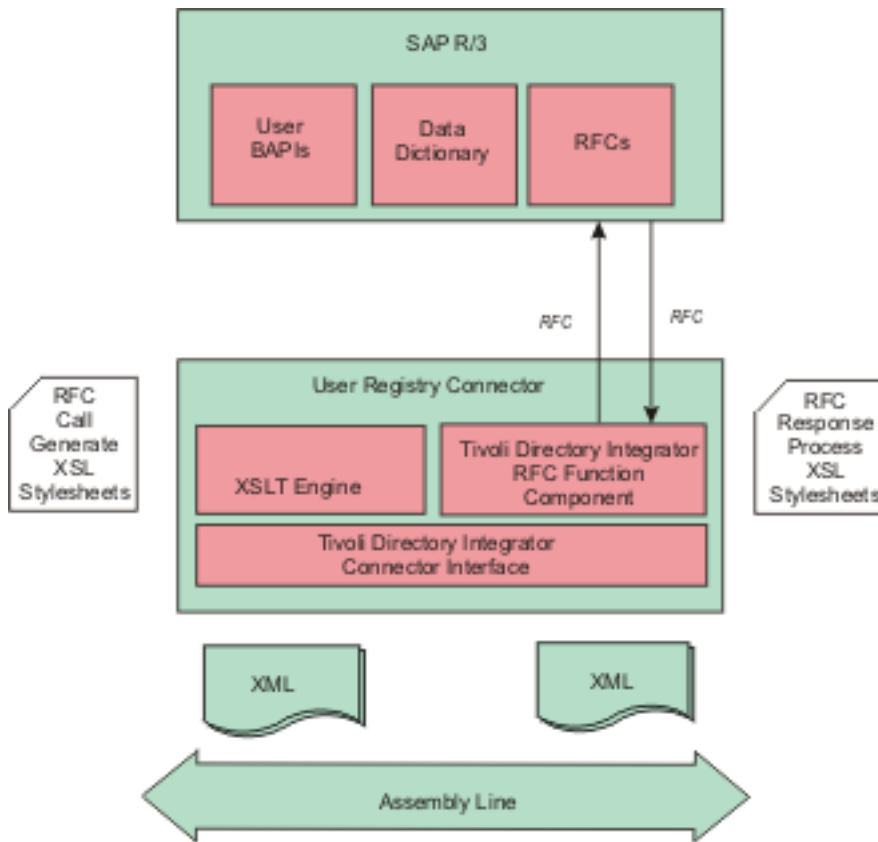


Figure 2. Component design of the SAP R/3 User Registry

## Configuration

The User Registry Connector for SAP R/3 may be added directly into an assembly line. The following section lists the configuration parameters that are available for R/3 client connections and XSL style sheet behavior. The runtime names are shown in parentheses.

### Parameters

#### R3 Client (client)

SAP R/3 Logon client for R/3 connection (for example, 100). This is passed directly to the RFC Function Component.

#### R3 User (user)

SAP R/3 Logon user for R/3 connection. This is passed directly to the RFC Function Component.

#### Password (passwd)

SAP R/3 Logon password for R/3 connection. This is passed directly to the RFC Function Component.

#### R3 System Number (sysnr)

The SAP R/3 system number for R/3 connection (for example, 100). This is passed directly to the RFC Function Component.

#### R3 Hostname (ashost)

SAP R/3 application server name for R/3 connection. This is passed directly to the RFC Function Component.

### Gateway host (gwhost)

Gateway host name for R/3 connection. This is passed directly to the RFC Function Component.

### RFC Trace (trace)

Set to one (1) to enable RFC API tracing. If enabled, the SAP RFC API will produce separate rfc\_nnnn.trc files in the working directory of IBM Tivoli Directory Integrator. This option may be useful to help diagnose RFC invocation problems. It logs the activity and data between the Connector and SAP R/3. This should be set to zero (0) for production deployment.

### Optional RFC Connection Parameters

Used to define a list of other optional RFC connection parameters. The value for this configuration list is a key=value list where each connection parameter is separated by the space character. For example the following string value would set the SAP Gateway Service to "sapgw00" and enable the SAP GUI.

```
"gwserv=sapgw00 use_sapgui=1"
```

Here is a list of optional SAP Java Connector parameters that are accessible.

- Alias user name (alias\_user)
- SAP message server (mshost)
- Gateway service (gwserv)
- Logon language (lang)
- 1 (Enable) or 0 (disable) RFC trace (trace)
- Initial codepage in SAP notation (codepage)
- Secure network connection (SNC) mode, 0 (off) or 1 (on) (snc\_mode)
- SNC partner, e.g. p:CN=R3, O=XYZ-INC, C=EN (snc\_partnername)
- SNC level of security, 1 to 9 (snc\_qop).
- SNC name. Overrides default SNC partner (snc\_myname)
- Path to library which provides SNC service (snc\_lib)
- SAP R/3 name (r3name)
- Group of SAP application servers (group)
- Program ID of external server program (tpname)
- Host of external server program (tphost)
- Type of remote host 2 = R/2, 3 = R/3, E = External (type)
- Enable ABAP debugging 0 or 1 (abap\_debug)
- Use remote SAP graphical user interface (0/1/2) (use\_sapgui)
- Get/Don't get a SSO ticket after logon (1 or 0) (getss2)
- Use the specified SAP Cookie Version 2 as logon ticket (mysaps2)
- Use the specified X509 certificate as logon ticket (x509cert)
- Enable/Disable logon check at open time, 1 (enable) or 0 (disable) (lcheck)
- String defined for SAPLOGON on 32-bit Windows (saplogon\_id)
- Data for external authentication (PAS) (extiddata)
- Type of external authentication (PAS) (extidtype)
- Idle timeout (in seconds) for the connection after which it will be closed by R/3.  
Only positive values are allowed. (idle\_timeout)
- Enable (1) or Disable (0) dsr support (dsr)

### RFC Function Component Name (sapr3.userconn.rfcFC)

The name of the RFC Function Component registered with IBM Tivoli Directory Integrator. This option should be changed only on the advice of IBM support. The default value is:

```
ibmdi.SapR3RfcFC
```

### Add Mode StyleSheets (sapr3.userconn.putStylesheets)

The list of XSLT style sheets files to be executed by the Connector when deployed in **Add Only** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapUserXml**. Each XSL style sheet filename must be entered on a new line within the text box. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_create.xsl, xsl/bapi_user_actgroups_assign.xsl,  
xsl/bapi_user_profiles_assign.xsl
```

#### **Update Mode StyleSheets (sapr3.userconn.modifyStylesheets)**

The list of XSLT style sheets files to be executed by the Connector when deployed in **Update** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapUserXml**. Each XSL style sheet filename must be entered on a new line within the text box. This configuration parameter should be changed only at the direction of IBM support. The default XSL list is:

```
xsl/bapi_user_change.xsl, xsl/bapi_user_actgroups_assign.xsl,  
xsl/bapi_user_profiles_assign.xsl
```

#### **Delete Mode StyleSheets (sapr3.userconn.deleteStylesheets)**

The list of XSLT style sheets files to be executed by the Connector when deployed in **Delete** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapUserXml**. Each XSL style sheet filename must be entered on a new line within the text box. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_delete.xsl
```

#### **Lookup Mode Pre StyleSheet (sapr3.userconn.findPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request that is able to obtain all user attributes for a given user. This configuration value must be set when the Connector is deployed in **Update**, **Delete**, and **Lookup** modes. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getdetail_precall.xsl
```

#### **Lookup Mode Post StyleSheet (sapr3.userconn.findPostStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating the user XML formatted response from the Connector. This configuration value must be set when the Connector is deployed in **Update**, **Delete**, and **Lookup** modes. The XSLT transforms the response XML from the RFC executed as a result of the XSLT from **Lookup Mode Pre StyleSheet** configuration. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getdetail_postcall.xsl
```

#### **Select Entries Pre StyleSheet (sapr3.userconn.selectEntriesPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request that is able to obtain all user names from SAP. This configuration value must be set when the Connector is deployed in **Iterator** mode. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getlist_precall.xsl
```

#### **Select Entries Post StyleSheet (sapr3.userconn.selectEntriesPostStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating the user XML for the **getNextEntry()** processing. This configuration value must be set when the Connector is deployed in **Iterator** mode. The XSLT transforms the response XML from the RFC executed as a result of the XSLT from **Select Entries Pre StyleSheet** configuration. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getlist_postcall.xsl
```

#### **Iterator Mode Pre StyleSheet (sapr3.userconn.getNextPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request that is able to obtain all user attributes for a given user. This configuration value must be set when the Connector is deployed in **Iterator** mode. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getdetail_precall.xsl
```

### Iterator Mode Post StyleSheet (sapr3.userconn.getNextPostStylesheet)

The XSLT style sheet file to be executed by the Connector when creating the user XML formatted response from the Connector. This configuration value must be set when the Connector is deployed in **Iterator** mode. The XSLT transforms the response XML from the RFC executed as a result of the XSLT from **Iterator Mode Pre StyleSheet** configuration. This configuration parameter should be changed only at the direction of IBM support. The default value is:

```
xsl/bapi_user_getdetail_postcall.xsl
```

### Detailed Log

When checked, generates additional log messages. The Connector logs data and activity when this option is enabled.

## Using the User Registry Connector for SAP R/3

This section describes how to use the Connector in each of the IBM Tivoli Directory Integrator Connector modes. The section also describes the IBM Tivoli Directory Integrator Entry schema supported by the Connector.

**Note:** The default XSL style sheet file name values are relative path locations with respect to the IBM Tivoli Directory Integrator AssemblyLine execution directory. In some situations, it may be necessary to prepend the default file name values with the fully qualified installation location of the XSL files. Such modification is likely if the IBM Tivoli Directory Integrator Component Suite for SAP R/3 has been installed in (or if the AssemblyLine is executing from) a directory location separate from the IBM Tivoli Directory Integrator installation.

### IBM Tivoli Directory Integrator Entry Schema

The User Registry Connector supports only two fixed IBM Tivoli Directory Integrator entry attributes. The schema is available through the **discover schema** feature (the torch icon) in the IBM Tivoli Directory Integrator configuration tool. The attribute schema is described below.

Table 42. IBM Tivoli Directory Integrator Schema

| Attribute Name | Type             | Description  |
|----------------|------------------|--|
| sapUserXml     | java.lang.String | <p>A string representing the attributes of an R/3 user. The XSchema is defined in "XSchema for User Registry Connector XML" on page 422.</p> <p>This attribute and value must be present on the <b>Output Map</b> when the Connector is deployed in <b>Add Only</b>, <b>Update</b> and <b>Delete</b> modes.</p> <p>This attribute and value are available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.</p> |
| sapUserName    | java.lang.String | <p>A string representing the name of a given SAP R/3 user. The Connector supports this attribute primarily for configuration of <b>Link Criteria</b>.</p>  |

### Add Only Mode

When deployed in **Add Only** mode, the Connector is able to create a new user in the SAP R/3 database. The Connector should be added to the **Flow** section of a IBM Tivoli Directory Integrator AssemblyLine. The **Output Map** must define a mapping for the **sapUserXml** Connector attribute. The value of this attribute represents the details of the user to be added to SAP. The value will be applied to each configured XSLT file in the order defined. The XSLT transforms produce separate RFC XML requests to be executed by the RFC Function Component, which is managed internally by the Connector.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

## Update Mode

When deployed in **Update** mode, the Connector is able to modify an existing user in the SAP R/3 database. The Connector should be added to the **Flow** section of a IBM Tivoli Directory Integrator AssemblyLine. The **Output Map** must define a mapping for the **sapUserXml** Connector attribute. The value of this attribute represents the details of the user to be changed in SAP. The value will be applied to each configured XSLT file in the order defined. The XSLT transforms produce separate RFC XML requests to be executed by the RFC Function Component, which is managed internally by the Connector.

Additionally, the **sapUserName** attribute should be defined in the **Link Criteria** of the Connector. The **Link Criteria** is required by the AssemblyLine, since the AssemblyLine will invoke the Connectors **findEntry()** method to verify the existence of the given user. The value of **sapUserName**, as defined in the **Link Criteria**, must match the value of the <sapUserName> XML element present in the value of **sapUserXml**. All parameters defined in the **Link Criteria** are passed as XSLT style sheet parameters. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied. The style sheets are not required to use the parameter.

The only operator supported for **Link Criteria** is an **equals exact match**. Wildcard search criteria are not supported, because the RFC lookup method does not currently support wild cards. The Connector will not return duplicate entries.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

**Note:** This mode allows role and profile assignments to be changed. If **sapRoleList** or **sapProfileList** are present in the XML supplied to the Connector, then Connector will perform a complete delete and replace of the current assignments in SAP. This means the supplied XML must contain the complete assignments that need to exist after the operation is executed. This is true also for date ranges associated with roles. If the intention is to change a date range for a role already assigned, and not add or remove existing assignments, the complete list of role assignments with the new date ranges needs to be supplied in the XML. Date ranges should be present with all roles, unless the SAP defaults date values are acceptable.

## Delete Mode

When deployed in **Delete** mode, the Connector is able to delete an existing user from the SAP R/3 database. The Connector should be added to the **Flow** section of a IBM Tivoli Directory Integrator AssemblyLine. The **sapUserName** attribute must be defined in the **Link Criteria** of the Connector. The **Link Criteria** is required by the AssemblyLine, since the AssemblyLine will invoke the Connector's **findEntry()** method to verify the existence of the given user. All parameters defined in the **Link Criteria** are passed as XSLT style sheet parameters. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied. The style sheets are not required to use the parameter.

The only operator supported for **Link Criteria** is an equals exact match. Wildcard search criteria are not supported, because the RFC lookup method does not currently support wild cards.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

## Lookup Mode

When deployed in **Lookup** mode, the Connector is able to obtain all details of a given SAP R/3 user. The Connector should be added to the **Flow** section of a IBM Tivoli Directory Integrator AssemblyLine. The **sapUserName** attribute must be defined in the **Link Criteria** of the Connector. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied. The Connector will populate the XML string value of the attribute **sapUserXml**. This attribute is available to the AssemblyLine in the Connector's **Input Map** .



The Connector's **findEntry()** method is the main code executed. It uses the result of the XSLT transform configured in **Lookup Mode Pre StyleSheet**, to execute an RFC to obtain all details for the given user. The result of the RFC is then transformed using the XSLT transform configured in **Lookup Mode Post StyleSheet**.

The only operator supported for **Link Criteria** is an equals exact match. Wildcard search criteria are not supported, because the RFC lookup method does not currently support wild cards.

The Connector does not support duplicate or multiple entries. The Connector will return only one entry at a time.

## Iterator Mode

When deployed in **Iterator** mode, the Connector is able to retrieve the details of each user in the SAP R/3 database, in turn, and make those details available to the AssemblyLine. The XSLT style sheets for **Select Entries Pre StyleSheet**, **Select Entries Post StyleSheet**, **Iterator Mode Pre StyleSheet**, and **Iterator Mode Post StyleSheet** must be configured.

When deployed in this mode, the IBM Tivoli Directory Integrator AssemblyLine will first call the Connector's **selectEntries()** method to obtain and cache a list of all user names in the SAP R/3 database. The AssemblyLine will then call the Connector's **getNextEntry()** method. This method will maintain a pointer to the current name cached in the list. The method will use this name to call an RFC to obtain all details for the user. The results of the RFC are formatted by an XSLT transform and set as the value of **sapUserXml** and returned by the Connector.

## Transactional Operations Not Supported

Neither the Connector nor IBM Tivoli Directory Integrator currently supports transactions with SAP R/3. Some of the known consequences are explained in this section.

When the Connector is deployed in a mode that results in write operations with SAP (that is, **Add Only**, **Update** and **Delete**) it is possible for operations to be partially complete. This can occur if multiple XSL style sheets, which generate RFC requests, are required to complete the operation. If one of the earlier RFC requests fails, then RFC requests executed subsequently may fail as a result. The Connector attempts to perform all XSL transformations and resulting RFC invocations on a best effort basis.

Consider the **Add Only** case to create a user account in SAP. The first style sheet generates an RFC request for **BAPI\_USER\_CREATE**. The second style sheet generates an RFC request for **BAPI\_USER\_ACTGROUPS\_ASSIGN**. The third style sheet generates an RFC request for **BAPI\_USER\_PROFILES\_ASSIGN**. If the third request fails, then the user may be created without the assignment of profiles.

Another case exists when attempting to create a user that already exists in SAP. The first style sheet results in a call to **BAPI\_USER\_CREATE**. This invocation will result in an ABAP application level error return result (this is not the same as an API or infrastructure error). The Connector will log this. The Connector will then proceed with the subsequent style sheet and RFC invocations, which attempt to assign roles and profiles to the user. Since the user already exists, the role and profile assignments will succeed.

For the case explained above, should the Connector stop processing after the first RFC, or should the Connector continue with the role and profile assignments that the IBM Tivoli Directory Integrator user expected to exist for the newly created user? If the required behavior is to stop after the first RFC error, then an additional configuration of the IBM Tivoli Directory Integrator AssemblyLine can satisfy this requirement. Deploy a second instance of the Connector in **Lookup** mode before the **Add Only** mode instance. The **Lookup** Connector can assist some custom JavaScript code to conditionally terminate or continue the AssemblyLine, depending on the existence of the user to be created.

## Handling ABAP Errors

The Connector invokes BAPI/RFC functions in SAP to perform the Connector mode operations. In some cases, data passed to the BAPI/RFC functions from the XML input, may result in ABAP data validation failures. An example of this case could be the value for post code is not valid within the country region. The BAPI/RFC functions return the results of validation checks in the RETURN parameter of the RFC.

The Connector has been designed to make the RFC return status available to the AssemblyLine. The Connector does not interpret or translate ABAP errors or warnings into thrown exceptions. The Connector registers a script bean named **urcAbapErrorCache**. The bean is registered for all Connector modes and can be accessed in Connector hooks. The bean is an instance of **AbapErrorCache**. Script code in a Connector hook can use this information to perform contingency actions as required. The cache is reset before the execution of each Connector method.

Example script code is shown below. For specific details, refer to the Javadoc contained in the distribution package.

```
var errs = urcAbapErrorCache.getLastErrorSet();
if (errs.size() > 0) {
    task.logmsg("***** There were ABAP Errors *****");
    for (var i = 0; i < errs.size(); ++i) {
        var errInfo = errs.get(i);
        task.logmsg("The message is: " + errInfo.getMsg());
        task.logmsg("The message number is: " + errInfo.getMsgNum().toString());
    }
}

var warns = urcAbapErrorCache.getLastWarningSet();
if (warns.size() > 0) {
    task.logmsg("***** There were ABAP Warnings *****");
    for (var i = 0; i < warns.size(); ++i) {
        var errInfo = warns.get(i);
        task.logmsg("The message is: " + errInfo.getMsg());
        task.logmsg("The message number is: " + errInfo.getMsgNum().toString());
    }
}
```

---

## Human Resources/Business Object Repository Connector for SAP R/3

This section describes the configuration and operation of the IBM Tivoli Directory Integrator Human Resources/Business Object Repository Connector for SAP R/3.

This chapter contains the following sections:

- “Introduction”
- “Configuration” on page 399
- “Using the Human Resources Connector for SAP R/3” on page 402

### Introduction

The SAP Human Resources modules include a large range of business features. The major feature areas address the business needs of payroll, personnel time management, and general personnel master data management.

From a data perspective, the backbone of the SAP HR system is the *infotype*. Infotypes are a logical grouping of related attributes. SAP defines a large set of default infotypes, which are grouped and identified in SAP using number ranges. The table below shows the ranges:

*Table 43. Infotype Number Ranges*

| Number Range | HR Submodule       |
|--------------|--------------------|
| 0000 to 0999 | HR Master Data     |
| 1000 to 1999 | Personnel Planning |
| 2000 to 2999 | Time Management    |
| 4000 to 4999 | Recruitment        |
| 9000 to 9999 | Custom extensions  |

Since there are such a large number of infotypes, it is quite difficult to design a single Tivoli Directory Integrator Connector to cover and suit all SAP HR integration requirements. Fortunately, SAP supports access to its HR data repositories via Business APIs (BAPI) that are attached to objects in the Business Object Repository (BOR). As a result, a generic BOR Connector has been designed and implemented. This Connector can invoke any method of any BOR object. The Connector projects an XML representation of the data managed by the given BOR object. The Connector requires the configuration of a set of XSL style sheets, and specification of the class identification name for the given BOR object (in fact, the XSL style sheets define the XML data representation).

The figure below illustrates the component design of the Connector.

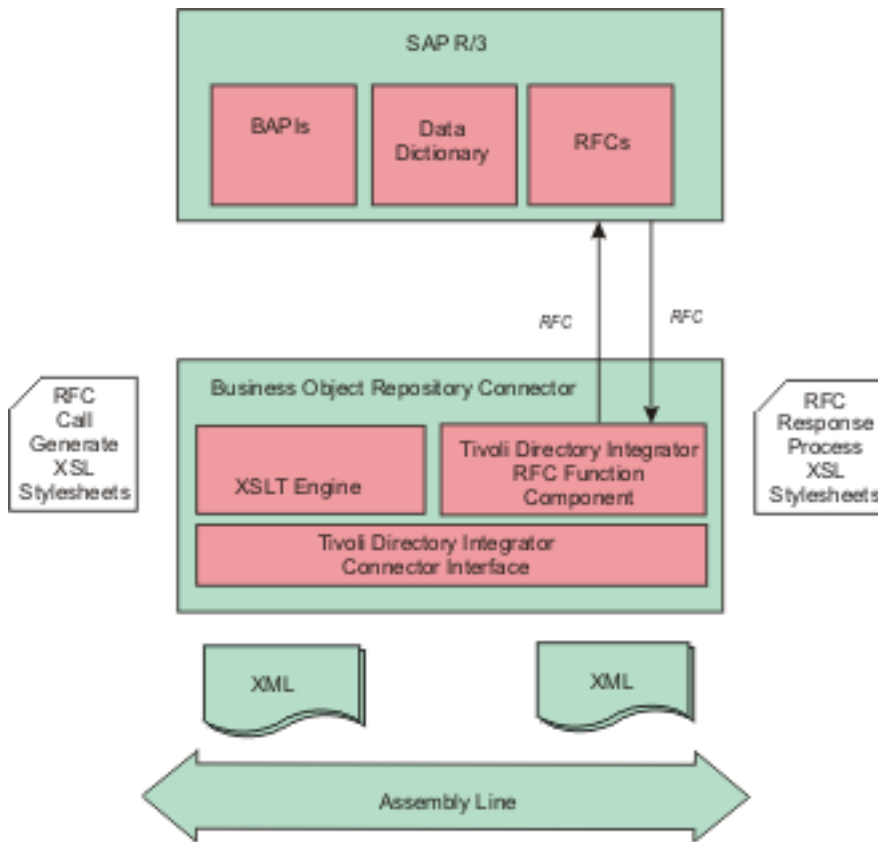


Figure 3. Component design of the Human Resources/Business Object Repository Connector for SAP R/3

The integration distribution package supplies an example set of XSL style sheets that enable the Connector to manage HR Personal Data (Infotype 0002). The style sheets have been setup to invoke the BAPI RFC methods of the PERSDATA BOR object. The Connector uses the generic RFC invocation feature of the Tivoli Directory Integrator Function Component for SAP R/3.

The key features and benefits of the Connector are:

- Support for Create, Read, Update, and Delete (C.R.U.D) operations for SAP R/3 HR data.
- Modifiable behavior through XSL transformations for SAP R/3 RFC execution.
- Minimal compile time dependency between the Connector and SAP R/3. The Connector does not use any generated RFC proxy code. It relies on the RFC Function Component as a dynamic proxy.
- No need for custom ABAP or Java coding (although specific new features might be supported with custom code).

The Connector supports the following standard Tivoli Directory Integrator Connector modes, but relies on the standard BAPI methods to deliver the functionality of each mode:

- Add Only
- Update
- Delete
- Lookup
- Iterator

The table below gives an example of Connector mode to BAPI method mappings

Table 44. Example Mappings

| Connector Mode | BAPI Method                   |
|----------------|-------------------------------|
| Add            | Create, CreateFromData        |
| Update         | Change                        |
| Delete         | Delete                        |
| Lookup         | Get, GetDetail                |
| Iterator       | GetList, Get, GetDetailedList |

## Key Fields and XML Representation

Key fields of BOR objects are given special treatment by the Connector. This is reflected in the XML representation of BOR object data.

While it is possible to define alternate XSL style sheets to process request and response XML, the style sheets must support an element named **sapBorObjIdentifier**. This element is processed by the Java code of the Connector when returning entries in **Lookup** and **Iterator** modes. The **sapBorObjIdentifier** may appear anywhere within the XML. The contents of the element are elements whose tag names match the names of the key fields of the given BOR object.

The general form of the HR Personal Data XML is shown below.

```
<sapPersonalData>
  <sapBorObjIdentifier>
    <EmployeeNumber>00000001</EmployeeNumber>
    <SubType />
    <ObjectID />
    <LockIndicator />
    <ValidityEnd>99991231</ValidityEnd>
    <ValidityBegin>19740320</ValidityBegin>
    <RecordNumber>000</RecordNumber>
  </sapBorObjIdentifier>
  <personalDataDetail>
    <title>1</title>
    <firstname></firstname>
    <lastname></lastname>
    <nameAtBirth />
    <knownAs></knownAs>
    <surnamePrefix />
    <gender></gender>
    <dateOfBirth></dateOfBirth>
    <birthPlace />
    <stateOfBirth />
    <countryOfBirth />
    <maritalStatus></maritalStatus>
    <numberOfChildren></numberOfChildren>
    <religion />
    <language></language>
    <languageCode></languageCode>
    <nationality></nationality>
    <idNumber />
  </personalDataDetail>
</sapPersonalData>
```

## Configuration

The BOR Connector for SAP R/3 may be added directly into an assembly line. The following section lists the configuration parameters that are available for R/3 client connections and XSL style sheet behavior. Runtime names are shown in parentheses.

## Parameters

### R3 Client (client)

SAP R/3 Logon client for R/3 connection (for example, 100). This is passed directly to the RFC Function Component.

### R3 User (user)

SAP R/3 Logon user for R/3 connection. This is passed directly to the RFC Function Component.

### Password (passwd)

SAP R/3 Logon password for R/3 connection. This is passed directly to the RFC Function Component.

### R3 System Number (sysnr)

The SAP R/3 system number for R/3 connection (for example, 100). This is passed directly to the RFC Function Component.

### R3 Hostname (ashost)

SAP R/3 application server name for R/3 connection. This is passed directly to the RFC Function Component.

### Gateway host (gwhost)

Gateway host name for R/3 connection. This is passed directly to the RFC Function Component.

### RFC Trace (trace)

Set to one (1) to enable RFC API tracing. If enabled, the SAP RFC API will produce separate rfc\_nnnn.trc files in the working directory of Tivoli Directory Integrator. This option may be useful to help diagnose RFC invocation problems. It logs the activity and data between the Connector and SAP R/3. This should be set to zero (0) for production deployment.

### Optional RFC Connection Parameters

Used to define a list of other optional RFC connection parameters. The value for this configuration list is a key=value list where each connection parameter is separated by the space character. For example the following string value would set the SAP Gateway Service to "sapgw00" and enable the SAP GUI.

```
"gwserv=sapgw00 use_sapgui=1"
```

Here is a list of optional SAP Java Connector parameters that are accessible.

Alias user name (alias\_user)

SAP message server (mshost)

Gateway service (gwserv)

Logon language (lang)

1 (Enable) or 0 (disable) RFC trace (trace)

Initial codepage in SAP notation (codepage)

Secure network connection (SNC) mode, 0 (off) or 1 (on) (snc\_mode)

SNC partner, e.g. p:CN=R3, O=XYZ-INC, C=EN (snc\_partnername)

SNC level of security, 1 to 9 (snc\_qop).

SNC name. Overrides default SNC partner (snc\_myname)

Path to library which provides SNC service (snc\_lib)

SAP R/3 name (r3name)

Group of SAP application servers (group)

Program ID of external server program (tpname)

Host of external server program (tphost)

Type of remote host 2 = R/2, 3 = R/3, E = External (type)

Enable ABAP debugging 0 or 1 (abap\_debug)

Use remote SAP graphical user interface (0/1/2) (use\_sapgui)

Get/Don't get a SSO ticket after logon (1 or 0) (getsso2)

Use the specified SAP Cookie Version 2 as logon ticket (mysapsso2)

Use the specified X509 certificate as logon ticket (x509cert)

Enable/Disable logon check at open time, 1 (enable) or 0 (disable) (lcheck)  
String defined for SAPLOGON on 32-bit Windows (saplogon\_id)  
Data for external authentication (PAS) (extiddata)  
Type of external authentication (PAS) (extidtype)  
Idle timeout (in seconds) for the connection after which it will be closed by R/3.  
Only positive values are allowed. (idle\_timeout)  
Enable (1) or Disable (0) dsr support (dsr)

**BOR Class Name (sapr3.conn.borObjName)**

The name of the BOR class with which this Connector will be integrating. The names of BOR classes are available using transaction BAPI in SAP R/3. This value is used to obtain the keyfield names of the BOR object when a schema query is performed.

**RFC Function Component Name (sapr3.conn.rfcFC)**

The name of the RFC Function Component that is registered with Tivoli Directory Integrator. This option should be changed only on the advice of IBM support. The default value is:

ibmdi.SapR3rfcFC

**Add Mode StyleSheets (sapr3.conn.putStylesheets)**

The list of XSLT style sheets files to be executed by the Connector when deployed in **Add Only** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapXml**. Each XSL style sheet filename must be entered on a new line within the text box.

**Update Mode StyleSheets (sapr3.conn.modifyStylesheets)**

The list of XSLT style sheets files to be executed by the Connector when deployed in **Update** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapXml**. Each XSL style sheet filename must be entered on a new line within the text box.

**Delete Mode StyleSheets (sapr3.conn.deleteStylesheets)**

The list of XSLT style sheets files to be executed by the Connector when deployed in **Delete** mode. At runtime, each style sheet is applied to the XML contained within the Container Entry. The XSL will be applied to the value of the attribute named **sapXml**. Each XSL style sheet filename must be entered on a new line within the text box.

**Lookup Mode Pre StyleSheet (sapr3.conn.findPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request that is able to obtain all user attributes for a given user. This configuration value must be set when the Connector is deployed in **Update**, **Delete**, and **Lookup** modes.

**Lookup Mode Post StyleSheet (sapr3.conn.findPostStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating the user XML formatted response from the Connector. This configuration value must be set when the Connector is deployed in **Update**, **Delete**, and **Lookup** modes. The XSLT transforms the response XML from the RFC executed as a result of the XSLT from **Lookup Mode Pre StyleSheet** configuration.

**Select Entries Pre StyleSheet (sapr3.conn.selectEntriesPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request that is able to obtain all user names from SAP. This configuration value must be set when the Connector is deployed in **Iterator** mode.

**Select Entries Post StyleSheet (sapr3.conn.selectEntriesPostStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating the user XML for the **getNextEntry()** processing. This configuration value must be set when the Connector is deployed in **Iterator** mode. The XSLT transforms the response XML from the RFC executed as a result of the XSLT from **Select Entries Pre StyleSheet** configuration.

**Iterator Mode Pre StyleSheet (sapr3.conn.getNextPreStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating an RFC XML request

that is able to obtain all user attributes for a given user. This configuration value must be set when the Connector is deployed in **Iterator** mode.

#### **Iterator Mode Post StyleSheet (sapr3.conn.getNextPostStylesheet)**

The XSLT style sheet file to be executed by the Connector when creating the user XML formatted response from the Connector. This configuration value must be set when the Connector is deployed in **Iterator** mode. The XSLT transforms the response XML from the RFC that is executed as a result of the XSLT from **Iterator Mode Pre StyleSheet** configuration.

#### **Detailed Log**

When checked, generates additional log messages. The Connector logs data and activity when this option is enabled.

## **Using the Human Resources Connector for SAP R/3**

This section describes the details of using the Connector in each of the supported Tivoli Directory Integrator Connector modes. The section also describes the Tivoli Directory Integrator Entry schema supported by the Connector.

**Note:** The default XSL style sheet file name values are relative path locations with respect to the Tivoli Directory Integrator AssemblyLine execution directory. In some situations, it may be necessary to prepend the default file name values with the fully qualified installation location of the XSL files. Such modification is likely if the Tivoli Directory Integrator Component Suite for SAP R/3 has been installed in (or if the AssemblyLine is executing from) a directory location separate from the Tivoli Directory Integrator installation.

### **IBM Tivoli Directory Integrator Entry Schema**

The BOR Connector supports one native attribute named **sapXml**. The value of **sapXml** is an XML string representing the attributes of a BOR object. Other attributes reflect the given BOR object key field names. They are supported to allow the definition of IBM Tivoli Directory Integrator **Link Criteria** when the Connector is deployed in **Lookup**, **Delete**, or **Update** modes.

The schema is available via the query schema feature in the IBM Tivoli Directory Integrator configuration tool. The attribute schema is described below.

*Table 45. Entry Schema Attributes*

| Attribute Name | Type             | Description   |
|----------------|------------------|---|
| sapXml         | java.lang.String | A string representing the attributes of an R/3 BOR Object. This attribute and value must be present on the <b>Output Map</b> when the Connector is deployed in <b>Add Only</b> and <b>Update</b> modes. This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.                                    |
| EmployeeNumber | java.lang.String | Personal Data Infotype 0002 specific. The 8 digit employee number. This attribute and value must be present on the <b>Link Criteria</b> when the Connector is deployed in <b>Lookup</b> , <b>Update</b> and <b>Delete</b> modes. This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.           |
| Subtype        | java.lang.String | Personal Data Infotype 0002 specific. The 4 character personal data subtype. This attribute and value must be present on the <b>Link Criteria</b> when the Connector is deployed in <b>Lookup</b> , <b>Update</b> and <b>Delete</b> modes. This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes. |



Table 45. Entry Schema Attributes (continued)

| Attribute Name | Type             | Description  |
|----------------|------------------|--|
| ObjectID       | java.lang.String | Personal Data Infotype 0002 specific.<br>The 2 character object ID for infotypes where all other key fields are the same.<br>This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.  |
| LockIndicator  | java.lang.String | Personal Data Infotype 0002 specific.<br>The 1 character flag indicating if the master data record is locked in SAP.<br>This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.   |
| ValidityEnd    | java.lang.String | Personal Data Infotype 0002 specific.<br>8 digit date value (YYYYMMDD).<br>This attribute and value must be present on the <b>Link Criteria</b> when the Connector is deployed in <b>Lookup</b> , <b>Update</b> and <b>Delete</b> modes.<br>This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes. |
| ValidityBegin  | java.lang.String | Personal Data Infotype 0002 specific.<br>8 digit date value (YYYYMMDD).<br>This attribute and value must be present on the <b>Link Criteria</b> when the Connector is deployed in <b>Lookup</b> , <b>Update</b> and <b>Delete</b> modes.<br>This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes. |
| RecordNumber   | java.lang.String | Personal Data Infotype 0002 specific.<br>2 digit value.<br>This attribute is available on the <b>Input Map</b> when the Connector is deployed in <b>Lookup</b> and <b>Iterator</b> modes.  |

## Add Only Mode

When deployed in **Add Only** mode, the Connector is able to create a new object in the SAP R/3 database. The Connector should be added to the **Flow** section of a Tivoli Directory Integrator AssemblyLine. The **Output Map** must define a mapping for the **sapXml** Connector attribute. The value of this attribute represents the details of the object to be added to SAP. The value will be applied to each configured XSLT file in the order defined. The XSLT transforms produce separate RFC XML requests to be executed by the RFC Function Component, which is managed internally by the Connector.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

For HR Personal Data (infotype 0002), a valid employee number must exist. The general form of the XML is shown below. The mandatory elements are **EmployeeNumber**, **ValidityBegin**, and **ValidityEnd**.

```
<sapPersonalData>
  <sapBorObjIdentifier>
    <EmployeeNumber>00000001</EmployeeNumber>
    <SubType />
    <ObjectID />
    <LockIndicator />
    <ValidityEnd>99991231</ValidityEnd>
    <ValidityBegin>19740320</ValidityBegin>
    <RecordNumber>000</RecordNumber>
  </sapBorObjIdentifier>
  <personalDataDetail>
    <title></title>
    <firstname></firstname>
```

```

<lastname></lastname>
<nameAtBirth />
<knownAs>Torpedo</knownAs>
<surnamePrefix />
<gender>1</gender>
<dateOfBirth></dateOfBirth>
<birthPlace />
<stateOfBirth />
<countryOfBirth />
<maritalStatus></maritalStatus>
<numberOfChildren></numberOfChildren>
<religion />
<language></language>
<languageCode></languageCode>
<nationality></nationality>
<idNumber />
</personalDataDetail>
</sapPersonalData>

```

## Update Mode

When deployed in **Update** mode, the Connector is able to modify an existing object in the SAP R/3 database. The Connector should be added to the **Flow** section of a Tivoli Directory Integrator AssemblyLine. The **Output Map** must define a mapping for the **sapXml** Connector attribute. The value of this attribute represents the details of the user to be changed in SAP. The value will be applied to each configured XSLT file in the order defined. The XSLT transforms produce separate RFC XML requests to be executed by the RFC Function Component, which is managed internally by the Connector.

Additionally, some of the key fields of the BOR object are needed for the **Link Criteria** of the Connector. The **Link Criteria** is required by the AssemblyLine, since the AssemblyLine will invoke the Connector's **findEntry()** method to verify the existence of the given object. All parameters defined in the **Link Criteria** are passed as XSLT style sheet parameters. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

For HR Personal Data (infotype 0002), the following attributes must be defined in the **Link Criteria**:

- EmployeeNumber,
- ValidityBegin,
- ValidityEnd.

Since these attributes are passed as parameters to the XSL style sheets, they are not required in the XML. The general form of the XML is shown below.

```

<sapPersonalData>
  <sapBorObjIdentifier>
    <SubType />
    <ObjectID />
    <LockIndicator />
    <RecordNumber>000</RecordNumber>
  </sapBorObjIdentifier>
  <personalDataDetail>
    <title></title>
    <firstname></firstname>
    <lastname></lastname>
    <nameAtBirth />
    <knownAs>Torpedo</knownAs>
    <surnamePrefix />
    <gender></gender>
    <dateOfBirth></dateOfBirth>
    <birthPlace />
    <stateOfBirth />
    <countryOfBirth />
  </personalDataDetail>
</sapPersonalData>

```

```

<maritalStatus></maritalStatus>
<numberOfChildren></numberOfChildren>
<religion />
<language></language>
<languageCode></languageCode>
<nationality></nationality>
<idNumber />
</personalDataDetail>
</sapPersonalData>

```

## Delete Mode

When deployed in **Delete** mode, the Connector is able to delete an existing object from the SAP R/3 database. The Connector should be added to the **Flow** section of a Tivoli Directory Integrator AssemblyLine. In **Delete** mode, the Connector relies solely on the **Link Criteria**. All parameters defined in the **Link Criteria** are passed as XSLT style sheet parameters. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied.

The Connector does not support duplicate or multiple entries. Only one entry should be supplied to the Connector at a time.

For HR Personal Data (infotype 0002), the following Attributes must be defined in the **Link Criteria**:

- EmployeeNumber,
- ValidityBegin,
- ValidityEnd.

## Lookup Mode

When deployed in **Lookup** mode, the Connector is able to obtain all details of a given SAP R/3 object. The Connector should be added to the **Flow** section of a Tivoli Directory Integrator AssemblyLine. Connector key field attributes should be defined in the **Link Criteria** of the Connector. If duplicate **Link Criteria** names are supplied, the Connector will use the last value supplied. The Connector will populate the XML string value of the attribute **sapXml** and make it available to the AssemblyLine in the Connector's **Input Map**. The key field names and values are also made available to the **Input Map**.

The Connector's **findEntry()** method is the main code executed. It uses the result of the XSLT transform configured in **Lookup Mode Pre StyleSheet** to execute an RFC and obtain all details for the given user. The result of the RFC is then transformed using the XSLT transform configured in **Lookup Mode Post StyleSheet**.

The Connector does not support duplicate or multiple entries. The Connector will return only entry at a time.

For HR Personal Data (infotype 0002), the following Attributes must be defined in the **Link Criteria**:

- EmployeeNumber,
- ValidityBegin,
- ValidityEnd.

## Iterator Mode

When deployed in **Iterator** mode, the Connector is able to retrieve the details of each object in the SAP R/3 database, in turn, and make those details available to the AssemblyLine. The XSLT style sheets for **Select Entries Pre StyleSheet**, **Select Entries Post StyleSheet**, **Iterator Mode Pre StyleSheet**, and **Iterator Mode Post StyleSheet** must be configured.

When deployed in this mode, the Tivoli Directory Integrator AssemblyLine will first call the Connector's **selectEntries()** method to obtain and cache a list of all key field names and values (for the given BOR object) in the SAP R/3 database. The AssemblyLine will then call the Connector's **getNextEntry()** method. This method will maintain a pointer to the current key field cached in the list. The method will use the

key field information to call an RFC to obtain all details for the object. The result of the RFC are formatted by an XSLT transform and set as the value of `sapXml` and returned by the Connector. The key field names and values are also made available to the **Input Map**.

## Transactional Operations Not Supported

When the Connector is deployed in a mode that results in write operations with SAP (**Add Only**, **Update**, **Delete**), it is possible for operations to be partially complete. This can occur if multiple XSL style sheets, which generate RFC requests, are required to complete the operation. If one of the earlier RFC requests fails, then RFC requests executed subsequently may fail as a result.

## Handling ABAP Errors

The Connector invokes BAPI/RFC functions in SAP to perform the Connector mode operations. In some cases, data passed to the BAPI/RFC functions from the XML input, may result in ABAP data validation failures. The BAPI/RFC functions return the results of validation checks in the "RETURN" parameter of the RFC.

The Connector has been designed to make the RFC return status available to the `AssemblyLine`. The Connector does not interpret or translate ABAP errors or warnings into thrown exceptions. The Connector registers a script bean named `borcAbapErrorCache`. The bean is registered for all Connector modes and can be accessed in Connector hooks. The bean is an instance of `AbapErrorCache`. Script code in a Connector hook can use this information to perform contingency actions as required. The cache is reset before the execution of each Connector method.

Example script code is shown below. For specific details, refer to the Javadoc contained in the distribution package.

```
var errs = borcAbapErrorCache.getLastErrorSet();
if (errs.size() > 0) {
    task.logmsg("***** There were ABAP Errors *****");
    for (var i = 0; i < errs.size(); ++i) {
        var errInfo = errs.get(i);
        task.logmsg("The message is: " + errInfo.getMsg());
        task.logmsg("The message number is: " + errInfo.getMsgNum().toString());
    }
}

var warns = borcAbapErrorCache.getLastWarningSet();
if (warns.size() > 0) {
    task.logmsg("***** There were ABAP Warnings *****");
    for (var i = 0; i < warns.size(); ++i) {
        var errInfo = warns.get(i);
        task.logmsg("The message is: " + errInfo.getMsg());
        task.logmsg("The message number is: " + errInfo.getMsgNum().toString());
    }
}
```

---

## ALE Intermediate Document (IDOC) Connector for SAP R/3 and SAP ERP

This section describes the configuration and operation of the IBM Tivoli Directory Integrator Connector for processing ALE IDOCs sent from an SAP R/3 or ERP system. The chapter contains the following sections:

- “Introduction”
- “Configuration” on page 408
- “Using the SAP ALE IDOC Connector” on page 410

### Introduction

In an SAP System the Application Link Enabling (ALE) is one of the core integration technologies. It involves the exchange of hierarchical data documents known as Intermediate Documents (IDOCs). There are two scenarios, inbound to SAP, and outbound from SAP. This release of the connector only integrates with IDOCs that are outbound from SAP, and inbound to IBM Tivoli Directory Integrator. This document will use the term inbound with reference to inbound to IBM Tivoli Directory Integrator. The SAP System will always be the IDOC client with IBM Tivoli Directory Integrator acting as the IDOC Server. The IDOC is sent to IBM Tivoli Directory Integrator as an asynchronous event, and when received, IBM Tivoli Directory Integrator pushes the IDOC data onto an AssemblyLine for processing as desired. As it is asynchronous communication, IBM Tivoli Directory Integrator will not provide a response to the client SAP system. SAP TID management is used to ensure data consistency between the SAP system client and IBM Tivoli Directory Integrator. Due to the asynchronous communication the Connector supports only Iterator mode.

When configuring ALE in an SAP System, the core task is to create what is called a distribution model. There are many pre-defined distribution models available as standard in an SAP system, but there is also the ability to create a customizable distribution model of your own. The core use of this connector is as an external application that acts as a logical system within the chosen SAP distribution model. The examples provided in this chapter will define integration into a custom SAP HR distribution model, and the pre-defined SAP Central User Management (CUA) distribution model. Of course the connector could be used for integration into any of the other SAP distribution models to access the master data for other SAP modules such as SAP FI/CO or SAP PP. For detailed information on SAP modules visit the SAP help site at <http://help.sap.com>. Almost any SAP master data business object with an IDOC interface can be exchanged this way.

Central to creating or configuring an SPA distribution model are the IDOC message types you want to support. What the connector provides is an XML version of the IDOC, which must be parsed accordingly. To facilitate parsing of the IDOC XML data the connector has been enabled to make use of the IBM Tivoli Directory Integrator XML parsers. You have the choice of the DOM Parser, the SAX Parser or the XSLT Parser. Using these will enable you to extract the required data from the IDOC for your business purpose. For example you may wish to extract particular infotypes from the SAP HR IDOC message type HRMD\_A to forward on to IBM Tivoli Identity Manager for automated provisioning purposes.

The figure below illustrates the interaction with the SAP System IDOC client and the IBM Tivoli Directory Integrator IDOC server.

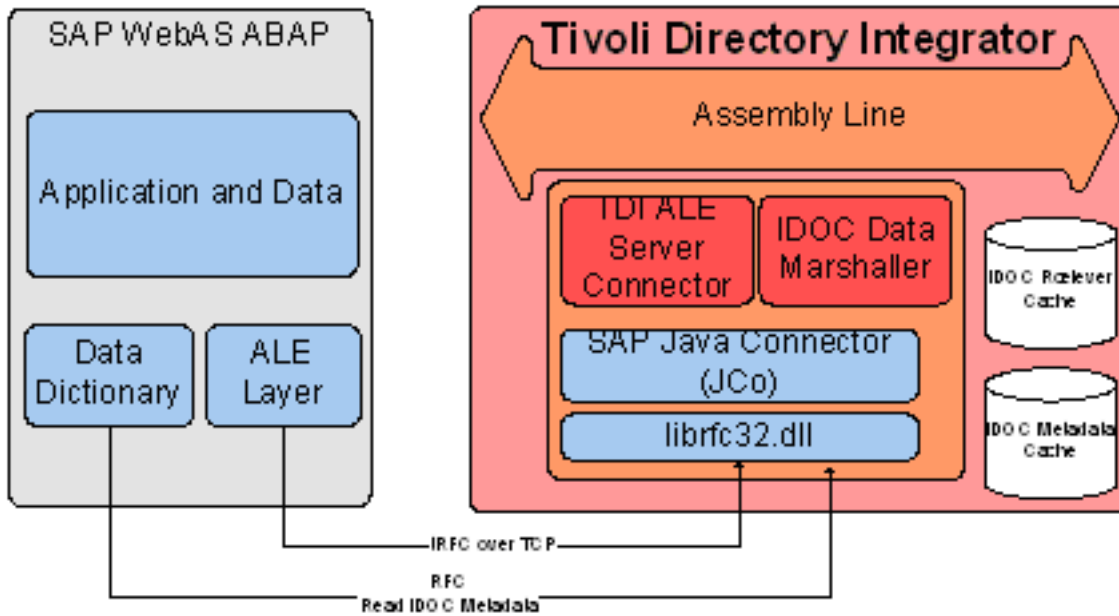


Figure 4. Interaction with the SAP System IDOC client and the IBM Tivoli Directory Integrator IDOC server

## Configuration

The SAP ALE IDOC Connector for SAP R/3 may be added directly into an assembly line. The following section lists the configuration parameters the connector.

### IDOC Server Parameters

#### IDOC Server SAP Gateway Host

A mandatory RFC Server Connection attribute that defines the host system that is the SAP Gateway.

#### IDOC Server SAP Gateway Service

A mandatory RFC Server Connection attribute that defines the SAP Gateway Service.

#### IDOC Server Program ID

A mandatory RFC Server Connection attribute that Defines the Server Program ID that is used in the configuration of the required TCP/IP RFC Destination to register the Server with the SAP Gateway.

#### IDOC Server Unicode Connection?

An optional RFC Server Connection attribute that defines the host system that is the SAP Gateway.

#### IDOC Server Optional Connection Parameters

An optional RFC Server Connection attribute used to define a list of other optional RFC connection parameters. The value for this configuration list is a key=value list where each connection parameter is separated by the space character. For example the following string value would set the SAP System number to "00" and enable the RFC trace mechanism:

```
"jco.server.trace=1 jco.server.sysnr=00"
```

### IDOC Client Configuration Parameters

#### IDOC Client Number

A mandatory RFC Client Connection attribute that defines the SAP Systems client. Consists of a 3 digit string value such as "000" or "100" defining the logon client.

**IDOC Client User**

A mandatory RFC Client Connection attribute that defines the SAP User Account logon id. Typically this would be a SAP User Account type of Communication or CPIC, although the Dialogue type can be used

**IDOC Client Password**

A mandatory RFC Client Connection attribute that defines the SAP User Account password.

**IDOC Client Lang**

A mandatory RFC Client Connection attribute that defines the logon language.

**IDOC Client Hostname**

A mandatory RFC Client Connection attribute that defines the hostname for the target SAP System.

**IDOC Client System Number**

A mandatory RFC Client Connection attribute that defines the system identifier (SID) for the target SAP System.

**IDOC Client SAP Gateway Service**

An optional RFC Client Connection attribute that defines the SAP Gateway Service. In most cases this will have the same value as the IDOC Server SAP Gateway Service.

**IDOC Client SAP Gateway Host**

An optional RFC Client Connection attribute that defines the SAP Gateway hostname.

**IDOC Client Max Connections**

A mandatory RFC Client Connection attribute that defines the maximum number of RFC connections supported by the internal connection pool.

**IDOC Client Optional Connection Parameters**

An optional RFC Client Connection attribute used to define a list of other optional RFC connection parameters. The value for this configuration list is a key=value list where each connection parameter is separated by the space character. For example the following string value would turn on the RFC trace mechanism and enable the use of the SAP GUI if it was installed on the same host as IBM Tivoli Directory Integrator.

```
"jco.client.trace=1 jco.client.use_sapgui=1"
```

The following is a list of optional SAP Java Connector parameters that are accessible.

Alias user name [jco.client.alias\_user]

SAP message server [jco.client.ms host]

RFC trace [jco.client.trace]

Initial codepage in SAP notation [jco.client.codepage]

Secure network connection (SNC) mode, 0 (off) or 1 (on) [jco.client.snc\_mode]

SNC partner, e.g. p:CN=R3, O=XYZ-INC, C=EN [jco.client.snc\_partnername]

SNC level of security, 1 to 9 [jco.client.snc\_qop]

SNC name. Overrides default SNC partner [jco.client.snc\_myname]

Path to library, which provides SNC service [jco.client.snc\_lib]

SAP R/3 name [jco.client.r3name]

Group of SAP application servers [jco.client.group]

Program ID of external server program [jco.client.tpname]

Host of external server program [jco.client.tphost]

Type of remote host 2 = R/2, 3 = R/3, E = External [jco.client.type]

Enable ABAP debugging 0 or 1 [jco.client.abap\_debug]

Use remote SAP graphical user interface (0/1/2) [jco.client.use\_sapgui]

Get/Don't get a SSO ticket after logon (1 or 0) [jco.client.getsso2]

Use the specified SAP Cookie Version 2 as logon ticket [jco.client.mysapsso2]

Use the specified X509 certificate as logon ticket [jco.client.x509cert]

Enable/Disable logon check at open time, 1 (enable) or 0 (disable) [jco.client.lcheck]

String defined for SAPLOGON on 32-bit Windows [jco.client.saplogon\_id]  
Data for external authentication (PAS) [jco.client.extiddata]  
Type of external authentication (PAS) [jco.client.extidtype]  
Idle timeout (in seconds) for the connection after which it will be closed by R/3.  
Only positive Enable (1) or Disable (0) dsr support [jco.client.dsr]

## General Configuration Parameters

### IDOC As XML Only?

A general attribute that defines if only the XML valued attribute for the IDOC is required. If set to “No”, the IDOC control data will be set as independent attributes within the resulting Entry for each IDOC. If set to “Yes”, only one attribute (idoc.xml) is created for the IDOC which contains the IDOC content as an XML valued string.

### Process SAP RFM Requests?

A general attribute that defines if the Connector will also process remote function module (RFM) calls made on it. If set to “Yes” all RFM calls will be added to an Entry which contain one attribute (rfm.xml) which is the content of the RFM as an XML valued string. If set to “No” then RFM requests on the IDOC Server will be ignored.

**Note:** The processing performed for RFM calls is merely to provide the RFM as an XML valued attribute. The IDOC Server does not currently attempt to populate the export and table arguments of the RFM call. If required this can be provided under an enhancement of the Connector. To do this contact IBM Support. Only RFM calls that form part of an ALE distribution models internal process should be considered.

### Parse IDOC or RFM XML?

A general attribute that defines if parsing is to be attempted on the XML valued attributes idoc.xml and rfm.xml. You must have one of the available IBM Tivoli Directory Integrator parsers configured to interact with the Connector in your AssemblyLine configuration.

### Enable JCo Middleware Trace Logging?

A general attribute that defines if the available JCo trace logs are to be enabled and included in the AssemblyLine logging and tracing.

### JCo Middleware Trace Level

A general attribute that defines the JCo middleware trace level.

### JCo Middleware Trace File Path

A general attribute that defines the directory where the JCo middleware trace file will be created. Also used to store RFM requests as a file with XML content.

## Using the SAP ALE IDOC Connector

This section describes details on using the Connector in the supported Iterator mode. Also described is the IBM Tivoli Directory Integrator schema supported by the Connector.

### IBM Tivoli Directory Integrator schema

The schema for the Connector is centred on providing an AssemblyLine with Entries, where each represents an individual IDOC. An IDOC itself contains 3 sections of data. These are Control Data, Segment Data, and Status Data. The simplest and most effective way of representing this data in IBM Tivoli Directory Integrator is an XML format, which can be easily dissected for the required data. As the control data is readily accessible, and can provide useful standalone information, this data is also available as individual attributes. The configuration parameter “IDOC As XML Only?” is used to enable or disable the production of the control data as stand alone attributes.

As the Connector is also able to accept Remote Function Module requests, there is a requirement to represent the data in one or more attributes. Currently the content of an RFM will be available as a single XML valued attribute. The configuration parameter “Process SAP RFM Requests?” is used to enable or disable the production of the RFM XML valued attribute.



The table below defines the schema available to this Connector.

*Table 46. SAP ALE IDOC Connector Schema*

| Attribute Name                | Attribute Description  | Attribute Syntax |
|-------------------------------|--|------------------|
| idoc.tid                      | Input schema attribute whose value is the associated TID value provided by the SAP System Client.  | java.lang.string |
| idoc.xml                      | Input schema attribute whose value is the complete IDOC in XML format.   | java.lang.string |
| idoc.segments.xml             | Input schema attribute whose value is the complete Segment hierarchy in XML format. No control attribute values are contained in this XML. | java.lang.string |
| idoc.ctrl.ArchiveKey          | Input schema attribute whose value represents the IDOC control data archive key (the value of the field "ARCKEY").                         | java.lang.string |
| idoc.ctrl.Client              | Input schema attribute whose value represents the IDOC control data client (the value of the field "MANDT").                               | java.lang.string |
| idoc.ctrl.CreationDate        | Input schema attribute whose value represents the IDOC control data creation date (the value of the field "CREDAT").                       | java.lang.string |
| idoc.ctrl.CreationTime        | Input schema attribute whose value represents the IDOC control data creation time (the value of the field "CRETIM").                       | java.lang.string |
| idoc.ctrl.Direction           | Input schema attribute whose value represents the IDOC control data direction (the value of the field "DIRECT").                           | java.lang.string |
| idoc.ctrl.EDIMessage          | Input schema attribute whose value represents the IDOC control data EDI message (the value of the field "REFMES").                         | java.lang.string |
| idoc.ctrl.EDIMessageGroup     | Input schema attribute whose value represents the IDOC control data EDI message group (the value of the field "REFGRP").                   | java.lang.string |
| idoc.ctrl.EDIMessageType      | Input schema attribute whose value represents the IDOC control data EDI message type (the value of the field "STDMES").                    | java.lang.string |
| idoc.ctrl.EDIStandardFlag     | Input schema attribute whose value represents the IDOC control data EDI standard flag (the value of the field "STD").                      | java.lang.string |
| idoc.ctrl.EDIStandardVersion  | Input schema attribute whose value represents the IDOC control data EDI standard version (the value of the field "STDVRS").                | java.lang.string |
| idoc.ctrl.EDITransmissionFile | Input schema attribute whose value represents the IDOC control data EDI transmission file (the value of the field "REFINT").               | java.lang.string |
| idoc.ctrl.ExpressFlag         | Input schema attribute whose value represents the IDOC control data express flag (the value of the field "EXPRSS").                        | java.lang.string |
| idoc.ctrl.IDocCompoundType    | Input schema attribute whose value represents the IDOC control data IDOC compound type (the value of the field "DOCTYP").                  | java.lang.string |
| idoc.ctrl.IDocNumber          | Input schema attribute whose value represents the IDOC control data IDOC number (the value of the field "DOCNUM").                         | java.lang.string |
| idoc.ctrl.IDocSAPRelease      | Input schema attribute whose value represents the IDOC control data IDOC SAP release (the value of the field "DOCREL").                    | java.lang.string |
| idoc.ctrl.IDocType            | Input schema attribute whose value represents the IDOC control data IDOC type (the value of the field "IDOCTYP").                          | java.lang.string |

Table 46. SAP ALE IDOC Connector Schema (continued)

| Attribute Name                     | Attribute Description  | Attribute Syntax |
|------------------------------------|--|------------------|
| idoc.ctrl.IDocTypeExtension        | Input schema attribute whose value represents the IDOC control data IDOC type extension that is also known as CIM type or customer extension type (the value of the field "CIMTYP"); | java.lang.string |
| idoc.ctrl.MessageCode              | Input schema attribute whose value represents the IDOC control data message code (the value of the field "MESCOD").  | java.lang.string |
| idoc.ctrl.MessageFunction          | Input schema attribute whose value represents the IDOC control data message function (the value of the field "MESFCT").  | java.lang.string |
| idoc.ctrl.MessageType              | Input schema attribute whose value represents the IDOC control data message type (the value of the field "MESTYP").  | java.lang.string |
| idoc.ctrl.OutputMode               | Input schema attribute whose value represents the IDOC control data output mode (the value of the field "OUTMOD").   | java.lang.string |
| idoc.ctrl.RecipientAddress         | Input schema attribute whose value represents the IDOC control data recipient address (the value of the field "RCVSAD").   | java.lang.string |
| idoc.ctrl.RecipientLogicalAddress  | Input schema attribute whose value represents the IDOC control data logical recipient address (the value of the field "RCVLAD").   | java.lang.string |
| idoc.ctrl.RecipientPartnerFunction | Input schema attribute whose value represents the IDOC control data recipient partner function (the value of the field "RCVPFC").  | java.lang.string |
| idoc.ctrl.RecipientPartnerNumber   | Input schema attribute whose value represents the IDOC control data recipient partner number (the value of the field "RCVPRN").  | java.lang.string |
| idoc.ctrl.RecipientPartnerType     | Input schema attribute whose value represents the IDOC control data recipient partner type (the value of the field "RCVPRT").  | java.lang.string |
| idoc.ctrl.RecipientPort            | Input schema attribute whose value represents the IDOC control data recipient port (the value of the field "RCVPOR").  | java.lang.string |
| idoc.ctrl.SenderAddress            | Input schema attribute whose value represents the IDOC control data sender address (the value of the field "SNDSAD").  | java.lang.string |
| idoc.ctrl.SenderLogicalAddress     | Input schema attribute whose value represents the IDOC control data logical sender address (the value of the field "SNDLAD").  | java.lang.string |
| idoc.ctrl.SenderPartnerFunction    | Input schema attribute whose value represents the IDOC control data sender partner function (the value of the field "SNDPFC").   | java.lang.string |
| idoc.ctrl.SenderPartnerNumber      | Input schema attribute whose value represents the IDOC control data sender partner number (the value of the field "SNDPRN").   | java.lang.string |
| idoc.ctrl.SenderPartnerType        | Input schema attribute whose value represents the IDOC control data sender partner type (the value of the field "SNDPRT").   | java.lang.string |
| idoc.ctrl.SenderPort               | Input schema attribute whose value represents the IDOC control data Returns the sender port (the value of the field "SNDPOR").   | java.lang.string |
| idoc.ctrl.Serialization            | Input schema attribute whose value represents the IDOC control data serialization (the value of the field "SERIAL").   | java.lang.string |

Table 46. SAP ALE IDOC Connector Schema (continued)

| Attribute Name               | Attribute Description  | Attribute Syntax |
|------------------------------|--|------------------|
| idoc.ctrl.Status             | Input schema attribute whose value represents the IDOC control data status (the value of the field "STATUS").                | java.lang.string |
| idoc.ctrl.TableStructureName | Output schema attribute whose value represents the IDOC control data table structure name (the value of the field "TABNAM"). | java.lang.string |
| idoc.ctrl.TestFlag           | Input schema attribute whose value represents the IDOC control data test flag (the value of the field "TEST").               | java.lang.string |
| rfm.xml                      | Input schema attribute whose value represents the complete content of an RMF request in XML format.                          | java.lang.string |

Attributes of type `java.lang.String` can be of arbitrary length.

## XML Attribute Parsing

The main mode of operation for the connector is the production of the XML valued attributes that represent the complete content of an IDOC, or RFM. As a result the best way to handle this data is with one of the available IBM Tivoli Directory Integrator XML Parsers attached to the Connector. Due to the nested nature of the resulting XML, the DOM parser is not recommended, but still can be used. The recommended parsers are the SAX Parser or the XSLT Parser depending on the type of SAP ALE distribution model the Connector is to integrate with. If the Connector has to handle multiple IDOC message types, or is configured to process RFM requests, then the SAX Parser is recommended. This is because you will have different XML schemas for the different IDOC message types, and the RFM XML. The SAX Parser is the only IBM Tivoli Directory Integrator parser that can handle XML values with different XML schemas. You do this by not configuring the SAX Parser to have a specific value for its "Group" configuration parameter. This has the effect of not having to define a particular root element. If you are certain that the Connector will process only one type of IDOC, then you can use the XSLT Parser, which allows for a more complete Connector Entry to Work Entry attribute mapping. For example if the Connector was configured to be the recipient of SAP HR Master Data, then you would only ever expect to see IDOCs of the message type HRMD\_A. At the time this connector was developed the latest version of this message type was HRMD\_A06. You could then use an XSL like the following to parse the IDOCs contents for the required data.

```
<XSL:stylesheet xmlns:XSL="http://www.w3.org/1999/XSL/Transform" version="1.0">
  <XSL:output method="XML" indent="yes" />

  <XSL:template match="HRMD_A06">
    <DocRoot>
      <Entry>
        <XSL:apply-templates select="./IDOC"/>
      </Entry>
    </DocRoot>
  </XSL:template>

  <XSL:template match="IDOC">
    <XSL:apply-templates select="./EDI_DC40"/>
    <XSL:apply-templates select="./E1PLOGI"/>
  </XSL:template>

  <XSL:template match="EDI_DC40">
    <Attribute name="IDOC_CTRL_DOCNUM">
      <XSL:for-each select="DOCNUM">
        <Value>
          <XSL:value-of select="." />
        </Value>
      </XSL:for-each>
    </Attribute>
    <Attribute name="IDOC_CTRL_MANDT">
      <XSL:for-each select="MANDT">
        <Value>
```

```

        <XSL:value-of select="." />
    </Value>
</XSL:for-each>
</Attribute>
<Attribute name="IDOC_CTRL_DOCREL">
    <XSL:for-each select="DOCREL">
        <Value>
            <XSL:value-of select="." />
        </Value>
    </XSL:for-each>
</Attribute>
<Attribute name="IDOC_CTRL_IDOCTYP">
    <XSL:for-each select="IDOCTYP">
        <Value>
            <XSL:value-of select="." />
        </Value>
    </XSL:for-each>
</Attribute>
<Attribute name="IDOC_CTRL_SNDPOR">
    <XSL:for-each select="SNDPOR">
        <Value>
            <XSL:value-of select="." />
        </Value>
    </XSL:for-each>
</Attribute>
<Attribute name="IDOC_CTRL_RCVPOR">
    <XSL:for-each select="RCVPOR">
        <Value>
            <XSL:value-of select="." />
        </Value>
    </XSL:for-each>
</Attribute>
</XSL:template>

<XSL:template match="E1PLOGI">
    <XSL:apply-templates select="./E1PITYP"/>
</XSL:template>

<XSL:template match="E1PITYP">
    <XSL:apply-templates select="./E1P0002"/>
    <XSL:for-each select="E1P0105">
        <Attribute name="PR_COMM_SUBTY">
            <XSL:for-each select="SUBTY">
                <Value>
                    <XSL:value-of select="." />
                </Value>
            </XSL:for-each>
        </Attribute>
        <Attribute name="PR_COMM_USRID">
            <XSL:for-each select="USRID">
                <Value>
                    <XSL:value-of select="." />
                </Value>
            </XSL:for-each>
        </Attribute>
        <Attribute name="PR_COMM_USRID_LONG">
            <XSL:for-each select="USRID_LONG">
                <Value>
                    <XSL:value-of select="." />
                </Value>
            </XSL:for-each>
        </Attribute>
    </XSL:for-each>
</XSL:template>

<XSL:template match="E1P0002">
    <Attribute name="PR_PERNR">

```

```

    <XSL:for-each select="PERNR">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="PR_LASTNAME">
    <XSL:for-each select="NACHN">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="PR_FIRSTNAME">
    <XSL:for-each select="VORNA">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="PR_BIRTHDATE">
    <XSL:for-each select="GBDAT">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>
</XSL:stylesheet>

```

If the IDOC message type was always going to be the USERCLONE message type, then you could use XSL like the following to get the required attribute mappings.

```

<XSL:stylesheet xmlns:XSL="http://www.w3.org/1999/XSL/Transform" version="1.0">
  <XSL:output method="XML" indent="yes" />

  <XSL:template match="USERCLONE05">
    <DocRoot>
      <Entry>
        <XSL:apply-templates select="./IDOC"/>
      </Entry>
    </DocRoot>
  </XSL:template>

  <XSL:template match="IDOC">
    <XSL:apply-templates select="./EDI_DC40"/>
    <XSL:apply-templates select="./E1BPBNAME"/>
    <XSL:apply-templates select="./E1BPLOGOND"/>
    <XSL:apply-templates select="./E1BPADDR3"/>
    <XSL:apply-templates select="./E1BPLOGOND"/>
    <XSL:apply-templates select="./E1BPUSCOMP"/>
  </XSL:template>

  <XSL:template match="EDI_DC40">
    <Attribute name="TDI_DOCNUM">
      <XSL:for-each select="DOCNUM">
        <Value>
          <XSL:value-of select="." />
        </Value>
      </XSL:for-each>
    </Attribute>
    <Attribute name="TDI_MANDT">
      <XSL:for-each select="MANDT">
        <Value>
          <XSL:value-of select="." />
        </Value>
      </XSL:for-each>
    </Attribute>
  </XSL:template>

```

```

    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_DOCREL">
    <XSL:for-each select="DOCREL">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_IDOCTYP">
    <XSL:for-each select="IDOCTYP">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_USERCLONE">
    <XSL:for-each select="USERCLONE">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_SNDPOR">
    <XSL:for-each select="SNDPOR">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_RCVPOR">
    <XSL:for-each select="RCVPOR">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>

<XSL:template match="E1BPBNAME">
  <Attribute name="TDI_BAPIBNAME">
    <XSL:for-each select="BAPIBNAME">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>

<XSL:template match="E1BPLOGOND">
  <Attribute name="TDI_CLASS">
    <XSL:for-each select="CLASS">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
  <Attribute name="TDI_TZONE">
    <XSL:for-each select="TZONE">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>

<XSL:template match="E1BPADDR3">

```

```

<Attribute name="TDI_FIRSTNAME">
  <XSL:for-each select="FIRSTNAME">
    <Value>
      <XSL:value-of select="." />
    </Value>
  </XSL:for-each>
</Attribute>
<Attribute name="TDI_LASTNAME">
  <XSL:for-each select="LASTNAME">
    <Value>
      <XSL:value-of select="." />
    </Value>
  </XSL:for-each>
</Attribute>
<XSL:apply-templates select="./E1BPADDR1"/>
</XSL:template>

<XSL:template match="E1BPADDR1">
  <Attribute name="TDI_E_MAIL">
    <XSL:for-each select="E_MAIL">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>

<XSL:template match="E1BPUSCOMP">
  <Attribute name="TDI_COMPANY">
    <XSL:for-each select="COMPANY">
      <Value>
        <XSL:value-of select="." />
      </Value>
    </XSL:for-each>
  </Attribute>
</XSL:template>
</XSL:stylesheet>

```

## Configuration in SAP ALE Distribution Models

To enable the connector to be part of an SAP ALE distribution model the Connector must be setup as a logical system on the SAP system. To do this two actions are required.

1. An RFC Destination of type TCP/IP is created where the Connector is registered as an external program. Take care to make sure that the program name provided in the RFC Destination, is the same value you give to the Connector configuration parameter "IDOC Server Program ID". To test the RFC connection ensure the Connector is running in an IBM Tivoli Directory Integrator AssemblyLine. This AssemblyLine may be bare bones one with only the connector, and possibly a script component to dump the resulting work entry attributes. Create RFC Destinations using SAP GUI transaction SM59.
2. A logical System is created that has the same name as the RFC Destination created in step 1. This is done using SAP GUI transaction SALE. You don't need to assign a client to the logical system like you do for other SAP logical systems that actually represent a real SAP System client.

Once the logical system is in place you can pretty much use it as you would any other logical system in an SAP ALE distribution model. The Connector has been tested as part of a SAP HR Master Data distribution model, and as part of the pre-defined SAP CUA distribution model. If you run into other issues using other SAP ALE distribution models please contact IBM Support. This is a new Connector for IBM Tivoli Directory Integrator and will no doubt have some teething issues.





---

## Troubleshooting the SAP R/3 Component Suite

Problems may be experienced for any of the following reasons:

### SAP Java Connector not installed properly

Check the installation and re-install if necessary.

### Missing `sapjco.jar`

If you attempt to use the SAP R/3 RFC FC and get an error similar to the following:

```
13:01:58 Error in: InitConnectors: java.lang.ClassCastException:
    java.lang.NoClassDefFoundError
```

```
java.lang.ClassCastException: java.lang.NoClassDefFoundError
```

It may be that SAP JCo is not installed correctly. Check that `sapjco.jar` is in the `TDI_Home/jars` directory. Refer to the instructions in “Configuring the SAP Java Connector” on page 381.

### Missing `librfc32.dll`

If you attempt to use SAP R/3 RFC FC and get an error similar to the following:

*"The dynamic linked library LIBRFC32.dll could not be found in the specified path"*

On Windows machines, ensure that `librfc32.dll` is in the `TDI_Home/libs` directory. On Solaris and AIX machines, ensure that `librfccm.{o/so}` has been added to the loadable library path.

### Old version of `librfc32.dll`

If you get an error of the following type:

```
java.lang.ClassCastException: java.lang.ExceptionInInitializerError
```

It is possible that the `librfc32` being used is an older version and is not compatible with JCo 2.1.6. Check that there is no other `librfc32` in your `PATH`. Also check that any `librfc32*.{dll/so}` that is in your system path is at least version 6403.3.81.4751.

```
15:13:44 [YourAssemblyLine] BEGIN selectEntries
```

```
15:13:45 [YourAssemblyLine] handleException: initialize,
java.lang.ClassCastException: java.lang.ExceptionInInitializerError
```

```
15:13:45 [YourAssemblyLine] initialize
```

```
java.lang.ClassCastException: java.lang.ExceptionInInitializerError
    at com.ibm.di.script.ScriptEngine.call(Unknown Source)
    at com.ibm.di.connector.ScriptConnector.selectEntries(Unknown Source)
    at com.ibm.di.server.AssemblyLineComponent.initialize(Unknown Source)
    at com.ibm.di.server.AssemblyLine.initConnectors(Unknown Source)
    at com.ibm.di.server.AssemblyLine.msInitConn(Unknown Source)
    at com.ibm.di.server.AssemblyLine.executeMainStep(Unknown Source)
    at com.ibm.di.server.AssemblyLine.executeMainLoop(Unknown Source)
    at com.ibm.di.server.AssemblyLine.executeAL(Unknown Source)
    at com.ibm.di.server.AssemblyLine.run(Unknown Source)
```

### RFC\_ERROR\_SYSTEM\_FAILURE: Screen output without connection to user

If the connector returns this message, please see SAP Note 49730 for more information.

### Query Schema Issues

When performing a schema query using the Connectors with the IBM Tivoli Directory Integrator GUI, an attempt to connect to the data source may result in an exception. These exceptions can be ignored. Any subsequent use of the **discover** schema button will succeed.

The Connectors do not support the *Get Next Entry* style of schema query. The Connectors support the torch button *Discover the Schema of the data source* style of schema discovery.

### User Registry Company Code Assignment

If the value associated with the XML element, `<companyKeyName>`, does not represent a valid company code within SAP, or is not supplied at all, SAP will assign the configured default.

### Changing Mode of Connectors Already in AssemblyLine

During testing, it was observed that changing the mode of Connector in the AssemblyLine did not always work. The Connector sometimes appeared to execute in its original mode, resulting in AssemblyLine errors. If this occurs, delete the Connector and add it to the AssemblyLine in the new mode.

### Function Component differences to SE37 Test RFC Feature

In some cases, the RFC Function Component exhibits slightly different behavior to that observed when executing a given RFC from SAP's *Test Function Feature*, available from transaction SE37. In some cases, the SAP test feature will automatically convert values to internal German abbreviated values (for example, BAPI\_SALESORDER\_GETLIST). Therefore, some of the values returned by the connector in **Lookup** and **Iterator** mode may differ slightly from those returned by the SAP test function feature. When you are required to provide input XML files to set the values of parameters, you should supply the internal values (that is, the same format as the values returned by the connector in **Lookup** and **Iterator** modes).

The RFC Function Component will not pad out values of character string types to the maximum length.

### User Registry Connector Warnings

In some cases, the Connectors may log warning severity messages as a result of application level ABAP warnings return from SAP. An example of warning messages logged by the User Registry Connector running in **Iterator** mode is shown below.

```
15:50:10 [newGetUsers] W: Unable to read the address (69) (D:\Program
Files\IBM\IBMDirectoryIntegrator\xsl\bapi_user_get_detail_precall.xml)

15:50:10 [newGetUsers] W: Unable to determine the company (76) (D:\Program
Files\IBM\IBMDirectoryIntegrator\xsl\bapi_user_get_detail_precall.xml)
```

In most cases, these warning messages can be ignored.

### User Registry Connector In Update Mode

When run in this mode, the Connector expects the **sapUserName** attribute to be defined in the **Link Criteria** and as an XML element, <sapUserName>, within the value associated with the attribute **sapUserXml**. The values of **sapUserName** should match in both cases. The Connector does not verify the equality.

### Password Behavior In SAP

After a new user is created in SAP, or the password of an existing user is changed, SAP will prompt that user to reset their password at the next logon. This is standard SAP behavior and occurs if the user is created or modified through the SAP transaction SU01, or the Connector.

### Delete HR Personal Data With HR Connector

In some cases, an attempt to delete a Personal Data entry using the Connector, or SAP transaction PA30, may fail. The failure message states "*Record cannot be deleted (time constraint 1)*". Currently, there is no known solution to this problem.

---

## Supplemental information for the SAP R/3 Component Suite

### Example User Registry Connector XML Instance Document

The following code sample shows an example User Registry Connector XML Instance Document:

```
<User>
  <sapUserName></sapUserName>
  <sapUserPassword></sapUserPassword>
  <sapUserAlias>
    <aliasName></aliasName>
  </sapUserAlias>
  <sapAddress>
    <title></title>
    <academicTitle></academicTitle>
    <firstName></firstName>
    <lastName></lastName>
    <namePrefix></namePrefix>
    <nameFormat></nameFormat>
    <nameFormatRuleCountry></nameFormatRuleCountry>
    <isoLanguage></isoLanguage>
    <language></language>
    <searchSortTerm></searchSortTerm>
    <department></department>
    <function></function>
    <buildingNumber></buildingNumber>
    <buildingFloor></buildingFloor>
    <roomNumber></roomNumber>
    <name></name>
    <name2></name2>
    <name3></name3>
    <name4></name4>
    <city></city>
    <postCode></postCode>
    <poBoxPostCode></poBoxostCode>
    <poBox></poBox>
    <street></street>
    <streetNumber></streetNumber>
    <houseNumber></houseNumber>
    <country></country>
    <countryIso></countryIso>
    <region></region>
    <timeZone></timeZone>
    <primaryPhoneNumber></primaryPhoneNumber>
    <primaryPhoneExtension></primaryPhoneExtension>
    <primaryFaxNumber></primaryFaxNumber>
    <primaryFaxExtension></primaryFaxExtension>
  </sapAddress>
  <sapCompany>
    <companyNameKey></companyNameKey>
  </sapCompany>
  <sapDefaults>
    <startMenu></startMenu>
    <outputDevice></outputDevice>
    <printTimeAndDate></printTimeAndDate>
    <printDelete></printDelete>
    <dateFormat></dateFormat>
    <decimalFormat></decimalFormat>
    <logonLanguage></logonLanguage>
    <cattTestStatus></cattTestStatus>
    <costCenter></costCenter>
  </sapDefaults>
  <sapLogonData>
    <validFromDate></validFromDate>
    <validToDate></validToDate>
    <userType></userType>
    <userGroup></userGroup>
  </sapLogonData>
</User>
```

```

    <accountId></accountId>
    <timeZone></timeZone>
    <lastLogonTime></lastLogonTime>
    <codeVerEncryption></codeVerEncryption>
</sapLogonData>
<sapSncData>
  <printableName></printableName>
  <allowUnsecure></allowUnsecure>
</sapSncData>
<sapUserGroupList>
  <group>
    <name></name>
  </group>
  <group>
    <name></name>
  </group>
</sapUserGroupList>
<sapParameterList>
  <parameter>
    <parameterId></parameterId>
    <parameterValue></parameterValue>
  </parameter>
  <parameter>
    <parameterId></parameterId>
    <parameterValue></parameterValue>
  </parameter>
</sapParameterList>
<sapUserEmailAddressList>
  <email>
    <defaultNumber></defaultNumber>
    <smtpAddress></smtpAddress>
    <isHomeAddress></isHomeAddress>
    <sequenceNumber></sequenceNumber>
  </email>
  <email>
    <defaultNumber></defaultNumber>
    <smtpAddress></smtpAddress>
    <isHomeAddress></isHomeAddress>
    <sequenceNumber></sequenceNumber>
  </email>
</sapUserEmailAddressList>
<sapRoleList>
  <role>
    <name></name>
    <validFromDate></validFromDate>
    <validToDate></validToDate>
  </role>
  <role>
    <name></name>
    <validFromDate></validFromDate>
    <validToDate></validToDate>
  </role>
</sapRoleList>
<sapProfileList>
  <profile>
    <name></name>
  </profile>
  <profile>
    <name></name>
  </profile>
</sapProfileList>
</User>

```

## XSchema for User Registry Connector XML

The XSchema for User Registry Connector XML is show below:

```

<?xml version="1.0" encoding="UTF-8"?>
<xsd:schema xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <xsd:element name="User">
    <xsd:complexType>
      <xsd:sequence>
        <xsd:element ref="sapUserName" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="sapUserPassword" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="sapUserAlias" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapAddress" minOccurs="1" maxOccurs="1"/>
        <xsd:element ref="sapCompany" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapDefaults" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapLogonData" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapSncData" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapUserGroupList" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapParameterList" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapUserEmailAddressList" minOccurs="0"
          maxOccurs="1"/>
        <xsd:element ref="sapRoleList" minOccurs="0" maxOccurs="1"/>
        <xsd:element ref="sapProfileList" minOccurs="0" maxOccurs="1"/>
      </xsd:sequence>
    </xsd:complexType>
  </xsd:element>
  <xsd:element name="academicTitle">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="20"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="accountId">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="12"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="aliasName">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="40"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="allowUnsecure">
    <xsd:simpleType >
      <xsd:restriction base="xsd:boolean">
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="buildingFloor">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="10"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="buildingNumber">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="10"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="cattTestStatus">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="1"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>

```

```

    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="companyNameKey">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="42"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="costCenter">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="8"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="dateFormat">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="1"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="decimalFormat">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="1"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="defaultNumber">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="1"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="department">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="email">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="defaultNumber" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="smtpAddress" minOccurs="1" maxOccurs="1"/>
      <xsd:element ref="isHomeAddress" maxOccurs="1" minOccurs="0"/>
      <xsd:element ref="sequenceNumber" minOccurs="1" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="firstName">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="function">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>

```

```

</xsd:simpleType>
</xsd:element>
<xsd:element name="group">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="name">
        <xsd:simpleType >
          <xsd:restriction base="xsd:string">
            <xsd:maxLength value="12"></xsd:maxLength>
          </xsd:restriction>
        </xsd:simpleType>
      </xsd:element>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="isHomeAddress">
  <xsd:simpleType >
    <xsd:restriction base="xsd:boolean">
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
<xsd:element name="isoLanguage">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="2"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="language">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="1"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="lastLogonTime">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:minLength value="8"></xsd:minLength>
      <xsd:maxLength value="8"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="lastName">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="logonLanguage">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="1"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="name">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="name2">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">

```

```

    <xsd:maxLength value="40"></xsd:maxLength>
  </xsd:restriction>
</xsd:simpleType>
</xsd:element>
<xsd:element name="name3">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="name4">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="40"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="nameFormat">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="2"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="nameFormatRuleCountry">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="3"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="namePrefix">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="20"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="outputDevice">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="4"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="parameter">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element ref="parameterId" minOccurs="0" maxOccurs="1"/>
      <xsd:element ref="parameterValue" minOccurs="0" maxOccurs="1"/>
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
<xsd:element name="parameterId">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="20"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="parameterValue">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="18"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>

```



```

</xsd:element>
<xsd:element name="poBox">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="10"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="postCode">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="10"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="primaryFaxExtension">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="10"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="primaryFaxNumber">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="30"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="primaryPhoneExtension">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="10"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="primaryPhoneNumber">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="30"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="printDelete">
  <xsd:simpleType >
    <xsd:restriction base="xsd:boolean">
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="printTimeAndDate">
  <xsd:simpleType >
    <xsd:restriction base="xsd:boolean">
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="printableName">
  <xsd:simpleType >
    <xsd:restriction base="xsd:string">
      <xsd:maxLength value="255"></xsd:maxLength>
    </xsd:restriction>
  </xsd:simpleType>
</xsd:element>
<xsd:element name="profile">
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name="name">
        <xsd:simpleType >

```

```

        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="12"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
    </xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="region">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="3"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="role">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element name="name">
                <xsd:simpleType >
                    <xsd:restriction base="xsd:string">
                        <xsd:maxLength value="30"></xsd:maxLength>
                    </xsd:restriction>
                </xsd:simpleType>
            </xsd:element>
            <xsd:element ref="validFromDate" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="validToDate" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="roomNumber">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="10"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="sapAddress">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="title" minOccurs="1" maxOccurs="1"/>
            <xsd:element ref="academicTitle" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="firstName" minOccurs="1" maxOccurs="1"/>
            <xsd:element ref="lastName" minOccurs="1" maxOccurs="1"/>
            <xsd:element ref="namePrefix" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="nameFormat" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="nameFormatRuleCountry" minOccurs="0"
                maxOccurs="1"/>
            <xsd:element ref="isoLanguage" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="language" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="searchSortTerm" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="department" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="function" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="buildingNumber" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="buildingFloor" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="roomNumber" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="name" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="name2" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="name3" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="name4" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="postCode" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="poBox" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="street" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="region" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="timeZone" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="primaryPhoneNumber" minOccurs="0"
                maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>

```

```

        <xsd:element ref="primaryPhoneExtension" minOccurs="0"
            maxOccurs="1"/>
        <xsd:element ref="primaryFaxNumber" minOccurs="0"
            maxOccurs="1"/>
        <xsd:element ref="primaryFaxExtension" minOccurs="0"
            maxOccurs="1"/>
    </xsd:sequence>
</xsd:complexType>
</xsd:element>
<xsd:element name="sapCompany">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="companyNameKey" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapDefaults">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="startMenu" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="outputDevice" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="printTimeAndDate" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="printDelete" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="dateFormat" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="decimalFormat" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="logonLanguage" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="cattTestStatus" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="costCenter" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapLogonData">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="validFromDate" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="validToDate" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="userType" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="userGroup" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="accountId" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="timeZone" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="lastLogonTime" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapParameterList">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element maxOccurs="unbounded" minOccurs="0" ref="parameter"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapProfileList">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element maxOccurs="unbounded" minOccurs="0" ref="profile"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapRoleList">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element maxOccurs="unbounded" minOccurs="0" ref="role"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapSncData">
    <xsd:complexType>

```

```

        <xsd:sequence>
            <xsd:element ref="printableName" minOccurs="0" maxOccurs="1"/>
            <xsd:element ref="allowUnsecure" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapUserAlias">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element ref="aliasName" minOccurs="0" maxOccurs="1"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapUserEmailAddressList">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element maxOccurs="unbounded" minOccurs="0" ref="email"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapUserGroupList">
    <xsd:complexType>
        <xsd:sequence>
            <xsd:element maxOccurs="unbounded" minOccurs="0" ref="group"/>
        </xsd:sequence>
    </xsd:complexType>
</xsd:element>
<xsd:element name="sapUserName">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="12"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="sapUserPassword">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="8"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="searchSortTerm">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="20"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="sequenceNumber">
    <xsd:simpleType >
        <xsd:restriction base="xsd:nonNegativeInteger">
            <xsd:totalDigits value="3"></xsd:totalDigits>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="smtpAddress">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="241"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>
<xsd:element name="startMenu">
    <xsd:simpleType >
        <xsd:restriction base="xsd:string">
            <xsd:maxLength value="20"></xsd:maxLength>
        </xsd:restriction>
    </xsd:simpleType>
</xsd:element>

```

```

    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="street">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="60"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="timeZone">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="6"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="title">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="30"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="userGroup">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="12"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="userType">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="1"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="validFromDate">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="10"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
  <xsd:element name="validToDate">
    <xsd:simpleType >
      <xsd:restriction base="xsd:string">
        <xsd:maxLength value="10"></xsd:maxLength>
      </xsd:restriction>
    </xsd:simpleType>
  </xsd:element>
</xsd:schema>

```



---

## Chapter 7. Script languages

With this version of IBM Tivoli Directory Integrator the only script language available is JavaScript, implemented by means of the IBM JavaScript Engine (IBMJS), with Rhino compatibility extensions. If you previously have used VBScript, PerlScript or even BeanShell, you will need to convert this to JavaScript.

---

### JavaScript

There are certain issues you might want to consider when using JavaScript. These are:

- "Comparing JavaScript strings" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.
- "JavaScript string methods" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.
- "Java and JavaScript"

---

### Java and JavaScript

In JavaScript you can access Java objects. This is very useful, because all the IBM Tivoli Directory Integrator internal objects are Java objects.

However, there is a pitfall when some of the Java Objects have methods with names that are reserved words or operators in JavaScript. In these cases, the JavaScript interpreter tries to process the reserved word instead of calling the Java method.

Such an example can be found with the **java.io.File** class which has a delete method. **delete** is also a JavaScript operator, so the following fails:

```
var myFile = java.io.File("file.txt"); myFile.delete();
```

Instead, you can do one of the following:

- `myFile['delete']()`;

This exploits the fact that you can access the Java methods as array elements.

- `system.deleteFile("file.txt");`

This works well, because the system library has a **deleteFile** method.





---

## Chapter 8. Objects

The objects discussed in this chapter are fully documented in the Javadocs in the *root\_directory/docs/api* directory of your installation. Check the Javadocs for the available methods; you can view the Javadocs by selecting **Help>Low Level API** in the Config Editor.

---

### The AssemblyLine Connector object

The AssemblyLine Connector object is a wrapper that provides additional functionality to the Connector Interface. The Connector Interface can be accessed from the AssemblyLine Connector as the connector object.

**Note:** In addition to using the name of the AssemblyLine Connector, you can always refer to the currently executing AssemblyLine Connector object with the name "thisConnector" in your JavaScript code.

The AssemblyLine Connector is the Connector calling the hook functions you define in the AssemblyLine and is also the Connector that performs the attribute mapping. Each AssemblyLine Connector in the AssemblyLine is given a name that is automatically available in your scripts as that name. If you name an AssemblyLine Connector **ldap**, that name is also used as the **script object name**. Make sure you name your Connectors in a way that can be used as a JavaScript variable. Typically, you must avoid using whitespace and special characters.

The AssemblyLine Connector has methods and properties described in the `com.ibm.di.server.AssemblyLineComponent`.

---

### The attribute object

An attribute object is usually contained in Entry objects. An attribute is a named object with associated values. Each value in the attribute corresponds to a Java object of some type. Attribute names are not case-sensitive, and cannot contain a slash ( / ) as part of the name. Remember that some of the Connectors for example, those accessing a database, might consider other characters as unsuitable. If you can, try to stick to alphanumeric characters in attribute names.

If the attribute was populated with Connector values by the attribute map, the values are of the same datatype that the Connector supplied.

For more information, see the Javadocs material included in the installation package (the `com.ibm.di.entry.Attribute` class).

## Examples

### Creating a new attribute object

```
var attr = system.newAttribute("AttributeName");
```

This example creates an attribute object with name **AttributeName** and assigns it to the **attr** variable. Note that upon initial creation, the attribute holds no value. Now, through the **attr** variable you can access and interact with the newly created attribute.

### Adding values to an attribute

```
attr.addValue("value 1");  
attr.addValue("value 2");
```

This example adds the string values "value 1" and "value 2" to the **attr** attribute, thereby creating a multiple values attribute. Consecutive calls to **addValue(obj)** add values in the same order in the attribute.

### Scanning attribute's values

```
var values = attr.getValues();
for (i=0; i<values.length; i++) {
    task.logmsg("Value " + i + " -> " + values[i]);
}
```

This example processes any attribute object, whether it holds single or multiple values. In reality, there is no difference between single and multiple-value attributes. Every attribute can hold zero, one or more values. A single-value attribute is therefore merely an underloaded multiple-values attribute.

### See also

"The Entry object."

---

## The Connector Interface object

The Connector Interface object is obtained either by loading a Connector Interface explicitly (system.loadConnector) or by retrieving the named AssemblyLine Connectors's .connector (myConnector.connector). When writing scripts in an AssemblyLine, you usually use the AssemblyLine Connector object that gives you access to another set of methods.

The Connector Interface is fully described as Connector in the Javadocs. For more information, see the Javadocs material included in the installation package (com.ibm.di.connector.Connector).

### Methods

Some of the often-used methods include:

#### getNextEntry()

Returns the next input entry.

#### putEntry ( entry )

Adds or inserts an **entry**.

#### modEntry ( entry, search )

Modify entry identified by **search** with contents of **entry**.

#### deleteEntry ( entry, search )

Deletes the **entry** identified by **search**.

#### findEntry ( search )

Searches for an entry identified by **search**. If no entries are found, a **null** value is returned.

#### findEntry ( attribute, value )

Performs a search using "attribute equals value" and returns the entry found. If no entries or more than one entry is found a null value is returned.

---

## The Entry object

The Entry object is used by AssemblyLines and EventHandlers. The Entry object is a Java object that holds attributes and properties. Attributes in turn contain any number of values. Properties contain a single value. For more information, see the Javadocs material included in the installation package (com.ibm.di.entry.Entry).

## Global Entry instances available in scripting

- conn** The local storage object in Connectors in an AssemblyLine. It only exists during the Attribute Mapping phase of the Connector's life. See "Attribute Mapping" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.
- work** The data container object of the AssemblyLine. It is therefore accessible in every Connector from the AssemblyLine.
- event** The **event** object is the **work** Entry object when scripting inside EventHandlers, like the **conn** object during Attribute Mapping.
- current**  
Available only in Connectors in Update and Delta mode. Stores the Entry that the Connector read from the data source to determine whether this is an Add or Modify operation.
- error** An Entry object that holds error status information in the following attributes:
- status* (**java.lang.String**)  
**ok** if there is no exception thrown (in this case, this is the error's only attribute). **fail** if an exception is thrown, when the following attributes are also available:
  - exception* (**java.lang.Exception**)  
The **java.lang.Exception** (or some its successor class) object that is thrown
  - class* (**java.lang.String**)  
The name of the exception class (**java.lang.Exception** or some of its successors)
  - message* (**java.lang.String**)  
The error message of the exception
  - operation* (**java.lang.String**)  
The operation type of the Connector (for example, AddOnly, Update, Lookup, Iterator and so forth)
  - connectorname* (**java.lang.String**)  
The name of the Connector whose Hook is being called

## See also

"The attribute object" on page 435.

---

## The FTP object

The FTP object is available as a scriptable object. This object is useful when the FTP Client Connector does not provide the required functionality. See the full documentation in the Javadocs for `com.ibm.di.protocols.FTPBean`.

## Example

```
var ftp = system.getFTP();

if ( ! ftp.connect ("ftpsrvr", "username",
  "password" )
{
  task.logsmg ("Connect failed: " +
    ftp.getLastError());
}

ftp.cd ("/home/user1");
var list = ftp.dir();
while ( list.next() )
{
  if (list.getType() == 1)
```

```

    task.logmsg ("Directory: " +
        list.getName());
    else
        task.logmsg ("File: " + list.getName());
}

ftp.setBinary();
ftp.get ("remotefile", "c:\\localfile");
ftp.put ("c:\\localfile", "remotefile");

```

---

## Main object

The **main** object is the top level thread (see Interface `RSInterface` in the Javadocs). This object has methods for manipulating `AssemblyLine` behavior. The most common methods are:

### **void dump(object)**

Dumps the object to the log file. If object is an `Entry`, Dumps the object to the log file; otherwise, just the class name and `object.toString()`.

### **void logmsg (String loglevel, String msg)**

Alternative version of the `logmsg()` method, with a Log Level parameter. The legal values for Log Level are: "FATAL", "ERROR", "WARN", "INFO", "DEBUG", corresponding to the log levels available for log Appenders. Any unrecognized value is treated as "DEBUG".

### **startAL ( name, initial-work-entry ), startAL ( name, runtime-provided-Connector ), startAL ( name, initial-work-entry, runtime-provided-Connector ), startAL ( name, java.util.Vector )**

Starts the `AssemblyLine` given by the **name** parameter. See also "IBM Tivoli Directory Integrator concepts – The `AssemblyLine`" in *IBM Tivoli Directory Integrator 6.1.1: Users Guide*.

---

## The Search (criteria) object

The **Search (criteria)** object is used by `AssemblyLines` and `Connectors` to specify a generic search criteria. See `com.ibm.di.server.SearchCriteria` in the Javadocs. It is up to each `Connector` how to interpret and translate the search criteria into a `Connector` specific search. The search criteria is a very simple multi-valued object where each value specifies an attribute, operand, and a value.

## Operands

The following operands have been defined for use with the criteria objects.

```

=      Equals
~      Contains
^      Starts with
$      Ends with
!      Not equals

```

## Example

```

for ( i = 0; i < search.size(); i++ ) {
    var sc = search.getCriteria ( i );
    task.logmsg ( sc.name + sc.match + sc.value );
}

```

---

## The shellCommand object

The **shellCommand** object contains the results from a command line process.

On Microsoft Windows platforms, the shell command starts, but you cannot get output or status from the shell command. See `com.ibm.di.function.ExecuteCommand` in the Javadocs for available methods.

For example:

```
var cmd = system.shellCommand ("/bin/ls -l");
if ( cmd.failed() ) {
    task.logmsg ( "Command failed: " + cmd.getError());
} else {
    task.logmsg ( cmd.getOutputBuffer() );
}
```

---

## The status object

The **status** object contains information about an AssemblyLine's Connectors and error codes. It is a synonym to `task.getStats()`

---

## The system object

The **system** object is available as a scriptable object in all scripting contexts and provides a basic set of functions. The Java object is `com.ibm.di.function.UserFunctions`, but linked to the Script object **system**. You can find a complete list of the methods by looking at the Javadocs.

---

## The task object

The **task** object is an instance of class that implements `com.ibm.di.server.TaskInterface` and represents the current thread of execution:

- For AssemblyLines, this is the AssemblyLine thread where you can access AssemblyLine specific information and methods. See class `com.ibm.di.server.AssemblyLine` in the Javadocs.
- For EventHandlers, this is the EventHandler thread where you can access EventHandler specific information and methods. See class `com.ibm.di.eventhandler.Switchboard` in the Javadocs.



---

## Appendix A. Password Synchronization plug-ins

The IBM Tivoli Directory Integrator provides an infrastructure and a number of ready-to-use components for implementing solutions that synchronize user passwords in heterogeneous software environments.

A password synchronization solution built with the IBM Tivoli Directory Integrator can intercept password changes on a number of systems. The intercepted changes can be directed back into:

- The same software systems, or
- A different set of software systems.

Synchronization is achieved through the IBM Tivoli Directory Integrator AssemblyLines, which can be configured to propagate the intercepted passwords to desired systems.

The components that make up a password synchronization solution are: Password Synchronizers, Password Stores, Connectors and AssemblyLines. The Password Synchronizers, Password Stores and Connectors are ready-to-use components included in the IBM Tivoli Directory Integrator. As a result, implementing the solution that intercepts the passwords and makes them accessible from IBM Tivoli Directory Integrator is achieved by deploying and configuring these components.

The following sections describe the specialized password synchronization components that are currently available.

### Password Synchronizers

#### **Password Synchronizer for Windows NT/2000/XP**

Intercepts the Windows login password change.

#### **Password Synchronizer for IBM Tivoli Directory Server**

Intercepts IBM Tivoli Directory Server password changes.

#### **Password Synchronizer for Sun ONE Directory Server**

Intercepts Sun ONE Directory Server password changes.

#### **Password Synchronizer for Domino**

Intercepts changes of the HTTP password for Lotus Notes users.

#### **Password Synchronizer for UNIX and Linux**

Intercepts changes of UNIX and Linux user passwords.

### Password Stores

#### **LDAP Password Store**

Provides the function necessary to store the intercepted user passwords in LDAP directory servers.

#### **MQ Everyplace Password Store**

Provides the function necessary to store user passwords into IBM WebSphere MQ Everyplace.

**Note:** IBM Tivoli Directory Integrator 6.1.1 components can be deployed to take advantage of MQe Mini-Certificate authenticated access. To use these MQe features, it is necessary to download and install IBM WebSphere MQ Everyplace 2.0.1.7 (or higher) and IBM WebSphere MQ Everyplace Server Support ES06. Use of certificate authenticated access prevents an anonymous MQe client Queue Manager and/or application submitting a change password request to the "MQe Password Store Connector" on page 155.

### Specialized Connectors

**MQe Password Store Connector**

Provides the function necessary to retrieve password update messages from IBM WebSphere MQ Everyplace and send them to IBM Tivoli Directory Integrator.

For more information about installing and configuring the IBM Password Synchronization plug-ins, please see the *IBM Tivoli Directory Integrator 6.1.1: Password Synchronization Plug-ins Guide*.

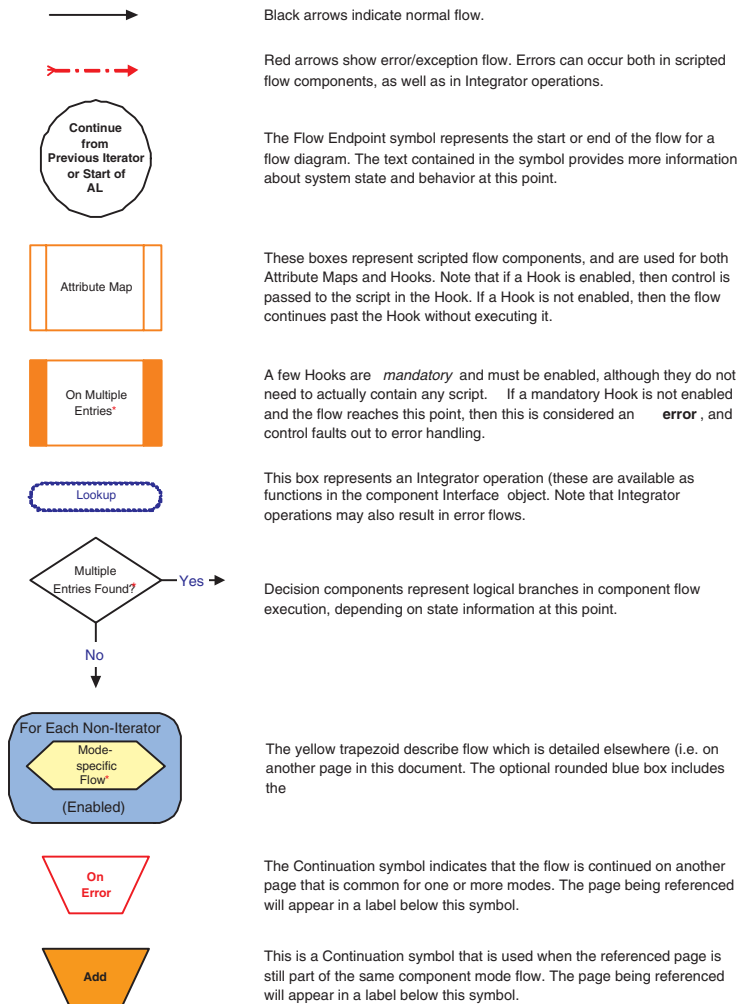


# Appendix B. AssemblyLine and Connector mode flowcharts



## Legend for Diagrams

### Hook Flow diagrams



# AssemblyLine flow

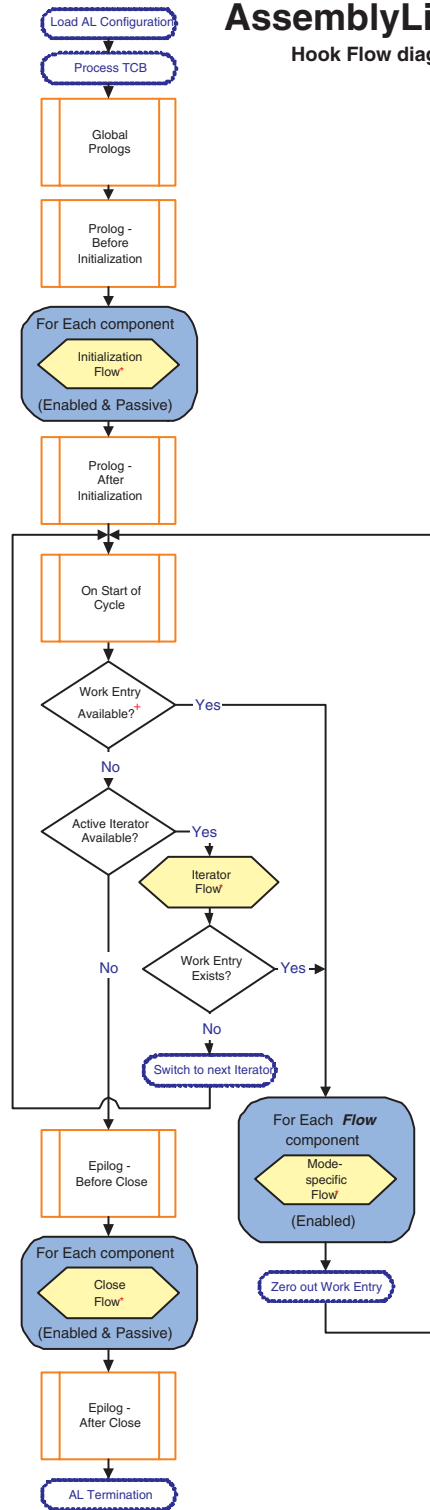
This flow diagram is for an AssemblyLine started by a main thread:



## AssemblyLine Flow Hook Flow diagrams

**\*Flow References**  
These yellow trapezoids represent flows found in the AssemblyLine components.  
**Initialization Flows** are found on the pages entitled **Initialization & Close Flows**  
**Iterator Flow** is described on the page for **Iterator Mode** flow.  
**Mode-specific Flow** can be found on the page(s) for that component Mode.

**+Work Entry Available**  
This test checks to see if there is an **Entry** object which is to be used as **work** for the new cycle.  
This Entry can be provided in a number of ways:  
o an **Initial Work Entry (IWE)**  
o via a call to **task.setWork()**  
o using **system.restartEntry()**



# Connector initialization



## Connector Initialization Flow

Hook Flow diagrams

Available temporary script variables

**Available Objects**

The **workobject** is not available in Initialization Hooks (unless it is provided as an **Initial Work Entry (IWE)**.

As always, if an **Error Hook** is enabled, the error flow continues and does not go to the **Error Flow**.

**Error Handling**

Please note that if the **Prolog On Error Hook** is enabled, then control is passed to back to the AssemblyLine flow: Otherwise, the AssemblyLine aborts.

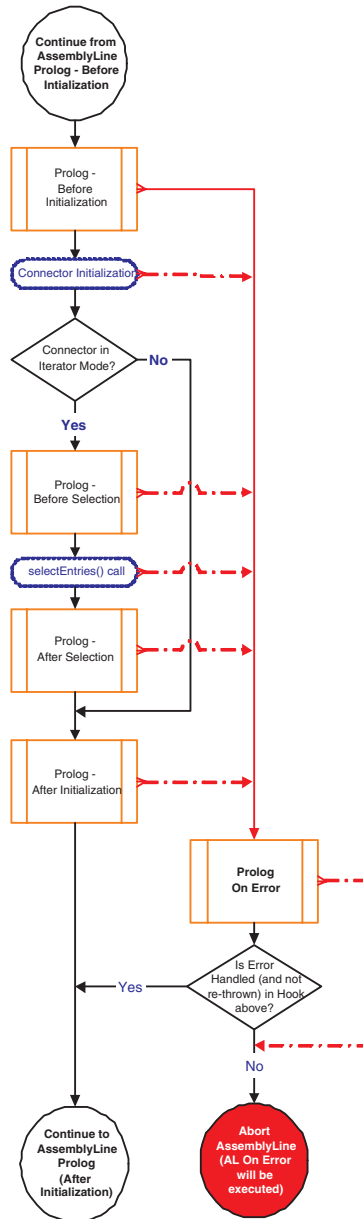
The error condition can be passed on to next On Error Hook (i.e. to the AssemblyLine Error Hook) by re-throwing the exception:

```
throw error.getObject("exception");
```

Furthermore, if an error occurs in an **On Error Hook**, then the AssemblyLine will also **abort**.

The **error** object (of type **Entry**) is available throughout an AssemblyLine and provides information about the error situation through its attributes: **status**, **exception**, **class**, **message**, **operation** and **connectorname**.

The **status** attribute will have the string value **OK** until an error situation arises, at which time it is assigned the value **Fail** and the other attributes are added to **error**.



Hook Flow rev. 6.1  
20060519

# Close flow



## Connector Close Flow Hook Flow diagrams

Available temporary  
script variables

**Available Objects**

Close Hooks will have access to the last **work** Entry processed by the **AssemblyLine**

As always, if an **Error Hook** is enabled, the error flow continues and does not go to the **Error Flow**

**Error Handling**

Please note that if the **Prolog On Error** Hook is enabled, then control is passed to back to the **AssemblyLine** flow; Otherwise, the **AssemblyLine** aborts.

The error condition can be passed on to next **On Error** Hook (i.e. to the **AssemblyLine** Error Hook) by re-throwing the exception:

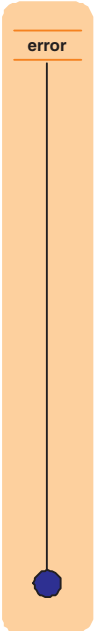
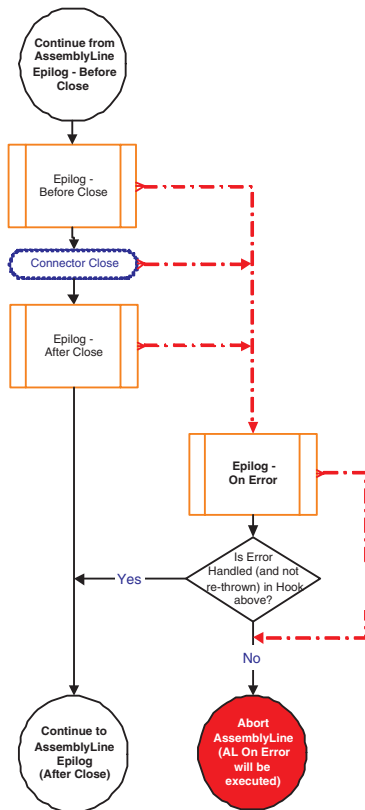
```
throw error.getObject("exception");
```

Furthermore, if an error occurs in an **On Error** Hook, then the **AssemblyLine** will also **abort**.

The error object (of type **Entry**) is available throughout an **AssemblyLine** and provides information about the error situation through its attributes:

**status exception class message operation and connectorname**

The **status** attribute will have the string value **OK** until an error situation arises, at which time it is assigned the value **fail** and the other attributes are added to **error**.



# AddOnly mode



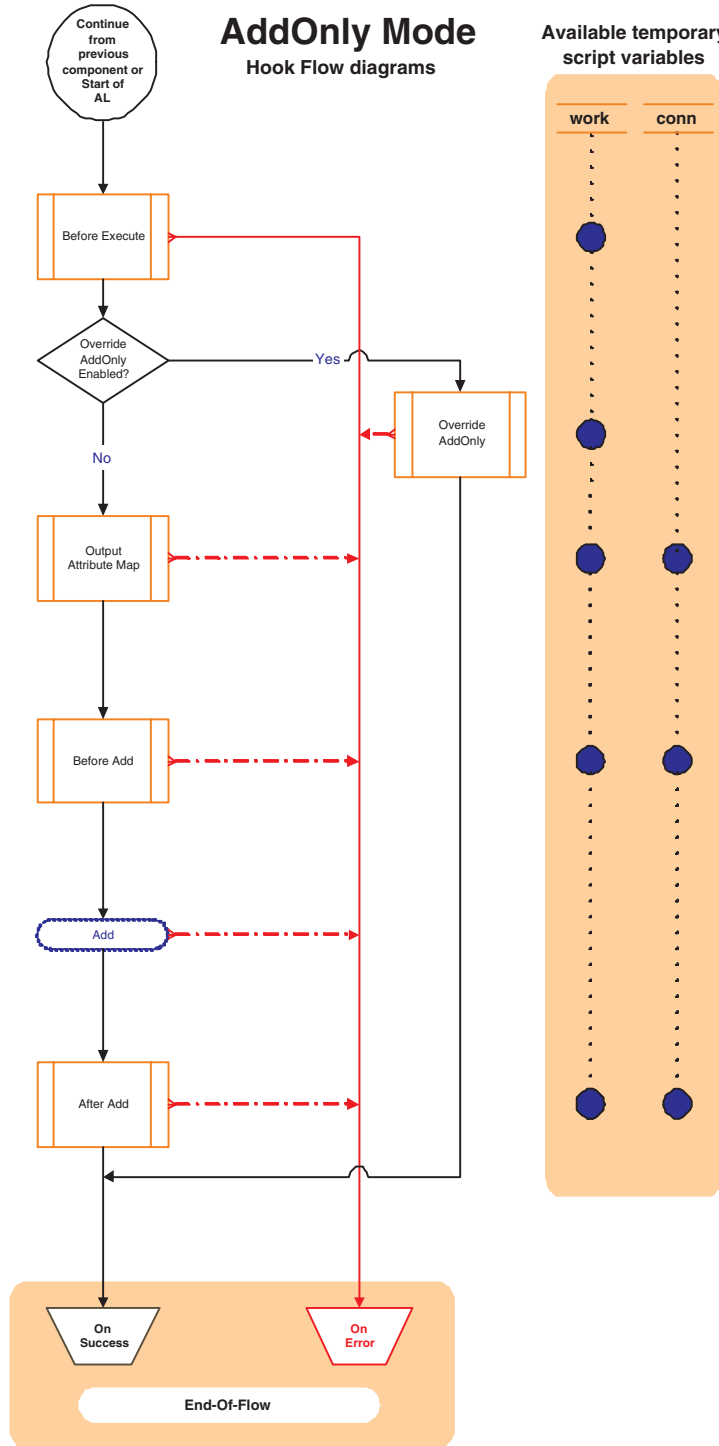
**Available Objects**

As always, `work` gives you access to the attributes that are currently in the AssemblyLine.

The information stored in the `conn` object is written to the data source by the `Add` operation.

## AddOnly Mode Hook Flow diagrams

### Available temporary script variables



Hook Flow rev. 6.1  
20060519

# Call/Reply mode



**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

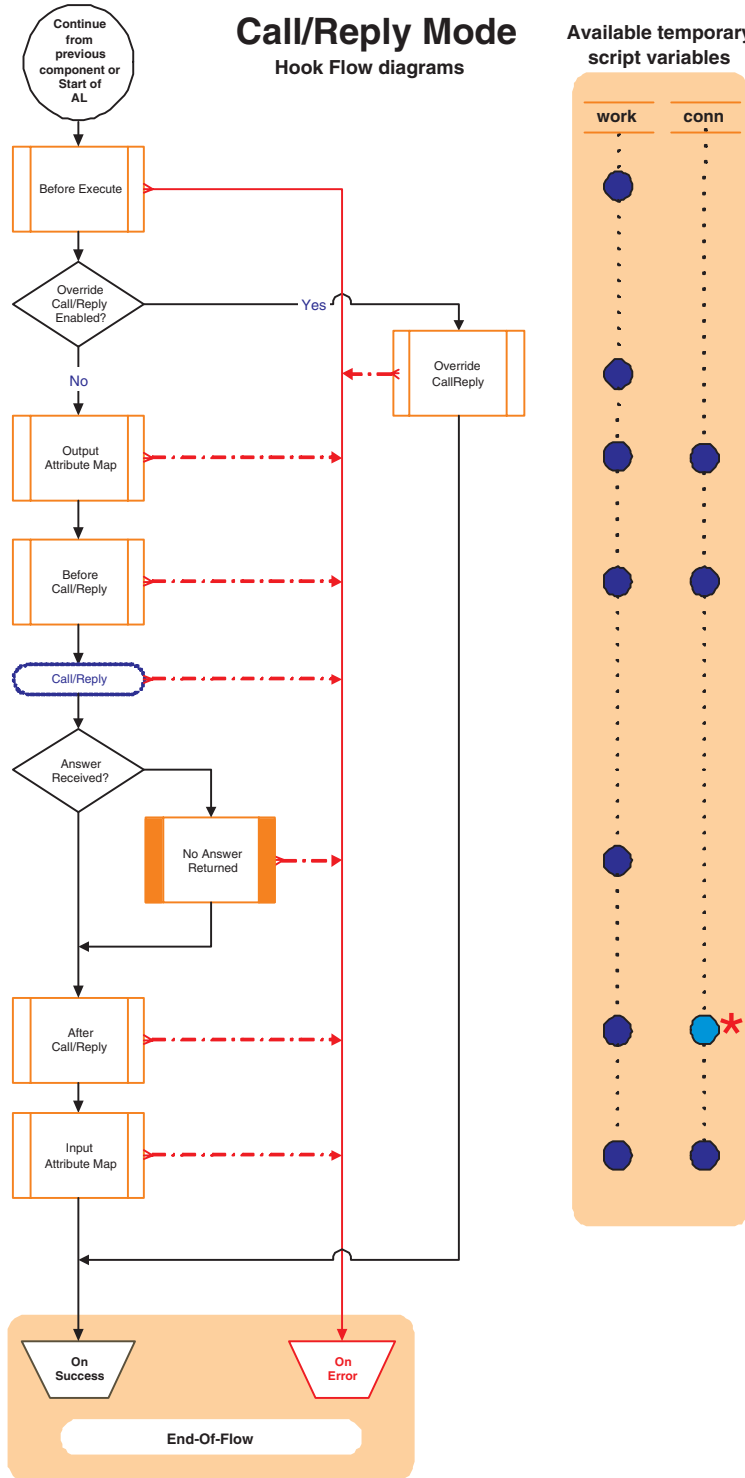
\*The information stored in the **conn** object is slightly different in this mode.

It is important to note that the **conn** object serves two different purposes in **Call/Reply** mode:

- 1) Storing the call attributes/parameters defined in the **Output Attribute Map** to be transmitted by the Call/Reply operation.
- 2) Receiving return attributes/parameters that will be accessed by the **Input Attribute Map** after the Call/Reply operation

## Call/Reply Mode Hook Flow diagrams

### Available temporary script variables



Hook Flow rev. 6.1  
20060519

# Delete mode



## Delete Mode 1/2 Hook Flow diagrams

Available temporary script variables

**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

After the **Build Link Criteria** operation, there is a script object called **search** available which gives you access to this information (i.e. for use in the Override Hook).

The record/entry matching the **Link Criteria** (and that is about to be deleted) is available for scripting as the **conn** object, and Attribute Mapping is carried out to allow your AssemblyLine to use Attributes from the Entry which is to be deleted.

**\*On Multiple Entries**

If more than one record/entry is found that matches the Link Criteria then the On Multiple Entries Hook must also be **enabled**, or this is treated as an **error**.

You can access the set of records/entries found by using either of these two Connector functions:

```
getFirstDuplicateEntry()
or
getNextDuplicateEntry()
```

Each of these functions returns an **Entry** object that can be used to call a Connector interface's data access methods (.update(), delete(), etc.).

If you wish to proceed with the delete flow/operation, then you must set the current Entry with the following Connector function:

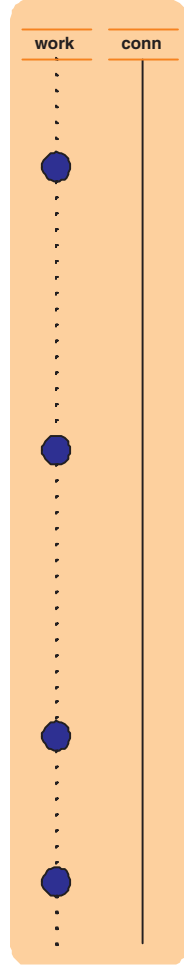
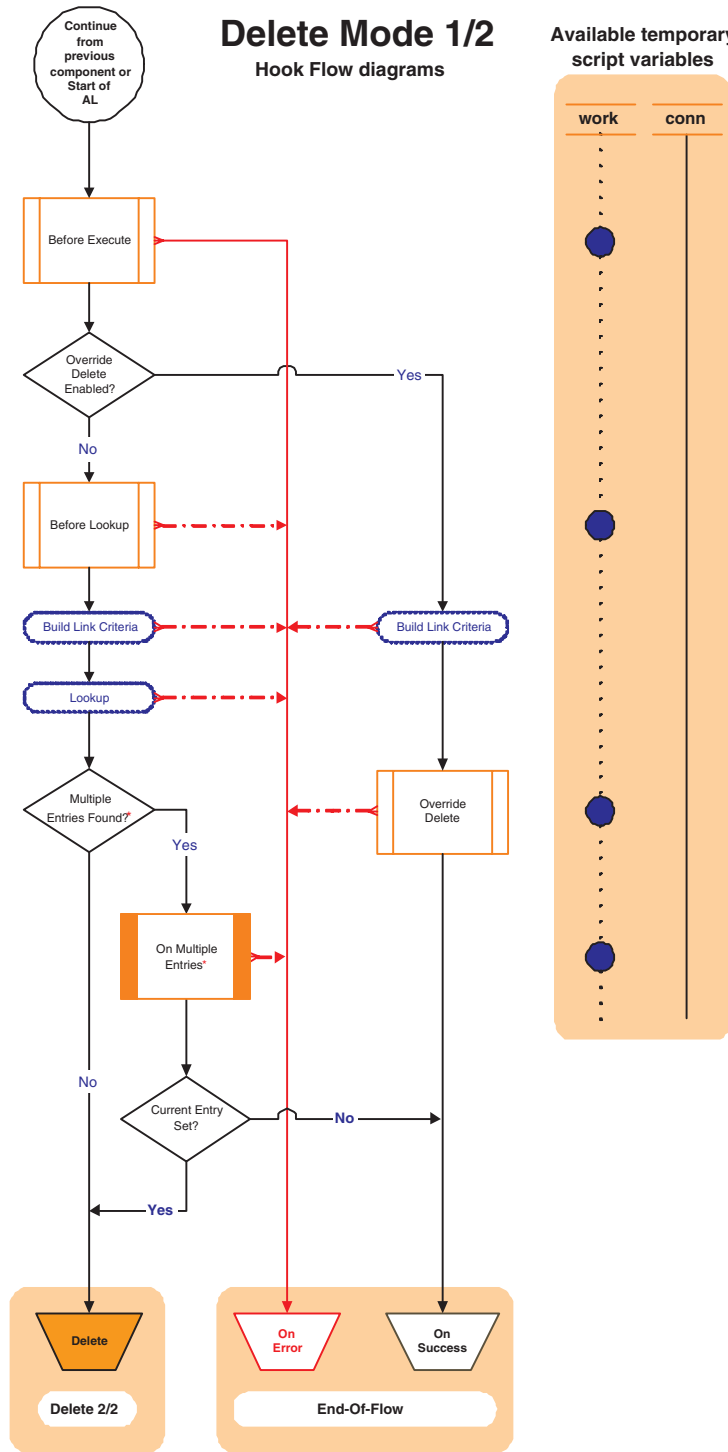
```
myConnector.setCurrent(myEntry)
```

If you do not set a current Entry, then execution will continue to On Success, bypassing the rest of the mode-specific flow.

**Note:**

Data sources behave differently when multiple Entries are to be handled.

Even if you select a specific Entry as described above, it is not recommended that you continue with the delete flow, as this may result in an error, or that the operation is performed on multiple entries.

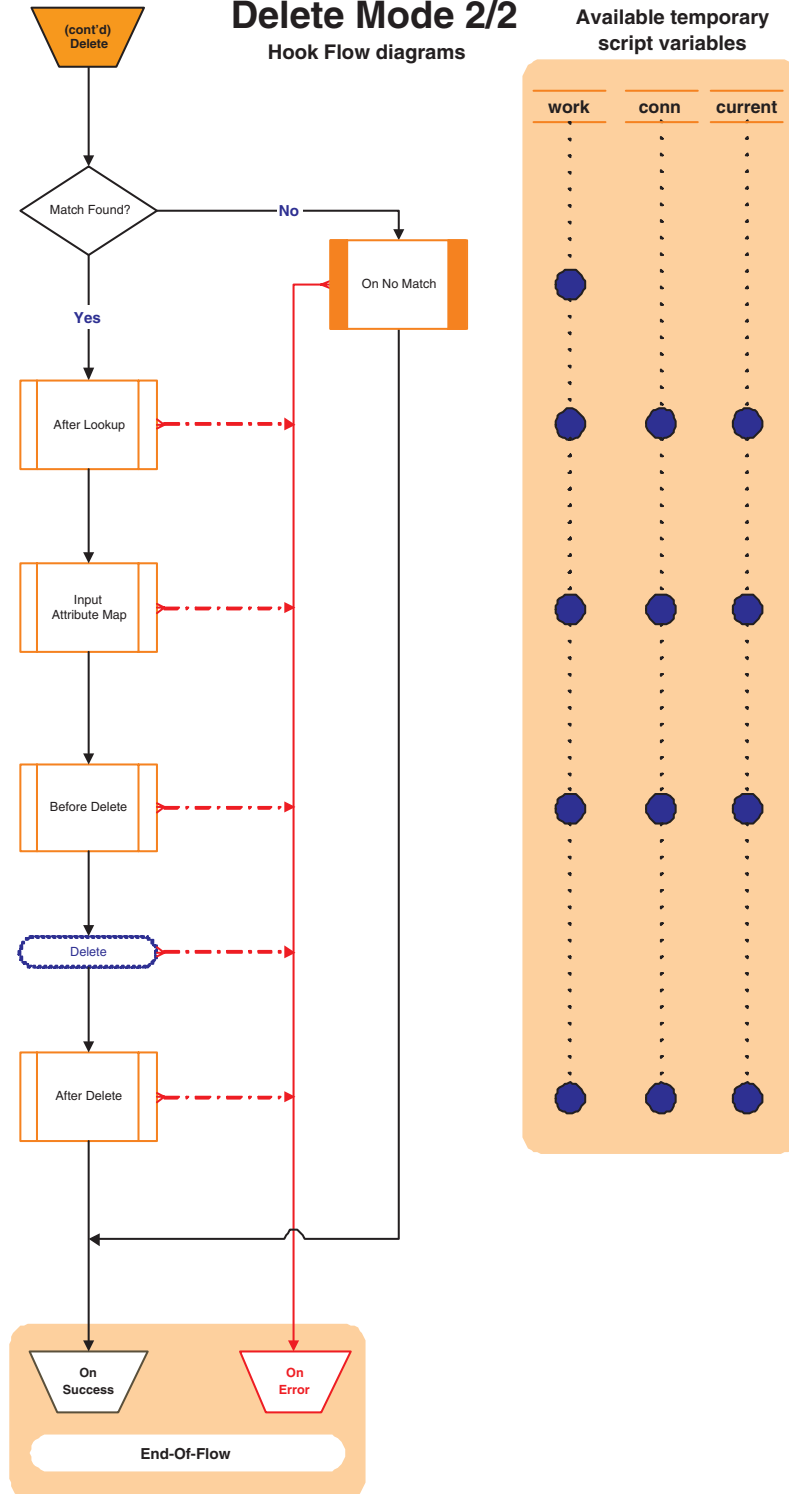


Hook Flow rev. 6.1  
20060519

## Delete Mode 2/2

Hook Flow diagrams

Available temporary script variables



Hook Flow rev. 6.1  
20060519



# Delta Mode



**Available Objects**

As always, `work` gives you access to the attributes that are currently in the AssemblyLine.

After the **Build Link Criteria** operation, there is a script object called `search` available which gives you access to this information (e.g. for use in the Override Hook).

**\* Valid Operation Code**

By default, an **exception** is thrown if Delta mode detects that the work Entry does not have a valid **operation code** (for example, `generic`). Operation code detection occurs after the **Before Execute** Hook. Delta mode can be configured to *ignore* these Entries instead.

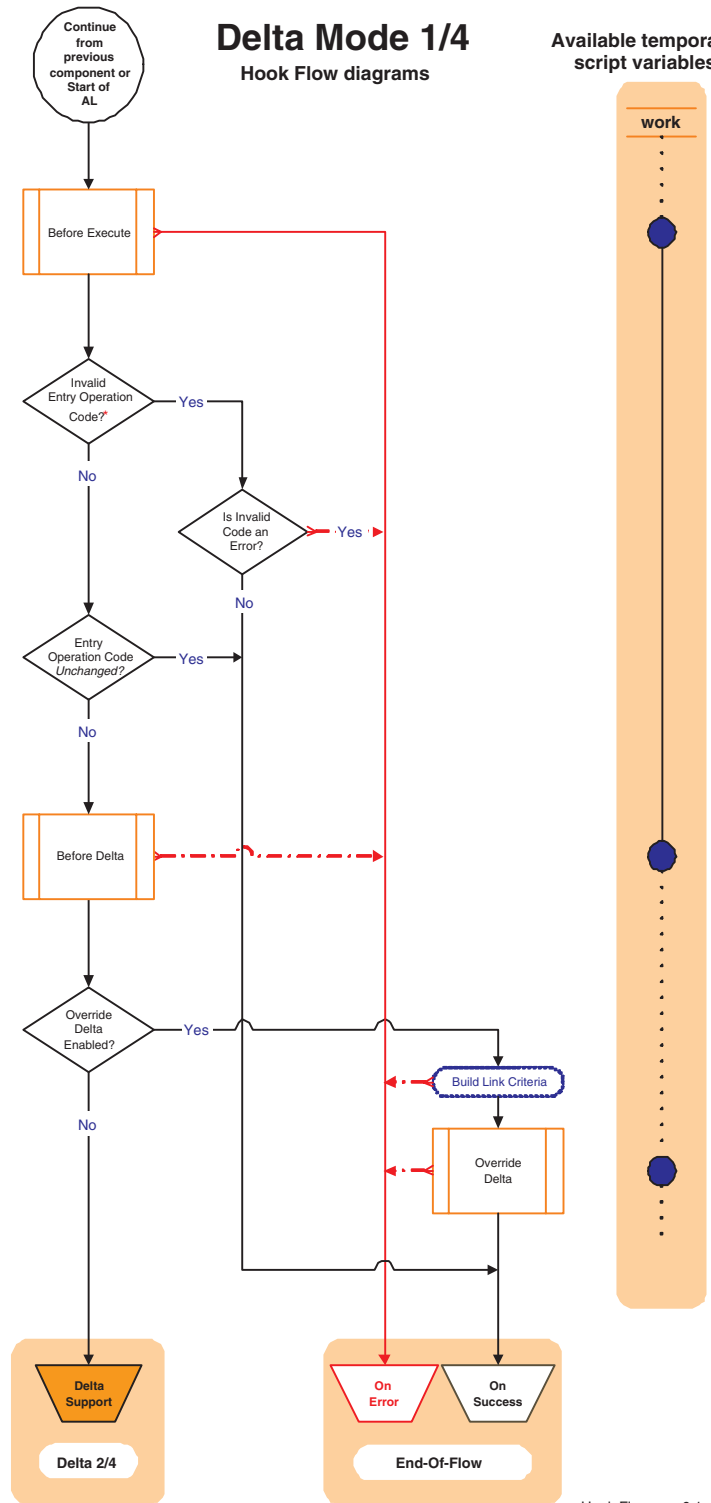
**Delta Application**

During Delta processing, the necessary steps are taken to prepare for applying the detected changes as efficiently as possible.

For example, **multi-value Attributes** require special handling so that **value-level Delta operation codes** are applied correctly.

## Delta Mode 1/4 Hook Flow diagrams

Available temporary script variables



Hook Flow rev. 6.1  
20060519

## Delta Mode 2/4 Hook Flow diagrams

Available temporary script variables

### # Incr. Mod. possible?

The Connector checks to see if the underlying system supports incremental modifications.

For the LDAP Connector, this will always be Yes.

For the JDBC Connector the answer is currently always be No.

### \* On Multiple Entries

If more than one record/entry is found that matches the Link Criteria then the On Multiple Entries Hook must also be **enabled** or this is treated as an **error**.

You can access the set of records/entries found by using either of these two Connector functions:

```
getFirstDuplicateEntry()
or
getNextDuplicateEntry()
```

Each of these functions returns an **Entry** object that can be used to call a Connector Interface's data access methods (.update(), .delete(), etc.).

In addition, **conn** may be set to the desired **Entry** object by calling the Connector's **setCurrent()** function:

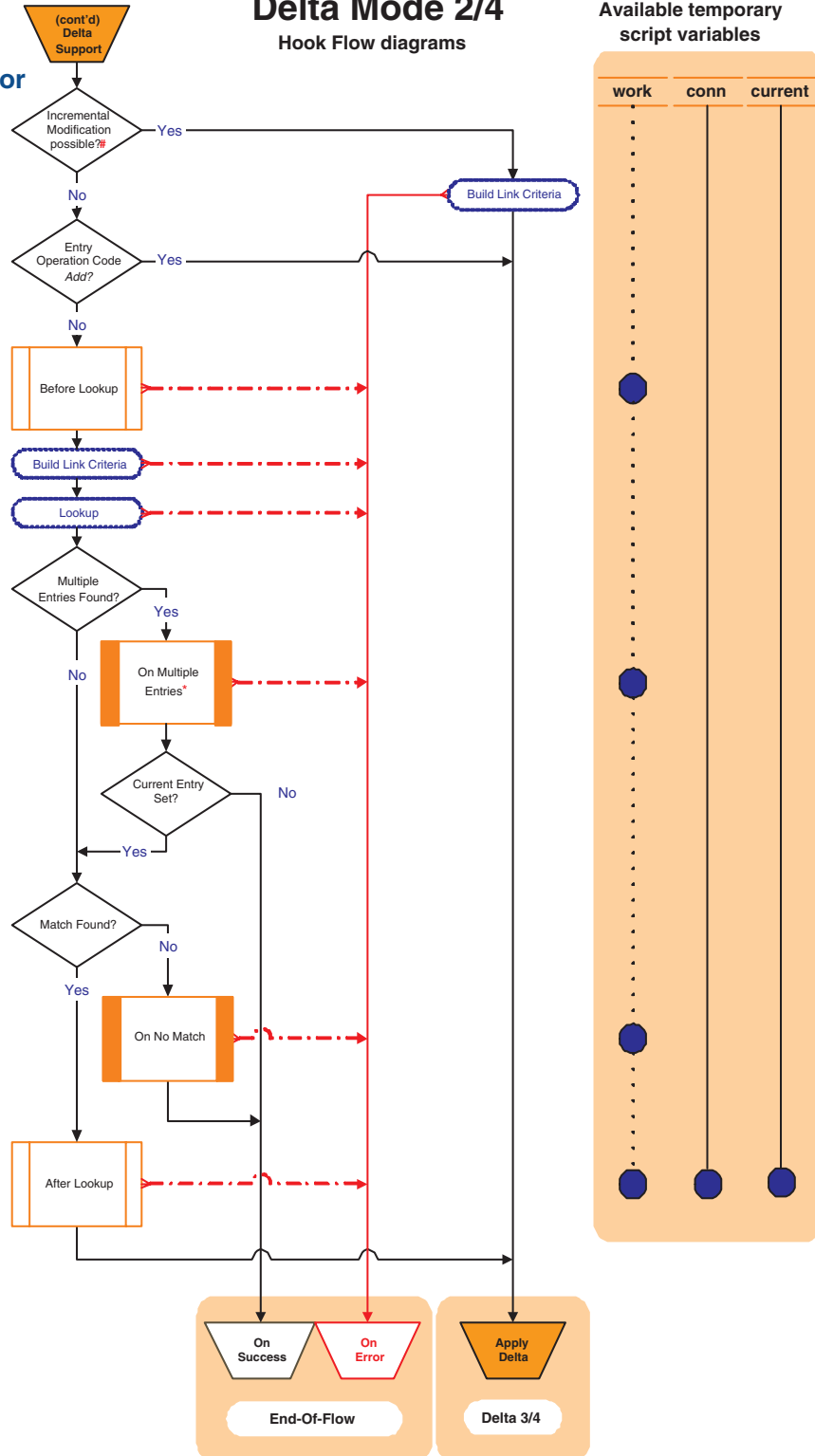
```
myConnector.setCurrent(myEntry)
```

If no Entry object is set, then execution will continue to **On Success** skipping the rest of the mode-specific flow.

#### Note:

Please note that data sources (and therefore related Connectors) behave differently when multiple Entries are to be handled.

Even if you set a specific Entry as described above, it is not recommended that you continue with the delta operation, as this may result in an error, or that the operation is performed on multiple entries.



Hook Flow rev. 6.1  
20060519



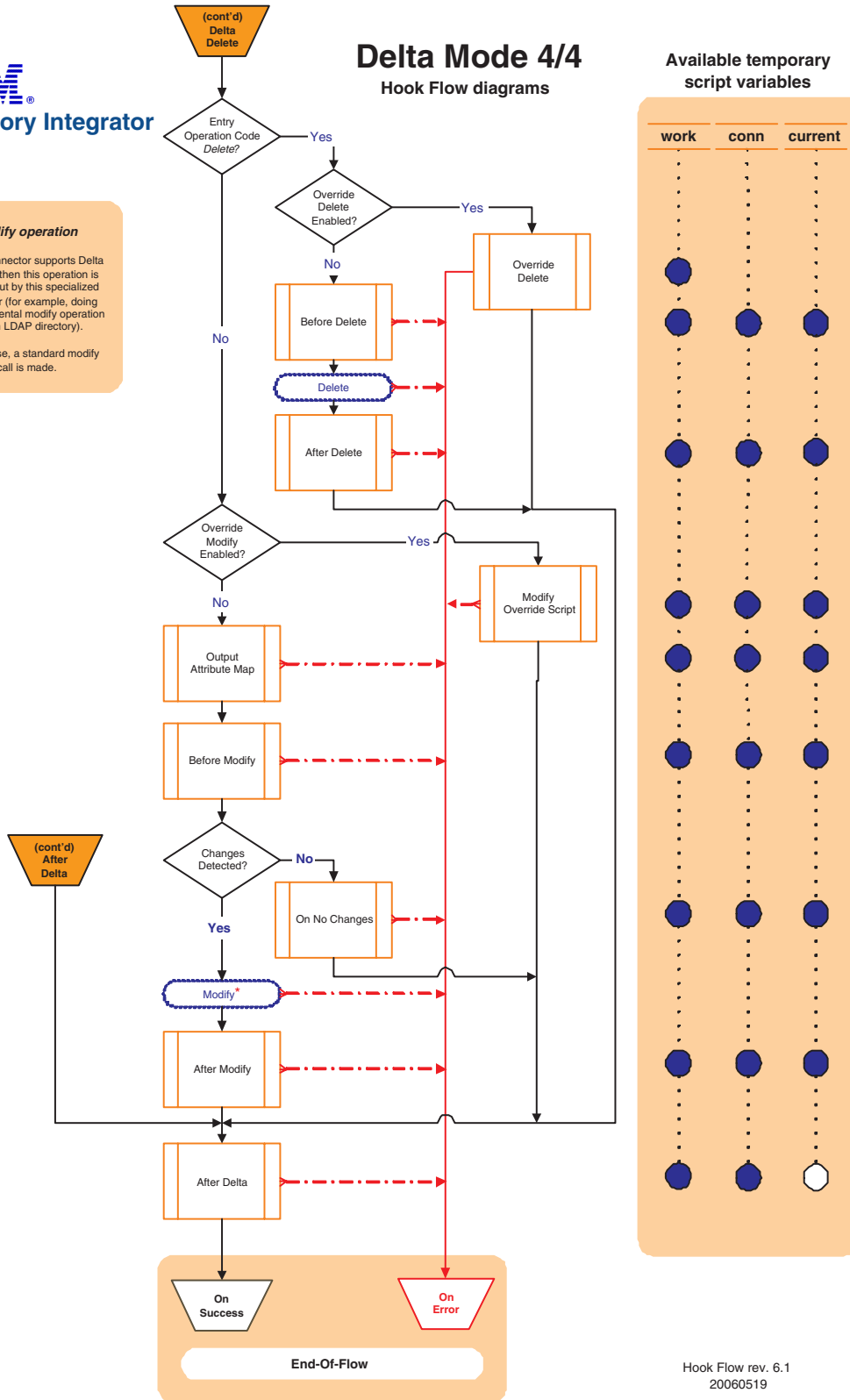
## Delta Mode 4/4 Hook Flow diagrams

### Available temporary script variables

**\*Modify operation**

If the Connector supports Delta directly, then this operation is carried out by this specialized behavior (for example, doing an incremental modify operation for an LDAP directory).

Otherwise, a standard modify call is made.



| work | conn | current |
|------|------|---------|
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ●       |
| ●    | ●    | ○       |

# Iterator mode



### Available Objects

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

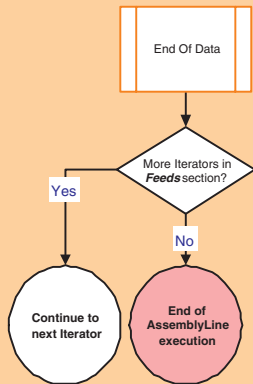
The data read in by each **GetNext** operation is available in the **conn** object.

#### Note:

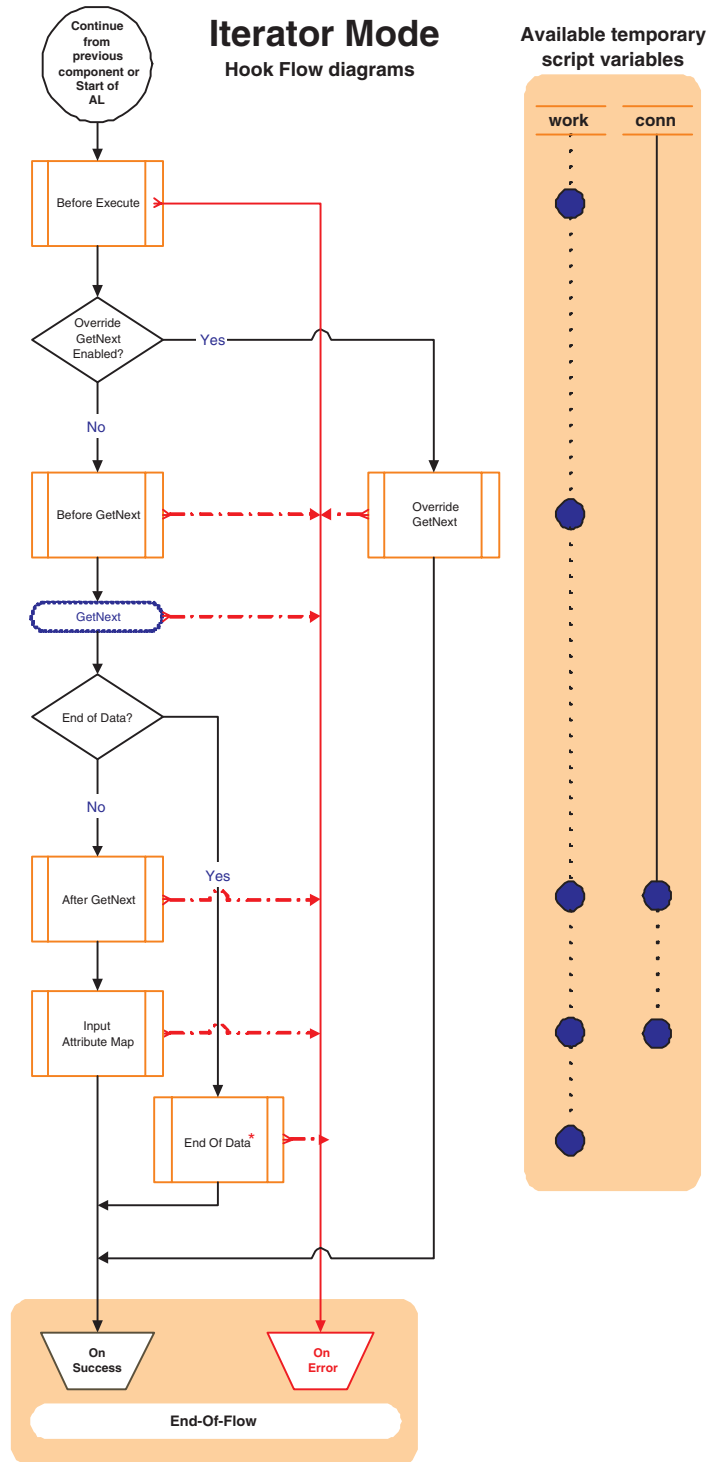
If a Connector in Iterator mode detects the presence of a valid **work** object at the start of its execution - for example, that there is another Iterator in front of this one in the same AssemblyLine, or that the initial **work** Entry has been passed into the AssemblyLine from a calling process or system - then this Connector will not be executed, passing instead this Entry to the next Connector in the AssemblyLine.

The sidebar below illustrates what happens when an Iterator reaches its end-of-data. At this point it will not pass a **work** object to the next Connector, which in the case of another Iterator, will signal it to begin its own iteration.

\*After the **End Of Data** hook, execution flow continues as shown below:



## Iterator Mode Hook Flow diagrams



Hook Flow rev. 6.1  
20060519

# Lookup mode



### Available Objects

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

After the **Build Link Criteria** operation, there is a script object called **search** available which gives you access to this information (i.e. for use in the Override Hook).

The record/entry matching the **Link Criteria** is available through the **conn** object.

### \*On Multiple Entries

If more than one record/entry is found that matches the Link Criteria then the On Multiple Entries Hook must also be **enabled**, or this is treated as an **error**.

During this hook, **conn** may be set to the desired **Entry** object by calling the Connector's **setCurrent()** function:

```
myConnector.setCurrent(myEntry)
```

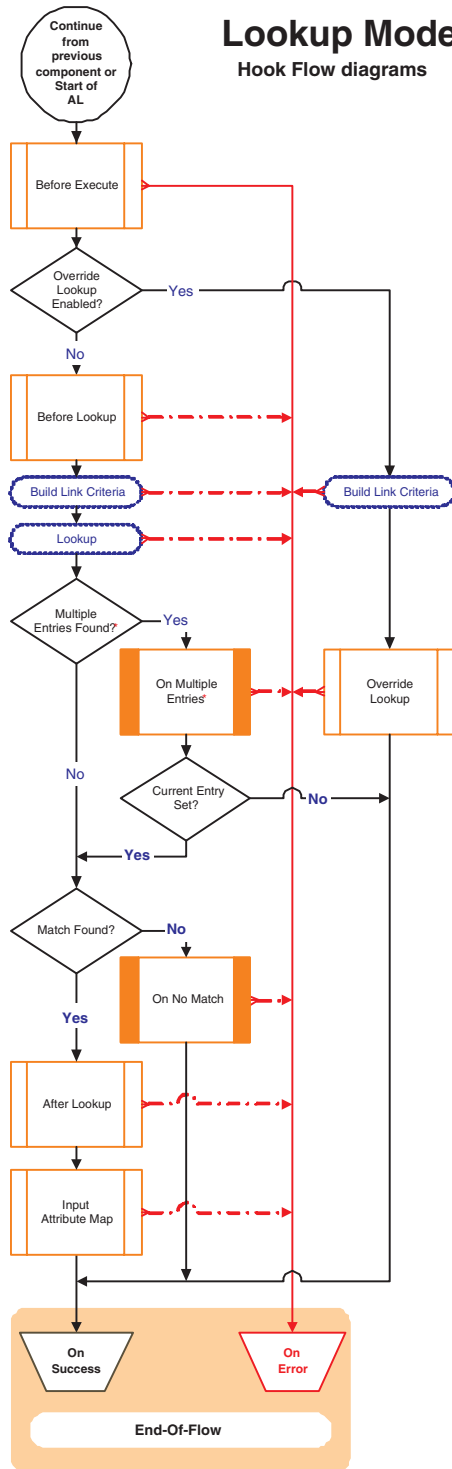
You can access the set of records/entries found by using either of these two Connector functions:

```
getFirstDuplicateEntry()
or
getNextDuplicateEntry()
```

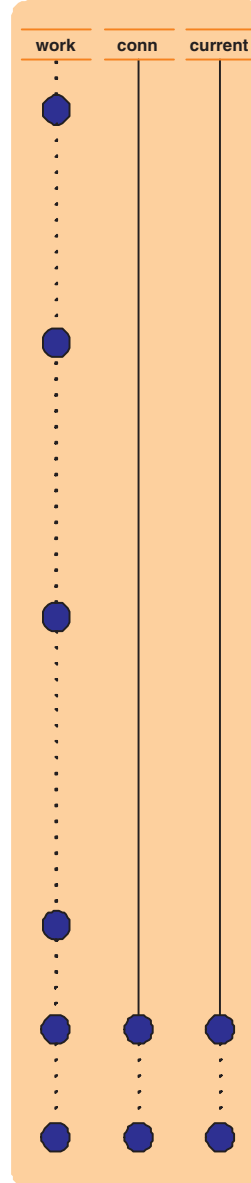
Each of these functions returns an **Entry** object that can be used in the **setCurrent()** call.

If **setCurrent()** is not called (e.g. no current entry is set) then the flow is passed on to **On Success** skipping the rest of the mode-specific flow.

## Lookup Mode Hook Flow diagrams



### Available temporary script variables



Hook Flow rev. 6.1  
20060519

# Server Mode



## Server Mode Hook Flow diagrams

### Available temporary script variables

**Available Objects**

The only temporary Entry object is **conn**, which is available in the **After Accepting Connection** Hook.

This Entry contains a single Attribute called

**connectorInterface**

Its only value is a reference to the Connector Interface that will be paired up with the **Flow** component list in **Iterator Mode** to feed it with event data.

**Server Behavior**

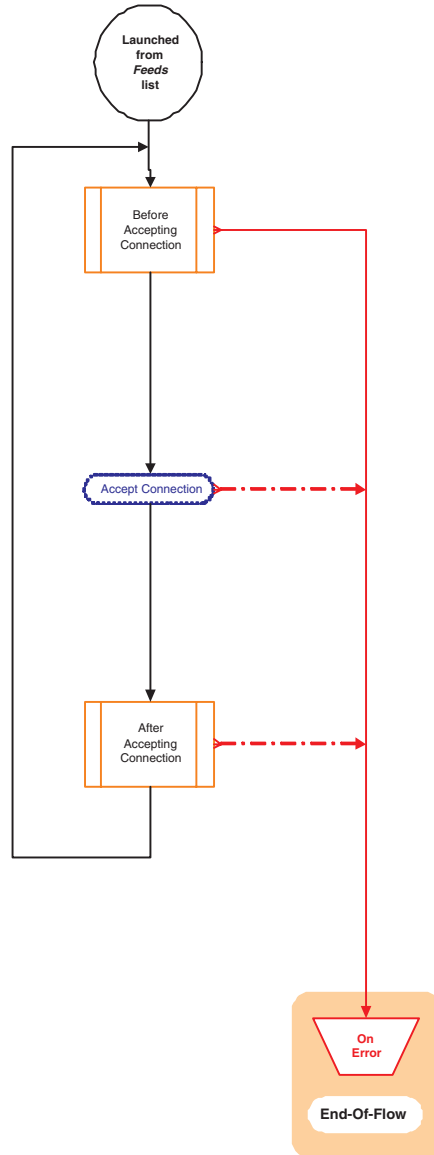
**Server Mode** Connectors do *not* run exclusively like Iterators do. Instead, each is launched as a separate process in **event listening** mode and control is passed to the next **Feeds** Connector.

When an event is detected (for example, a client attempts to connect) then the Connector creates a **clone** of itself in **Iterator Mode** once the **After Accepting Connection** Hook has completed.

This cloned Iterator is then paired up with the **AssemblyLine Flow** component list (possibly from the **AL Pool**) and Hook flow continues as with standard **Iterator** mode.

Furthermore, once the **Flow** section of the **AssemblyLine** completes, control is passed to the **Server Response** logic which then creates and sends the required reply to the caller/client system.

The Response Hook flow is detailed on the page entitled **Server Response**



Hook Flow rev. 6.1  
20060519

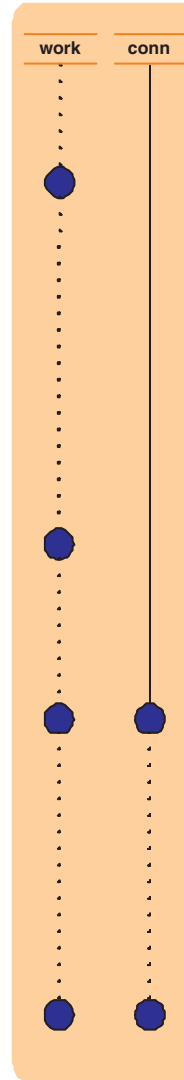
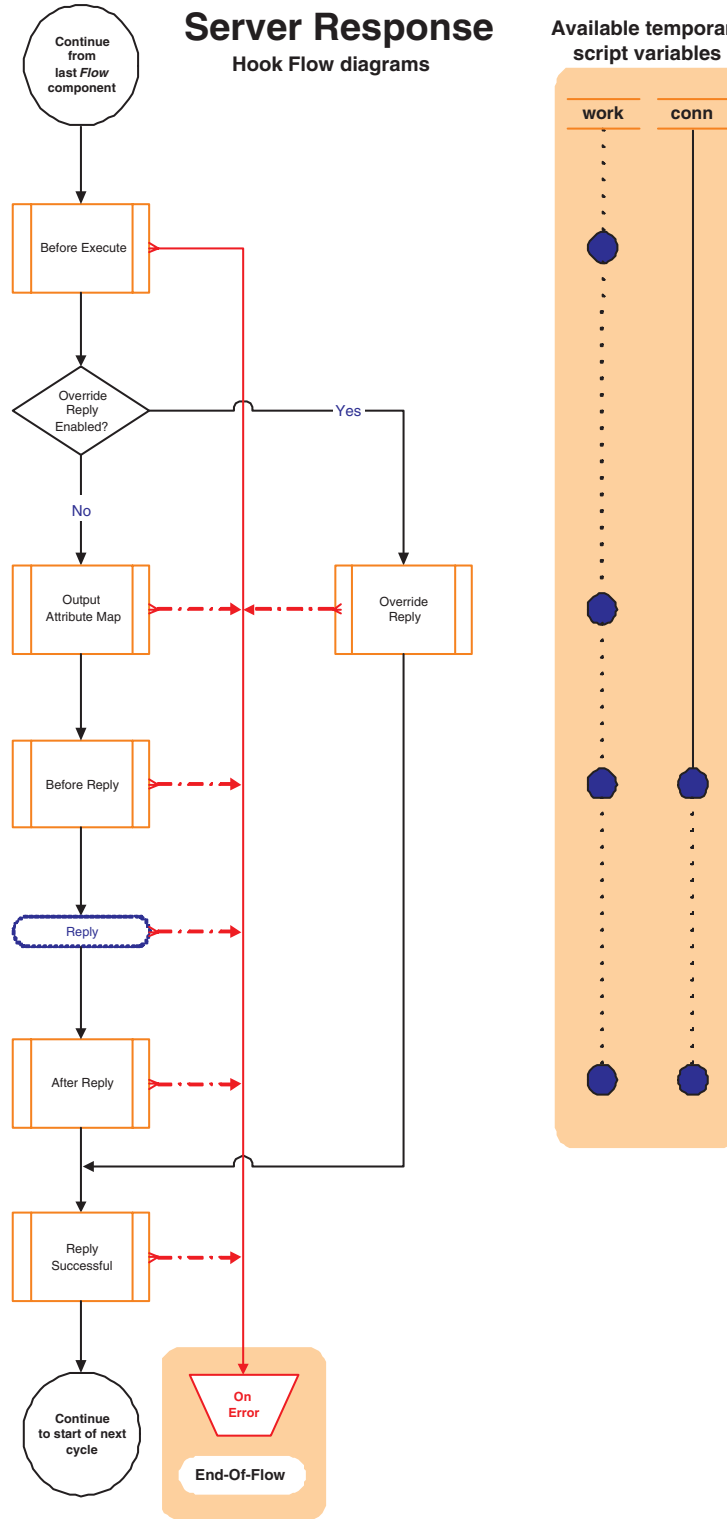
**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

The information stored in the **conn** object is sent to the data source by the **Reply** operation.

## Server Response Hook Flow diagrams

Available temporary script variables





# Update mode



## Update Mode 1/3 Hook Flow diagrams

Available temporary script variables

**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

After the **Build Link Criteria** operation, there is a script object called **search** available which gives you access to this information (e.g. for use in the Override Hook).

**\*On Multiple Entries**

If more than one record/entry is found that matches the Link Criteria then the On Multiple Entries Hook must also be **enabled**, or this is treated as an **error**.

You can access the set of records/entries found by using either of these two Connector functions:

```
getFirstDuplicateEntry()
or
getNextDuplicateEntry()
```

Each of these functions returns an **Entry** object that can be used to call a Connector's data access methods (.update(), .delete(), etc.).

In addition, **conn** may be set to the desired **Entry** object by calling the Connector's **setCurrent()** function:

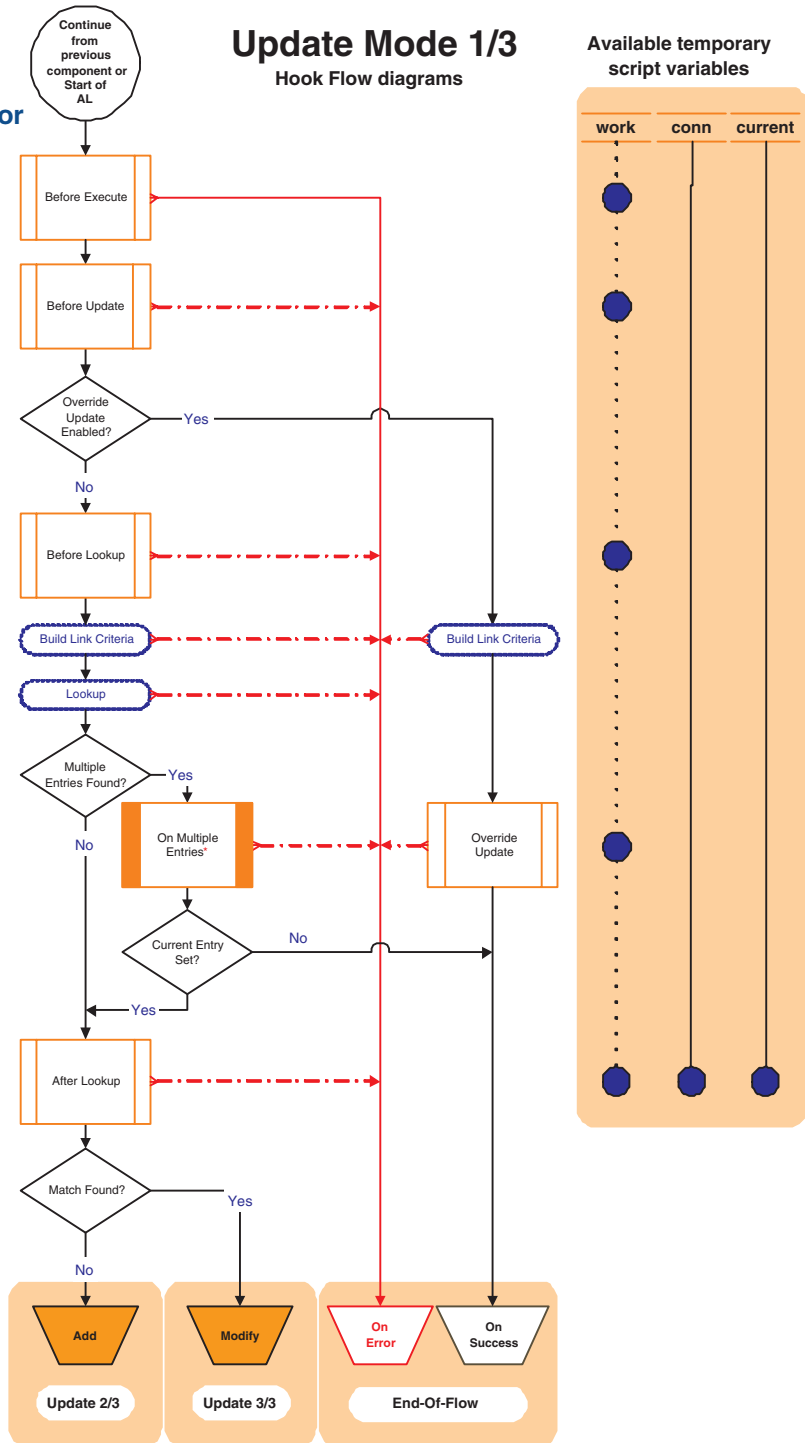
```
myConnector.setCurrent(myEntry)
```

If no Entry object is set, then execution will continue to **On Success**, skipping the rest of the mode-specific flow.

**Note:**

Please note that data sources (and therefore related Connectors) behave differently when multiple Entries are to be handled.

Even if you set a specific Entry as described above, it is not recommended that you continue with the update operation, as this may result in an error, or that the operation is performed on multiple entries.



Hook Flow rev. 6.1  
20060519

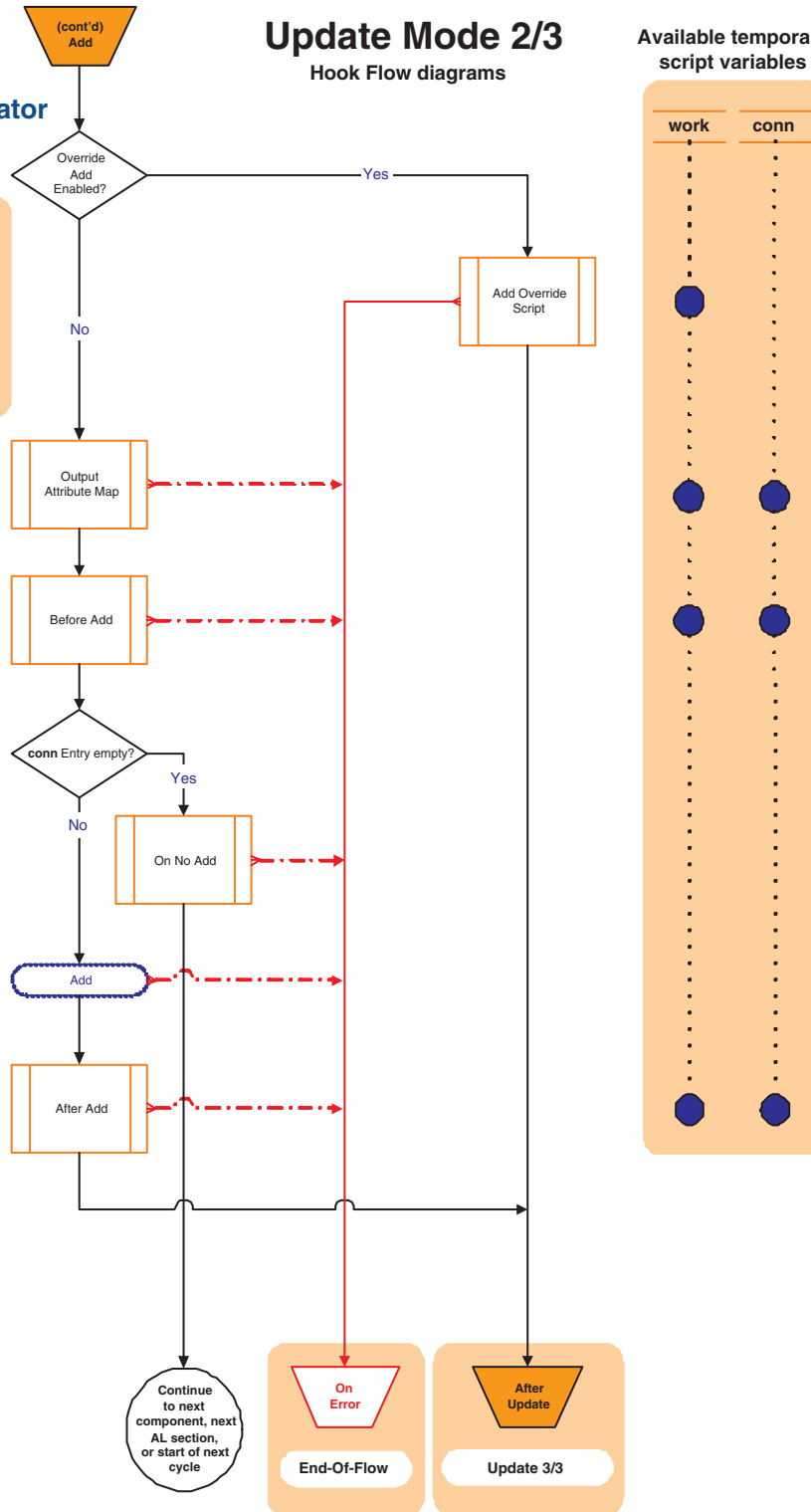
## Update Mode 2/3 Hook Flow diagrams

Available temporary script variables

**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

If the Update results in an **Add** operation, **conn** holds the data that is written to the data source.





# End-of-flow for all modes



## End-Of-Flow for All Connector Modes

Hook Flow diagrams

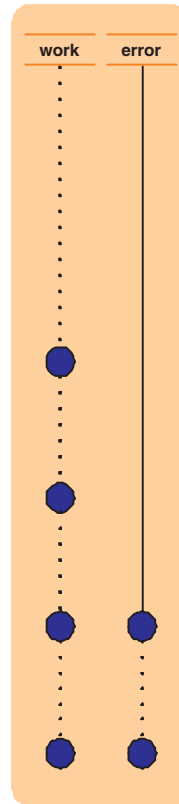
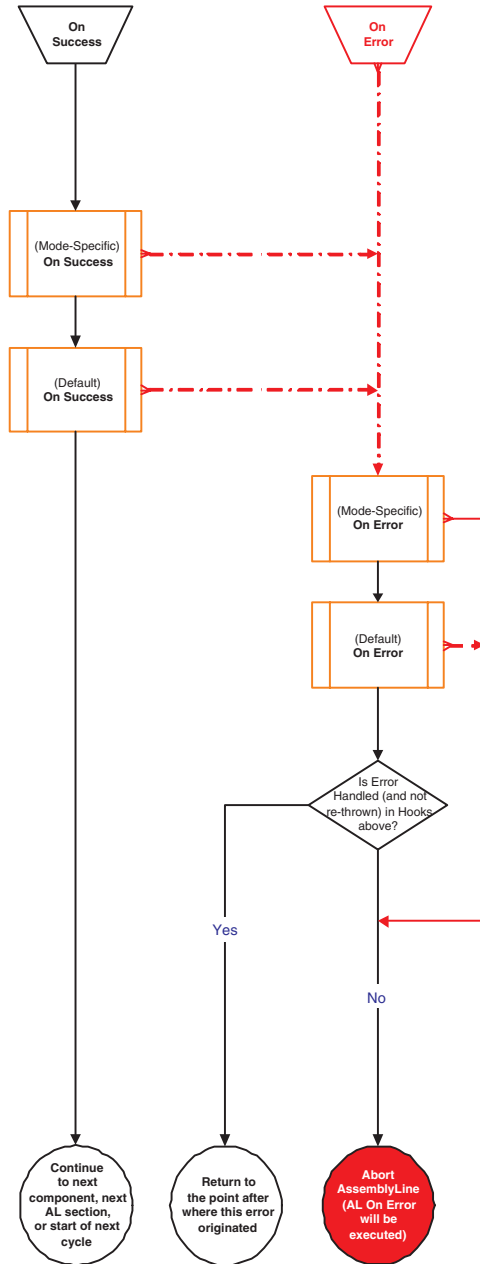
Available temporary script variables

**Available Objects**  
As always, **work** gives you access to the attributes that are currently in the AssemblyLine.  
The **conn** and **current** objects are available in the **On Error** and **On Success** Hooks if they were present previously in the flow

**End-Of-Flow**  
This flow applies to all components that either terminate normally (e.g. successfully) or due to an error.

**Error Handling**  
Please note that if either **On Error** Hook is enabled, then control is passed to the next component, as if the Connector had terminated successfully. Otherwise, the AssemblyLine **aborts**.  
The error condition can be passed on to next On Error Hook (either the Default for the Connector, or the AssemblyLine Error Hook) by re-throwing the exception:  
`throw error.getObject("exception");`  
Furthermore, if an error occurs in an **On Error** Hook, then the AssemblyLine will also **abort**.  
The **error** object (of type **Entry**) is available throughout an AssemblyLine and provides information about the error situation through its attributes: **status**, **exception class**, **message operation** and **connectorname**.  
The **status** attribute will have the string value **OK** until an error situation arises, at which time it is assigned the value **fail** and the other attributes are added to **error**.

**AssemblyLine End-of-Flow**  
If the AssemblyLine completes without unhandled errors, the AssemblyLine **On Success** Hook is invoked.  
Otherwise, if an error has occurred then control is passed to the AssemblyLine **On Error** Hook.



Hook Flow rev. 6.1  
20060519

# Connector Reconnect



## Connector Reconnect Hook Flow diagrams

**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine..

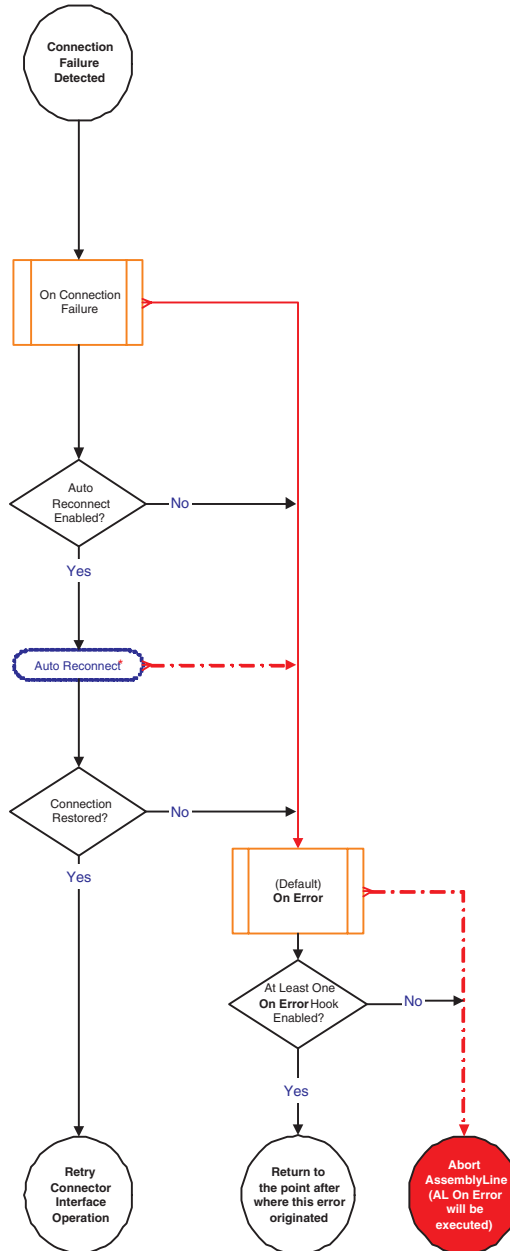
The **error** object (of type **Entry**) is available throughout an AssemblyLine, and provides information about the an error situation through its attributes: **status exception class message operation and connectname**

The **status** attribute will have the string value **OK** until an error situation arises, at which time it is assigned the value **fail** and the other attributes are added to **error**.

**\* Auto Reconnect**

The Auto Reconnect feature is configured through the parameters found in the Connector **Reconnect** tab.

These parameters control the maximum number of times a reconnect will be tried, as well as the number seconds to wait between each attempt.



Hook Flow rev. 6.1  
20060519

# Function Components



**Available Objects**

As always, **work** gives you access to the attributes that are currently in the AssemblyLine.

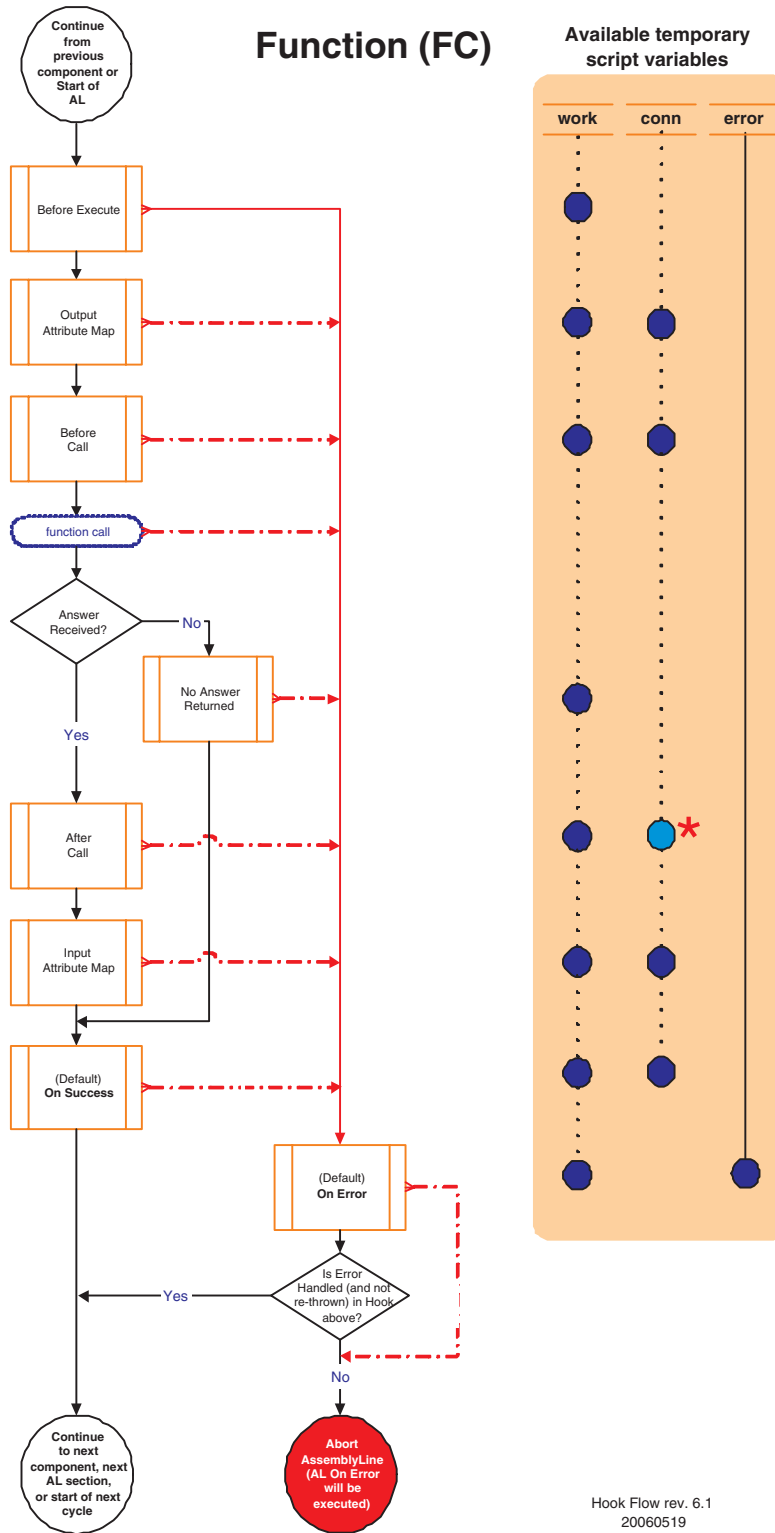
\*The information stored in the **conn** object changes during FC operation.

It is important to note that the **conn** object serves two different purposes in a **Function**:

- 1) Storing the call attributes/parameters defined in the **Output Attribute Map** to be transmitted by the Function call operation,
- 2) Receiving return attributes/parameters that will be mapped in by the **Input Attribute Map** after the Function call operation

## Function (FC)

### Available temporary script variables



Hook Flow rev. 6.1  
20060519

---

## Appendix C. Server API

---

### Overview

The IBM Tivoli Directory Integrator 6.1.1 Server API provides a set of programming calls that can be used to develop solutions and interact with the IBM Tivoli Directory Integrator (TDI) Server locally and remotely. It also includes a management layer that exposes the Server API calls through the Java Management Extensions (JMX) interface.

The Server API includes calls that allow you to:

- Get information about the TDI Server
- Get information about components installed on the Server
- Read, Modify and Write configurations loaded by the Server
- Create and Load new configurations on the Server
- Start, Query and Stop AssemblyLines and EventHandlers
- Cycle manually through AssemblyLines
- Register for and receive notifications for Server events
- Register for and receive AssemblyLines and EventHandlers log messages

All calls can be invoked locally from the TDI Server JVM, and remotely from another JVM (on the local or a remote network machine), through RMI:

#### Local access

This type access includes scripting in AssemblyLine or EventHandler hooks and also using the API from new components (Connectors, EventHandlers) implemented in Java and deployed on the Server.

#### Remote access:

This type of access enables the implementation of solutions that remotely connect to TDI and manage processes within TDI or/and build business logic on top of TDI. It could be an application dedicated solely to TDI or an application that uses TDI to accomplish some of its goals.

A management layer of the Server API exposes the Server API calls through JMX. This provides for Server manageability and enables you to plug TDI into a managing infrastructure that speaks JMX. The JMX interface is accessible:

- Locally, as defined in the JMX 1.2 specification
- Remotely, through RMI as defined by the JMX Remote API 1.0 specification

The notifications issued by the Server API internal engine are also available as JMX notifications.

Remote access to the Server API (including the JMX Remote API) is secured by using SSL with client and server authentication.

The different methods that can be used to access the TDI Server API are depicted on the diagram below:

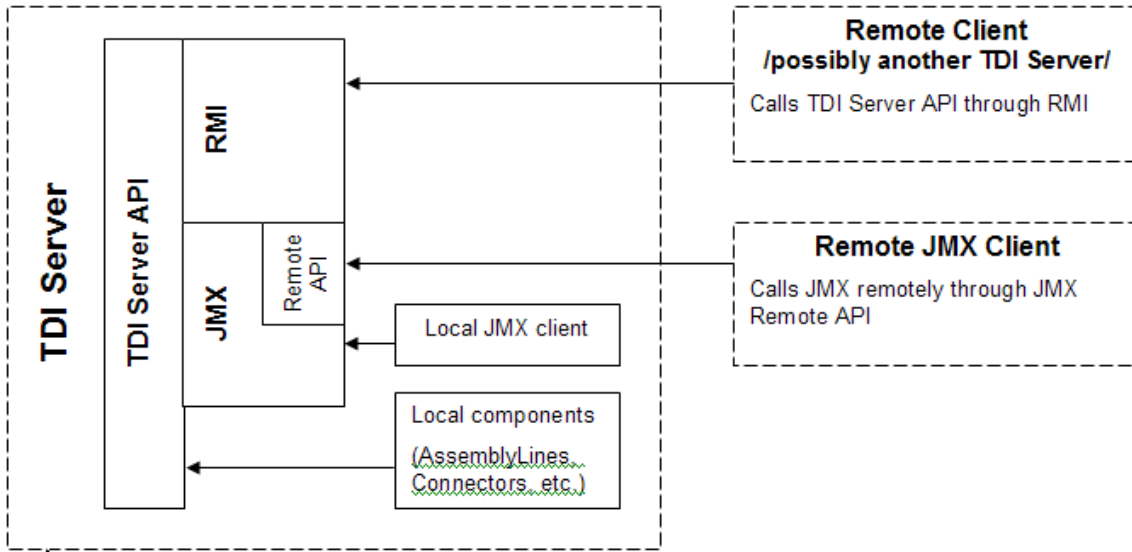


Figure 5.

## Sample use case

In this sample scenario, a client (a stand-alone Java application, for example) needs to start an AssemblyLine on TDI Server. The client could use the Server API and access it remotely through the RMI interface, using the Server API RMI client library.

In accordance with the security model described in “Security” on page 467, the client will first create a session to the remote TDI Server using its own certificate or custom authentication. The Server will successfully authenticate the client if it has the client certificate in its trust store or custom authentication succeeds. If the authentication is successful the client will be provided with an object that represents an entry point for calling Server API methods. Using that object the client will invoke the call for starting an AssemblyLine passing parameters that specify which AssemblyLine needs to be started.

Before actually executing the method the Server API will check whether the client is authorized to execute that method – the identity of the client is determined through the client certificate used to establish the SSL channel or with provided credentials for the custom authentication. If the client is allowed to start this AssemblyLine the method will be executed and the AssemblyLine will be started; otherwise, the method will not be executed and an error (exception) will be sent back to the client indicating that it is not authorized to perform this operation.

---

## Local and Remote Server API interfaces

The Server API provides two sets of interfaces: one for local use and one for remote use. Both sets of interfaces provide the same calls and functionality, but reside in different Java packages.

The package `com.ibm.di.api.local` contains the interfaces for local access and `com.ibm.di.api.remote` contains the interfaces for remote access to the Server through RMI.

Detailed specification of the local and remote interfaces and their methods can be found in the JavaDoc documentation shipped with the TDI (in the `docs/api` folder under the root folder where TDI is installed).

All interfaces in the remote package extend `java.rmi.Remote` and all their methods throw `java.rmi.RemoteException`. The interfaces for local access on the other hand do not extend



`java.rmi.Remote` and their methods do not throw `java.rmi.RemoteException` which facilitates coding and is one of the reasons to have separate set of interfaces for local and remote access.

---

## Server API structure

The structure of the local and remote interfaces is identical. The text below refers to the names of the Java interfaces only and is valid for the interfaces from both the local (`com.ibm.di.api.local`) and remote (`com.ibm.di.api.remote`) Server API Java packages.

The entry point to the Server API is the `SessionFactory` interface (`com.ibm.di.api.local.SessionFactory` for local use and `com.ibm.di.api.remote.SessionFactory` for remote use).

The `SessionFactory` interface provides two methods `createSession()` and `createSession(Username, Password)`. They create an API session for the user/entity that calls it and returns an object of type `Session`. It is this `Session` object that provides further access to the calls of the Server API.

Through the `Session` object one can get Server information or stop the Server itself, existing `Config` Instances can be obtained or new `Config` Instances can be loaded and created from scratch. Some of the calls of the `Session` object will return other Server API objects – for example `startConfigInstance(String aConfigUrl)` will return a `ConfigInstance` object. The `ConfigInstance` object gives access to the configuration data structure, to `AssemblyLines` and `EventHandlers` running in the `Config` Instance as well as calls for starting new `AssemblyLines` and `EventHandlers`. Some of its calls will also return Server API objects. `startAssemblyLine(String aAssemblyLineName)`, for example, returns an `AssemblyLine` object that you can use to query and perform different operations on the `AssemblyLine`.

To summarize, the `Session` object is the one that gives access to the hierarchy of Server API objects. All Server API calls are either invoked directly on the `Session` object or they are invoked on objects retrieved directly or indirectly through the `Session` object.

---

## Security

Authentication is performed in the process of obtaining the `Session` object. Once obtained, all methods called on the `Session` object or on other Server API objects retrieved directly or indirectly through this `Session` object are executed under the identity of the user that obtained the `Session` object.

Authorization is performed on each method call. Before executing the requested call, the Server will determine whether the identity associated with the current session is authorized to execute that call.

The following authentication options are available:

### SSL-based authentication (the mechanism available in TDI 6.0)

This option functions only when `api.remote.ssl.client.auth.on=true` (you will also need `api.on=true`, `api.remote.on=true`, `api.remote.ssl.on=true`).

The user is authorized as per the rights assigned to the SSL certificate user ID in the Server API User Registry.

**Note:** When SSL is used and the remote client application uses Server API listener objects, the client application must have its own certificate that is trusted by the TDI Server (this is analogous to the setup for SSL client authentication). If there is no client certificate trusted by the TDI Server, the listener objects will not work and the remote client application will not be able to receive notifications from the TDI Server.

### Username/password based authentication

This option functions only when `api.custom.authentication` is set to a JavaScript authentication file.

This authentication method works regardless of whether SSL is used and whether SSL client authentication is used. The user is authorized as per the rights assigned to the username user in the Server API User Registry.

An example authentication hook Javascript file is available in order to demonstrate what the Javascript of an authentication hook looks like. This example Javascript can also be used as the basis of real-world TDI authentication hooks.

You can view an JavaScript example that demonstrates how an authentication hook can use an LDAP server (Tivoli Directory Server, Active Directory, etc.) for authenticating client request in the examples/auth\_ldap TDI Server folder. The example file is called ldap\_auth.js.

### LDAP authentication

The TDI Server API provides support for LDAP Authentication. This allows customers to leverage their existing LDAP infrastructures which already hold their User IDs and Passwords.

In order to use LDAP authentication the appropriate properties must be configured in global.properties/solution.properties. These properties are described in the Administrator Guide.

### Host-based authentication

This option functions only when `api.remote.ssl.on=false`. If so, then opening of Server API sessions without username/password supplied from all hosts specified by the `api.remote.nonssl.hosts` property are successfully authenticated and granted admin authority. The `api.remote.nonssl.hosts` property can be specified in the global.properties/solution.properties files.

**Note:** It is strongly recommended that you use this authentication only for demo purposes, quick prototyping and in closed, trusted environments.

---

## Configuring the Server API

Configuring the Server API on the Server side includes specifying the relevant system properties in global.properties (solution.properties) and configuring the User Registry file.

### Configuring the Server API properties

The Server API engine is configured through a set of properties in the global.properties file (or solution.properties file, if a solution folder is used). Refer to “Security and TDI chapter, section Server API Access Security” in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide* for information on how to setup the Server API.

### Setting up the User Registry

Refer to the “Security and TDI” chapter in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide* for information and examples of how to setup the User Registry, assign user roles and encrypt/decrypt the User Registry file.

### Remote client configuration

This section describes what is necessary for a remote client that will use the remote Server API.

#### Prerequisites:

Java 1.4.2 or higher is required on the client side.

#### Configuring the client:

1. The following jar files must be included in the CLASSPATH of the remote side:
  - jars/common/diserverapi.jar
  - jars/common/diserverapirmi.jar
  - jars/3rdparty/others/log4j-1.2.jar
  - jars/common/miconfig.jar

- jars/common/miserver.jar
- jars/common/mmconfig.jar
- jars/3rdparty/IBM/icu4j\_3\_4\_1.jar
- jars/3rdparty/IBM/ITLMToolkit.jar

Users can copy these jar files from the TDI installation.

2. If custom non-TDI objects are used in the solution being implemented with the Server API (for example as Attribute values of an Entry that is transferred over the wire) the corresponding Java classes have to be available on the client side as well. These classes must be serializable and they have to be included in the CLASSPATH of the client JVM.

## SSL configuration of the remote client

There are two options for configuring SSL on the remote client:

### Using Server API specific SSL properties

When the Java System property `api.client.ssl.custom.properties.on` is set to true, then SSL is configured through the following TDI Server API-specific Java System properties:

- **api.client.keystore** – specifies the keystore file containing the client certificate
- **api.client.keystore.pass** – specifies the password of the keystore file specified by *api.client.keystore*
- **api.client.key.pass** – the password of the private key stored in keystore file specified by *api.client.keystore*; if this property is missing, the password specified by *api.client.keystore.pass* is used instead.
- **api.truststore** – specifies the keystore file containing the TDI Server public certificate.
- **api.truststore.pass** – specifies the password for the keystore file specified by *api.truststore*.

Using the Server API-specific SSL properties is convenient when your client application is using the standard Java SSL properties for configuration of another SSL channel used by the same application.

You can specify these properties as JVM arguments on the command line, for example:

```
java MyTDIServerAPIClientApp
-Dapi.client.ssl.custom.properties.on=true
-Dapi.truststore=C:\TDI\serverapi\testadmin.jks
-Dapi.truststore.pass=administrator
-Dapi.client.keystore=C:\TDI\serverapi\testadmin.jks
-Dapi.client.keystore.pass=administrator
```

This example refers to the sample `testadmin.jks` keystore file shipped with TDI. Note that it contains both the client private key and also the public key of the TDI Server, so it is used as both as a keystore and truststore.

### Using the standard SSL Java System properties:

When the Java System property `api.client.ssl.custom.properties.on` is missing or when it is set to false, then the standard JSSE system properties are used for configuring the SSL channel. Follow the standard JSSE procedure for configuring the keystore and truststore used by the client application.

You can specify these properties as JVM arguments on the command line; for example:

```
java MyTDIServerAPIClientApp
-Djavax.net.ssl.keyStore=C:\TDI\serverapi\testadmin.jks
-Djavax.net.ssl.keyStorePassword=administrator
-Djavax.net.ssl.trustStore=C:\TDI\serverapi\testadmin.jks
-Djavax.net.ssl.trustStorePassword=administrator
```

---

## Using the Server API

### Creating a local Session

If you are writing Java code that will be executed in the TDI Server JVM (for example a new Connector, or a Java class that you will access through scripting) and you want to execute Server API calls, you'll need a local Server API session.

You can obtain a local Server API session by calling:

```
import com.ibm.di.api.APIEngine;
import com.ibm.di.api.local.Session;
```

```
...
```

```
Session session = APIEngine.getLocalSession();
```

`getLocalSession()` is a static method of the `com.ibm.di.api.APIEngine` class. It creates and returns a new `com.ibm.di.api.local.Session` object. This session returned has admin rights and can execute all Server API calls.

### Access to the Server API in a scripting context

Users can get access to the Server API from a scripting context (for example from AssemblyLine hooks) by calling the session script object. TDI Server registers session objects by calling `com.ibm.di.api.APIEngine.getLocalSession()` method.

### Creating a remote Session

A client application that uses the remote Server API would first need to connect to the TDI Server and obtain a Server API Session.

Use the following Java code to lookup the RMI SessionFactory object and obtain a Server API Session:

```
import com.ibm.di.api.remote.Session;
import com.ibm.di.api.remote.SessionFactory;
```

```
...
```

```
SessionFactory sessionFactory = (SessionFactory) Naming.lookup("rmi://<TDI_Server_host>:
<TDI_Server_RMI_port>/SessionFactory");
```

```
Session session = sessionFactory.createSession();
```

You need to replace `TDI_Server_host` and `TDI_Server_RMI_port` with the host and the RMI port of the TDI Server; for example:

```
Naming.lookup("rmi://127.0.0.1:1099/SessionFactory")
```

The calls provided by the local and remote Session objects are identical. All examples below assume that you have already obtained a session and will operate in a remote context. In other words, the remote versions of the Server API interfaces will be used.

### Working with Config Instances

The Config Instance represents a configuration loaded on the TDI Server and the associated Server object. Each AssemblyLine or EventHandler is running in the context of a Config Instance. Through a Config Instance you can query the configuration of AssemblyLines, EventHandlers, Connectors, Parsers, Functional Components, start AssemblyLines and EventHandlers, get access to running AssemblyLines and EventHandlers and query their log files.

## Getting access to running Config Instances

You can obtain access to all Config Instances running on the TDI Server by executing the following piece of code:

```
ConfigInstance[] configInstances = session.getConfigInstances();
for (int i=0; i<configInstances.length; i++) {
    // do something with configInstances[i]
}
```

The `getConfigInstances()` method will return an array with Config Instance Server API objects representing all Config Instances running on the Server.

## Starting a Config Instance

In order to load a new configuration on the TDI Server you need to start a new Config Instance, pointing it to the XML configuration file:

```
ConfigInstance configInstance = session.startConfigInstance("testconfig.xml");
```

This loads the `testconfig.xml` configuration file and start a new Config Instance object associated with that configuration. Once you get that Config Instance object you can use it to change the configuration itself, start AssemblyLines and EventHandlers or stop the Config Instance on the Server when you no longer need it.

## Stopping a Config Instance

Assuming that you have a reference to the Config Instance Server API object, you can stop the Config Instance by calling:

```
configInstance.stop();
```

For a reference to the Config Instance object, you have the following options:

- Keep that reference from where you started the Config Instance, that is, `configInstance = session.startConfigInstance("testconfig.xml")`
- Retrieve the Config Instance object through its Config ID by calling `session.getConfigInstance(String aConfigId)`. The Config ID is a unique identifier for each Config Instance running on the Server. It is created by the Server API when the corresponding Server API Config Instance object is created. You can retrieve the Config ID through the Config Instance object by calling `configInstance.getConfigId()`.
- Iterate through all running Config Instances and find the one you need: `session.getConfigInstances()` will return an array of all running Config Instances.

## Working with AssemblyLines

### Getting access to the AssemblyLines available in a configuration

Assuming that you already have a reference to the Config Instance object, you must obtain the `MetamergeConfig` object representing the configuration data structure for the whole Config Instance and then get the available AssemblyLines:

```
import com.ibm.di.config.interfaces.MetamergeConfig;
import com.ibm.di.config.interfaces.MetamergeFolder;
import com.ibm.di.config.interfaces.AssemblyLineConfig;

...

MetamergeConfig configuration = configInstance.getConfiguration();
MetamergeFolder configFolder =
    configuration.getDefaultFolder(MetamergeConfig.ASSEMBLYLINE_FOLDER);
String[] assemblyLineNames = configFolder.getNames();
if (assemblyLineNames != null) {
    for (int i=0; i<assemblyLineNames.length; i++) {
        System.out.println(assemblyLineNames[i]);
    }
}
```

```

// get the AssemblyLine configuration object
AssemblyLineConfig alConfig =
    configuration.getAssemblyLine(assemblyLineNames[i]);
// do something with alConfig ...

```

This block of code prints to the standard output the names of all AssemblyLines in the configuration and demonstrates how to get the AssemblyLine configuration objects. You can use the AssemblyLine configuration object to get more detailed information, such as which Connectors are configured in the AssemblyLine, their parameters, etc.

Note that the MetamergeConfig, MetamergeFolder and AssemblyLineConfig interfaces are not part of the Server API interfaces. They are part of the TDI configuration driver (see the import clauses in the example) and they are not remote objects. When configInstance.getConfiguration() is executed the MetamergeConfig object is serialized and transferred over the wire. Your code will then work with the local copy of that object.

## Getting access to running AssemblyLines

You can get the active AssemblyLines either for a specific Config Instance or for all active AssemblyLines on the TDI Server for all running Config Instances.

### Getting the active AssemblyLines for a specific Config Instance:

You will need a reference to the Config Instance object. The following code will return all AssemblyLines currently running in the Config Instance:

```

AssemblyLine[] assemblyLines = configInstance.getAssemblyLines();
for (int i=0; i
for (int i=0; i<assemblyLines.length; i++) {
    System.out.println(assemblyLines[i].getName());

    // do something with assemblyLines[i]
}

```

### Getting the active AssemblyLines for the whole TDI Server:

If you want to get all AssemblyLines running on the Server, execute the following code:

```

AssemblyLine[] assemblyLines = session.getAssemblyLines();
for (int i=0; i<assemblyLines.length; i++) {
    System.out.println(assemblyLines[i].getName());

    // do something with assemblyLines[i]

    // which Config Instance this AssemblyLine belongs to?
    ConfigInstance alConfigInstance = assemblyLines[i].getConfigInstance();
}

```

Note that this is executed at the session level and not for a particular Config Instance. If you need to know which Config Instance a running AssemblyLine belongs to, you can get a reference to the parent Config Instance object through the AssemblyLine object.

You can use the AssemblyLine Server API object to get various AssemblyLine properties, the AssemblyLine configuration object, AssemblyLine log, AssemblyLine result Entry as well as stop the AssemblyLine.

## Starting an AssemblyLine

You can start an AssemblyLine through the Config Instance object to which the AssemblyLine belongs. You need to know the name of the AssemblyLine you want to start:

```

AssemblyLine assemblyLine = configInstance.startAssemblyLine("MyAssemblyLine");

```

You also receive a reference to the newly started AssemblyLine instance.

## Starting an AssemblyLine in manual mode

The Server API provides a mechanism for manually running an AssemblyLine. In manual mode the AssemblyLine is not running in its own thread. Instead, when you start the AssemblyLine, it is only initialized. Iterations on the AssemblyLine are done in a synchronous manner when the `executeCycle()` method of the AssemblyLine object is called. This call blocks the current thread and when the AssemblyLine iteration is done it returns the result Entry object.

The following code will start the TestAL AssemblyLine in manual mode and execute three iterations on it. The result Entry from each iteration is printed to the standard output:

```
AssemblyLineHandler alHandler = configInstance.startAssemblyLineManual("TestAL", null);
Entry entry = null;
for (int i=0; i<3; i++) {
    entry = alh.executeCycle();
    System.out.println("TestAL entry: " + entry);
}
alHandler.close();
```

The `startAssemblyLineManual(String aAssemblyLineName, Entry aInputData)` method of the Config Instance object starts an AssemblyLine in manual mode and returns an object of type `com.ibm.di.api.remote.AssemblyLineHandler`. Through this object you can manually iterate through the AssemblyLine, you can pass an initial work Entry and various Task Call Block parameters, you can get a reference to the AssemblyLine Server API object and you can terminate the AssemblyLine when you are done with it.

You can imitate the AssemblyLine runtime behavior by calling `executeCycle()` until it returns NULL.

## Starting an AssemblyLine with a listener

When you start an AssemblyLine through the Server API you can register a specific AssemblyLine listener that will receive notifications on each AssemblyLine iteration, delivering the result Entry, and also when the AssemblyLine terminates. Through this mechanism you can start an AssemblyLine from a remote application and easily receive all Entries produced by the AssemblyLine. The AssemblyLine listener will also deliver all messages logged during the execution of the AssemblyLine.

Your listener class must implement the `com.ibm.di.api.remote.AssemblyLineListener` interface (or `com.ibm.di.api.local.AssemblyLineListener` for local access).

The methods you must specify are:

- `assemblyLineCycleDone(Entry aEntry)` – this method will be called at the end of each AssemblyLine iteration; the `aEntry` parameter represents the result Entry from the AssemblyLine iteration.
- `assemblyLineFinished()` – this method is called by the Server API when the AssemblyLine terminates.
- `messageLogged(String aMessage)` – this method is called by the Server API whenever a message is logged through the AssemblyLine logger. Thus you can get remote real time access to the log messages produced by the AssemblyLine.

A sample AssemblyLine listener class that only prints to the standard output all Entries received and all AssemblyLine log messages might look like this:

```
import com.ibm.di.api.DIException;
import com.ibm.di.api.remote.AssemblyLineListener;
import com.ibm.di.entry.Entry;
import java.rmi.RemoteException;

public class MyRemoteALListener implements AssemblyLineListener {

    public void assemblyLineCycleDone(Entry aEntry)
        throws DIException, RemoteException
    {
        System.out.println("AssemblyLine iteration: " + aEntry.toString());
        System.out.println();
    }
}
```

```

}

public void assemblyLineFinished()
    throws DIException, RemoteException
{
    System.out.println("AssemblyLine terminated.");
    System.out.println();
}

public void messageLogged(String aMessage)
    throws DIException, RemoteException
{
    System.out.println("AssemblyLine log message: " + aMessage);
    System.out.println();
}
}

```

Once you have implemented your AssemblyLine listener class, you need to instantiate a listener object and pass it when starting the AssemblyLine:

```

MyRemoteALLListener allListener = new MyRemoteALLListener();
configInstance.startAssemblyLine("TestAL", null,
    AssemblyLineListenerBase.createInstance(allListener,true), true);

```

The startAssemblyLine(String aAssemblyLineName, Entry aInputData, AssemblyLineListener aListener, boolean aGetLogs) method specifies the name of the AssemblyLine, an initial work Entry, the listener object and whether you want to receive log messages – when aGetLogs is false, the messageLogged(String aMessage) listener method will not be called by the Server API.

When you are registering a listener in a remote context, you have to wrap your specific listener in an AssemblyLine Base Listener class – this is necessary to provide a bridge between your custom listener Java class that is not available on the Server side and the Server API notification mechanism. A base listener class is created by calling the static createInstance(AssemblyLineListener aListener, boolean aSSLon) method of the com.ibm.di.api.remote.impl.AssemblyLineListenerBase class. You need to provide the object representing your listener class and specify whether SSL is used for communication with the Server or not (you must specify how the Server API is configured on the Server side – otherwise the communication for that listener will fail).

## Stopping an AssemblyLine

You need a reference to the AssemblyLine object in order to stop it. You can keep the reference to the AssemblyLine object from when you started the AssemblyLine or you can iterate through all running AssemblyLines and find the one you need. Execute the following line of code to stop the AssemblyLine:

```
assemblyLine.stop();
```

## Working with EventHandlers

Everything stated in section “Working with AssemblyLines” about AssemblyLines is valid for EventHandlers as well. You can work with EventHandlers in exactly the same manner using the corresponding EventHandler classes, interfaces and methods. Please consult the JavaDocs for the signatures of the EventHandler related classes, interfaces and methods.

**Note:** The concept of EventHandlers is deprecated in TDI 6.1.1 and will be removed in a future version. Use AssemblyLines with Connectors in Server Mode instead.

## Editing configurations

### TDI Configurations folder

A TDI Server property `api.config.folder` is available in the TDI Server configuration file `global.properties` - it specifies a folder on the local disk. The Server API will provide calls for browsing and loading configurations placed in this folder or its subfolders. For example:



`api.config.folder=configs`

This means that all configuration files placed in “<TDL\_root>/configs” and its subfolders are eligible for browsing and loading through the Server API (locally and remotely).

The Server API provides new calls for browsing the files and folders in the folder specified by the `api.config.folder` property.

## Load for editing

In TDI 6.0 configurations can be edited only after the corresponding Config Instance has been started on the TDI Server. Then there are API calls for getting the Config object, setting the Config object back (probably modified) and saving the configuration on the disk.

TDI 6.1.1 will not allow modification of the Config object of an active Config Instance. Server API users will still be able to get the Config object for an active Config Instance, but the following calls for setting the Config object and saving it on the disk will throw an exception when executed on a normal running Config Instance:

- `ConfigInstance.setConfiguration(MetamergeConfig configuration)`
- `ConfigInstance.saveConfiguration()`
- `ConfigInstance.saveConfiguration(boolean aEncrypt)`

When a configuration is loaded for editing with a temporary Config Instance it will be able to execute the `setConfiguration(...)` method in order to test the changes applied to the configuration. The `saveConfiguration(...)` methods will however still throw exceptions. TDI 6.1.1 will present new Server API calls for loading configurations for editing and for saving the edited configurations on the disk.

## Configuration Locking

The Server API internally tracks all configurations loaded for editing. When another Server API user requests a configuration already loaded for editing, the method call will fail with exception. A new Server API call has been added for checking whether a configuration is currently loaded for editing (locked).

The lock on a configuration will be released when the user that loaded the configuration for editing saves it back or cancels the update. The Server API provides an option to specify a timeout value for keeping a configuration locked. When that timeout is reached for a configuration the lock is released and the user that locked the configuration will not be able to save it before loading it again.

A new property “`api.config.lock.timeout`” has been added in the TDI Server configuration file `global.properties`. It specifies the timeout value in minutes. When the property is left empty or is set a value of 0, this means that there is no timeout. The default value for this property is 0. The timeout logic is implemented by a new thread in the TDI Server. This thread is activated only when “`api.config.lock.timeout`” is set to a value greater than 0 and will check for and release expired locks each 30 seconds.

A special call for a forced releasing of the lock on a configuration loaded for editing has been added to the Server API. Only Server API users with the admin role will be able to execute it.

All configurations are identified through the relative file path of the configuration file according the TDI Server configurations folder.

All paths specified as method parameters are relative to the TDI Server configurations folder.

The following new calls will be added to the local and remote Server API Session objects and in the JMX interfaces:

- `public boolean releaseConfigurationLock(String aRelativePath) throws DIException;`

Administratively releases the lock of the specified configuration. This call can be only executed by users with the admin role.

- `public boolean undoCheckOut(String aRelativePath) throws DIException;`  
Releases the lock on the specified configuration, aborting all changes being done. This call can only be executed from a user that has previously checked out the configuration and if the configuration lock has not timed out.
- `public ArrayList listConfigurations(String aRelativePath) throws DIException;`  
Returns a list of the file names of all configurations in the specified folder. The configurations file paths returned are relative to the TDI Server configurations folder.
- `public ArrayList listFolders(String aRelativePath) throws DIException;`  
Returns a list of the child folders of the specified folder
- `public ArrayList listAllConfigurations() throws DIException;`  
Returns a list of the file names of all configurations in the directory subtree of the TDI Server configurations folder. The configurations file paths returned are relative to the TDI Server configurations folder.
- `public MetamergeConfig checkOutConfiguration(String aRelativePath) throws DIException;`  
Checks out the specified configuration. Returns the MetamergeConfig object representing the configuration and locks that configuration on the Server.
- `public MetamergeConfig checkOutConfiguration(String aRelativePath, String aPassword) throws DIException;`  
Checks out the specified password protected configuration. Returns the MetamergeConfig object representing the configuration and locks that configuration on the Server.
- `public void checkInConfiguration(MetamergeConfig aConfiguration, String aRelativePath) throws DIException;`  
Saves the specified configuration and releases the lock. If a temporary Config Instance has been started on check out, it will be stopped as well.
- `public void checkInConfiguration(MetamergeConfig aConfiguration, String aRelativePath, boolean aEncrypt) throws DIException;`  
Encrypts and saves the specified configuration and releases the lock. If a temporary Config Instance has been started on check out, it will be stopped as well.
- `public void checkInAndLeaveCheckedOut(MetamergeConfig aConfiguration, String aRelativePath) throws DIException;`  
Checks in the specified configuration and leaves it checked out. The timeout for the lock on the configuration is reset.
- `public MetamergeConfig createNewConfiguration(String aRelativePath, boolean aOverwrite) throws DIException;`  
Creates a new empty configuration and immediately checks it out. If a configuration with the specified path already exists and the aOverwrite parameter is set to false the operation will fail and an Exception will be thrown.
- `public ConfigInstance checkOutConfigurationAndLoad(String aRelativePath) throws DIException;`  
Checks out the specified configuration and starts a temporary Config Instance on the Server. This Config Instance will be stopped when the configuration is checked in or when the lock on the configuration expires. The method returns the ConfigInstance object. The MetamergeConfig object can be retrieved through the ConfigInstance object.
- `public ConfigInstance checkOutConfigurationAndLoad(String aRelativePath, String aPassword) throws DIException;`  
Checks out the specified password protected configuration and starts a temporary Config Instance on the Server. This Config Instance will be stopped when the configuration is checked in or when the lock on the configuration expires. The method returns the ConfigInstance object. The MetamergeConfig object can be retrieved through the ConfigInstance object.

- `public ConfigInstance createNewConfigurationAndLoad(String aRelativePath, boolean aOverwrite)` throws `DIException`;  
Creates a new empty configuration, immediately checks it out and loads a temporary Config Instance on the Server. If a configuration with the specified path already exists and the `aOverwrite` parameter is set to `false` the operation will fail and an Exception will be thrown. The temporary Config Instance will be stopped when the configuration is checked in or when the lock on the configuration expires. The method returns the `ConfigInstance` object. The `MetamergeConfig` object can be retrieved through the `ConfigInstance` object.
- `public boolean isConfigurationCheckedOut(String aRelativePath)` throws `DIException`;  
Checks if the specified configuration is checked out on the Server.

### Load for editing with temporary Config Instance

This is a special version of the load for edit mechanism – the difference is that when the configuration is loaded for editing a temporary Config Instance will be started as well. This will allow testing the configuration and its `AssemblyLines` while they are being developed and will be particularly useful for development tools like the TDI Config Editor.

The Config Instance will be automatically stopped when the configuration is released or when the lock on the configuration expires.

The temporary Config Instances are independent of the normal long running Config Instances on the Server. A normal Config Instance from configuration `rs.xml` might be running on the Server and at the same time the `rs.xml` configuration can be loaded for editing with a temporary Config Instance. This will result in starting a new temporary Config Instance from the `rs.xml` file in addition to the normal long running `rs.xml` Config Instance.

The same locking mechanism applies for configurations loaded for editing with a temporary Config Instance. This means that a configuration can be loaded for editing only once regardless of whether it has been loaded for editing with a temporary Config Instance or without.

### New Server API event for configuration update

A new Server API event `di.ci.file.updated` will be fired whenever a configuration that has been locked is saved on the TDI Server.

This notification will allow Server API clients to get notified for changes in configurations they are using and for example reload them to get the latest version.

### Working with the System Queue

A System Queue TDI module is introduced in TDI 6.1.1. The System Queue is a TDI server module which TDI internal objects as well as TDI components can use as a general purpose queue. The purpose of the System Queue is to connect to a JMS Provider and provide functionality for getting from JMS message queues and putting into JMS message queues general messages as well as TDI Entry objects. The System Queue can connect to different JMS Providers using different TDI JMS Drivers. For more information on the System Queue please see the “System Queue” chapter of the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide*.

The System Queue functionality is exposed through both the local and remote interfaces of the Server API as well as through the JMX layer of the Server API. TDI components and sub-systems which run in the Java Virtual Machine of the local TDI server are expected to use the local Server API interfaces to interact with the System Queue. Remote Server API client applications as well as TDI components and sub-systems which run in the Java Virtual Machine of a remote TDI server are expected to use the remote Server API interfaces.

A SystemQueue MBean has been introduced in the TDI 6.1.1 Server API JMX layer. This MBean provides JMX access to the SystemQueue. A JMX client can access the newly introduced SystemQueue JMX MBean and thus work with the System Queue through JMX.

The System Queue must be properly configured before it can be accessed through the Server API. A simple way to configure the System Queue is like the following:

- Setup the JMS Provider.

TDI provides the MQ Everyplace JMS Provider out of the box. You can setup a MQe Queue Manager via the *mqeconfig* command line utility (the *mqeconfig* utility is located in the 'jars/plugins' subfolder of your TDI installation).

Modify the *mqeconfig.props* configuration file.

- Specify the folder where you want to place the MQe Queue Manager:

```
serverRootFolder=C:\\TDI\\MQePWStore
```

- Specify the IP address of the TDI Server:

```
serverIP=127.0.0.1
```

- Having the configuration options set, create the MQe Queue Manager:

```
mqeconfig mqeconfig.props create server
```

- Create a queue for test purposes:

```
mqeconfig mqeconfig.props create queue myqueue
```

- Configure the System Queue and the JMS Provider in *global.properties/solution.properties*

- Turn on System Queue usage:

```
systemqueue.on=true
```

- Set the JMS driver for the System Queue to MQ Everyplace:

```
systemqueue.jmsdriver.name=com.ibm.di.systemqueue.driver.IBMMQe
```

- Set the configuration file for the MQe Queue Manager (this file has been generated by the *mqeconfig* utility):

```
systemqueue.jmsdriver.param.mqe.file.ini=C:\\TDI\\MQePWStore\\pwstore_server.ini
```

:

**Note:** For a stand-alone Java program to operate successfully with the System Queue through the Server API, a JMS implementation must be included in the CLASSPATH of the program. You can use the JMS implementation distributed with TDI: *jars/3rdparty/IBM/ibmjms.jar*

## Access the System Queue through the Server API

Once a Server API session is initiated, the System Queue can be accessed like this:

```
import com.ibm.di.api.remote.SystemQueue;
...
SystemQueue systemQueue = session.getSystemQueue();
```

## Put a message in the System Queue

The following code puts a text message into a queue named "myqueue" (the call will not create the specified queue automatically - the queue must be created manually first):

```
systemQueue.putTextMessage("myqueue", "mytextmessage");
```

## Retrieve a message from the System Queue

The following code retrieves a text message from a queue named "myqueue" (the queue must exist). The method call waits a maximum of 10 seconds for a message to become available:

```
String textMessage = systemQueue.getTextMessage("myqueue", 10);
```

## Working with the Tombstone Manager

A Tombstone Manager TDI module was introduced in TDI 6.1.1.

Previous versions of TDI do not keep track of configurations or AssemblyLines that have terminated. Therefore, administrators have no way of knowing when their AssemblyLines last ran, without going into the log of each one. Bundlers that initiate AssemblyLines have no way of querying their status after they've terminated.

The solution is a Tombstone Manager that creates records ("tombstones") for each AssemblyLine and configuration as they terminate, that contain exit status and other information that later can be requested through the Server API.

## Globally Unique Identifiers

Globally Unique Identifiers (GUID) are created by the Server API to uniquely identify Config Instance, AssemblyLine and EventHandler instances. The GUID is a string value that is unique for each instance of a Config Instance, an AssemblyLine or an EventHandler ever created by a particular TDI Server.

GUIDs are defined as the string representation of the Config Instance/AssemblyLine/EventHandler object hashcode concatenated with the string representation of the Config Instance/AssemblyLine/EventHandler start time in milliseconds.

A new method has been added to the Config Instance, AssemblyLine and EventHandler Server API interfaces: `String getGlobalUniqueID ();`

A new field `GlobalUniqueID` has been added to AssemblyLine, EventHandler and Config Instance stop Server API events.

## Server API support for the Tombstone Manager

**What is a tombstone:** The Server API provides a new class `com.ibm.di.api.Tombstone` whose instances represent tombstone objects. The public interface of the Tombstone class follows:

```
public class Tombstone implements Serializable {  
    public int getComponentTypeID ()  
    public int getEventTypeID ()  
    public java.util.Date getStartTime ()  
    public java.util.Date getTombstoneCreateTime ()  
    public String getComponentName ()  
    public String getConfigID ()  
    public int getExitCode ()  
    public String getErrorDescription ()  
    public String getGUID ()  
    public Entry getStat ()  
    public String getUserMessage ()  
}
```

**Retrieving tombstones:** Tombstones are retrieved through the Tombstone Manager. You can access the Tombstone Manager via the Server API like this:

```
import com.ibm.di.api.remote.TombstoneManager;  
...  
TombstoneManager tombstoneManager = session.getTombstoneManager();
```

With the Tombstone Manager at hand, you can search for specific Tombstones. The following code iterates through all tombstones created last week:

```
Calendar calendar = Calendar.getInstance();
calendar.add(Calendar.DATE, -7);

Tombstone[] tombstones = tombstoneManager.getTombstones(calendar.getTime(), new Date());

for (int i = 0; i < tombstones.length; ++i) {
    System.out.println("Tombstone found for : "+tombstones[i].getComponentName());
    System.out.println("\t GUID : "+tombstones[i].getGUID());
    System.out.println("\t statistics : "+tombstones[i].getStatistics());
}
```

All tombstones for a particular AssemblyLine can be retrieved this way (the example AssemblyLine is named "myline" and the ID of the configuration is "C\_\_TDI\_myconfig.xml"):

```
Tombstone[] allTombstones = tombstoneManager.getAssemblyLineTombstones("AssemblyLines/myline",
"C__TDI_myconfig.xml");
```

The following new Server API calls are provided for querying the Tombstone Manager – these are methods of the `com.ibm.di.api.local.TombstoneManager` interface:

- `Tombstone getTombstone (String aGUID)`  
Returns a single tombstone object uniquely identified by the specified GUID.
- `Tombstone[] getAssemblyLineTombstones (String aAssemblyLineName, String aConfigID)`  
Returns all available tombstones for the specified AssemblyLine.
- `Tombstone[] getAssemblyLineTombstones (String aAssemblyLineName, String aConfigID, java.util.Date aStartTime, java.util.Date aEndTime)`  
Returns all available tombstones for the specified AssemblyLine with timestamps in the interval specified by aStartTime and aEndTime.
- `Tombstone[] getEventHandlerTombstones (String aEventHandlerName, String aConfigID)`  
Returns all available tombstones for the specified EventHandler.
- `Tombstone[] getEventHandlerTombstones (String aEventHandlerName, String aConfigID, java.util.Date aStartTime, java.util.Date aEndTime)`  
Returns all available tombstones for the specified EventHandler with timestamps in the interval specified by aStartTime and aEndTime.
- `Tombstone[] getConfigInstanceTombstones (String aConfigID)`  
Returns all available tombstones for the specified Config Instance.
- `Tombstone[] getConfigInstanceTombstones (String aConfigID)`  
Returns all available tombstones for the specified Config Instance.
- `Tombstone[] getTombstones (java.util.Date aStartTime, java.util.Date aEndTime)`  
Returns all available tombstones with timestamps in the interval specified by aStartTime and aEndTime.

**Deleting tombstones:** When tombstones are no longer needed they should be deleted.

The following code deletes all tombstones from the last week:

```
tombstoneManager.deleteTombstones(7);
```

The following new Server API calls are provided for deleting old tombstone records:

- `int deleteTombstones (int aDays)`  
Deletes all tombstones that are older than the specified number of days. Returns the number of deleted tombstone records.
- `int keepMostRecentTombstones (int aMostRecentToKeep)`

After this method is executed only the *aMostRecentToKeep* most recent tombstone records are kept and all other are deleted. Returns the number of deleted tombstone records.

- `int deleteALTombstones (String aAssemblyLineName, String aConfigID)`  
Deletes all tombstones for specified AssemblyLine. Returns the number of deleted tombstone records.
- `int deleteALTombstones (String aAssemblyLineName, String aConfigID, int aDays)`  
Deletes all tombstones for the specified AssemblyLine that are older than the specified number of days. Returns the number of deleted tombstone records.
- `int keepMostRecentALTombstones (String aAssemblyLineName, String aConfigID, int aMostResentToKeep)`  
After this method is executed only the *aMostRecentToKeep* most recent tombstone records for the specified AssemblyLine are kept and all other are deleted. Returns the number of deleted tombstone records.
- `int deleteEHTombstones (String aEventHandlerName, String aConfigID)`  
Deletes all tombstones for specified EventHandler. Returns the number of deleted tombstone records.
- `int deleteEHTombstones (String aEventHandlerName, String aConfigID, int aDays)`  
Deletes all tombstones for the specified EventHandler that are older than the specified number of days. Returns the number of deleted tombstone records.
- `int keepMostRecentEHTombstones (String aEventHandlerName, String aConfigID, int aMostResentToKeep)`  
After this method is executed only the *aMostRecentToKeep* most recent tombstone records for the specified EventHandler are kept and all other are deleted. Returns the number of deleted tombstone records.
- `int deleteCITombstones (String aConfigID)`  
Deletes all tombstones for specified Config Instance. Returns the number of deleted tombstone records.
- `int deleteCITombstones (String aConfigID, int aDays)`  
Deletes all tombstones for the specified Config Instance that are older than the specified number of days. Returns the number of deleted tombstone records.
- `int keepMostRecentCITombstones (String aConfigID, int aMostResentToKeep)`  
After this method is executed only the *aMostRecentToKeep* most recent tombstone records for the specified Config Instance are kept and all other are deleted. Returns the number of deleted tombstone records.
- `boolean deleteTombstone (String aGUID)`  
Deletes the tombstone with the specified GUID. Returns true only when the tombstone object with the specified GUID is found and deleted.

### Adding a custom message to AssemblyLine tombstones

The *task* script object represents the AssemblyLine object in an AssemblyLine context so that you can use this object when scripting.

The interface of the *task* object is extended to provide a method for setting a custom message that will be saved in the UserMessage field of the tombstone for this AssemblyLine. The signature of the new method, accessible through the task script object is as follows:

```
task.setTombstoneUserMessage(String aUserMessage);
```

This method can be used from AssemblyLine scripts to provide additional information in the AssemblyLine tombstone.

The user message of a tombstone can be retrieved like this:

```
String userMessage = tombstone.getUserMessage();
```

**Note:** No user defined messages can be set for ConfigInstance and EventHandler tombstones.

## Working with TDI Properties

For a remote client to query/get/set properties (or stores), it needs to be provided a remote reference of the `TDIProperties` object in the server. A remote client can obtain the `com.ibm.di.api.remote.TDIProperties` interface remote reference via the following method in `com.ibm.di.api.remote.ConfigInstance`:

```
public TDIProperties getTDIProperties() throws DIException,RemoteException;
```

A similar interface and implementation is available in the local Server API interfaces.

For a description of the interface methods please see the TDI JavaDocs.

The following example lists all available Property Stores for a given configuration instance:

```
TDIProperties tdiProperties = configInstance.getTDIProperties();
```

```
List stores = tdiProperties.getPropertyStoreNames();
Iterator it = stores.iterator();
System.out.println("Available property stores :");
while (it.hasNext()) {
    String storeName = (String) it.next();
    System.out.println("\t"+storeName);
}
```

Individual properties can be acquired by their name. The following code prints all properties available in the Global Property Store (`global.properties`) :

```
String storeName = "Global-Properties";
System.out.println(storeName+" store contents :");
String[] storeKeys = tdiProperties.getPropertyStoreKeys(storeName);
for (int i = 0; i < storeKeys.length; ++i) {
    System.out.println("\t"+storeKeys[i]+" : "+tdiProperties.getProperty(storeName, storeKeys[i]));
}
```

Property values can be changed and new properties can be created like this:

```
tdiProperties.setProperty(storeName, "mykey", "myvalue");
```

The following code removes a property from a Property Store:

```
tdiProperties.removeProperty(storeName, "mykey");
```

Before any changes to a Property Store (adding a new property, changing the value of a property or removing a property) take effect, the changes must be committed:

```
tdiProperties.commit();
```

### JMX layer API

A `TDIPropertiesMBean` interface is available in the `com.ibm.di.api.jmx.mbeans` package. The methods exposed in `TDIPropertiesMBean` interface are similar to the ones exposed in the `com.ibm.di.api.remote.TDIProperties` interface.

A method `getTDIProperties()` is available in the `com.ibm.di.api.jmx.mbeans.ConfigInstanceMBean` class via which a JMX client can obtain a reference to a `javax.management.ObjectName` interface.

## Registering for Server API event notifications

The Server API provides an event notification mechanism for Server events like starting and stopping of Config Instances, AssemblyLines and EventHandlers. This allows a local or remote client application to register for event notifications and react to various events.

Applications that need to register and receive notifications should implement a listener class that implements the `DIEventListener` interface (`com.ibm.di.api.remote.DIEventListener` for remote



applications and `com.ibm.di.api.local.DIEventListener` for local access). This class is responsible for processing the Server events. The `handleEvent(DIEvent aEvent)` method from the `DIEventListener` interface is where you need to put your code that processes Server events. Of course you may implement as many listener classes as you need, with different implementations of the `handleEvent(DIEvent aEvent)` method and register all of them as event listeners. A sample listener that just logs the event object might look like this:

```
import java.rmi.RemoteException;

import com.ibm.di.api.DIEvent;
import com.ibm.di.api.DIException;
import com.ibm.di.api.remote.DIEventListener;

public class MyListener implements DIEventListener
{
    public void handleEvent (DIEvent aEvent) throws DIException, RemoteException
    {
        System.out.println("TDI Server event: " + aEvent);
        System.out.println();
    }
}
```

Once you have implemented your listener you will need to register it with the Server API. If however you are implementing a remote application there is one extra step you need to perform before actually registering the listener object with the Server API – you need to instantiate and use a base listener object that will wrap the listener you implemented. The base listener class allows you to use your own listener classes without having the same Java classes available on the Server:

```
DIEventListener myListener = new MyListener();
DIEventListener myBaseListener = DIEventListenerBase.createInstance(myListener, true);
```

The base listener object implements the same *DIEventListener* interface – its class however is already present on the Server and it can act as a bridge between your local client side listener class and the Server. A base listener object is created by calling the static method *createInstance(DIEventListener aListener, boolean aSSLon)* of the *com.ibm.di.api.remote.impl.DIEventListenerBase* class. The first parameter *aListener* represents the actual listener object and the second one specifies whether SSL is used or not by the Server API (note that this is not an option for you to select whether to use SSL or not with this listener object; here you have to specify how the Server API is configured on the Server side – otherwise the communication for that listener will fail).

When you have your listener object ready (or a base listener for remote access), you can register for event notifications through the session object:

```
session.addEventListener(myBaseListener, "di.*", "*");
```

The *addEventListener(DIEventListener aListener, String aTypeFilter, String aIdFilter)* method of the session object will register your listener. The first parameter *aListener* is the listener object (or the base listener object for remote access), *aTypeFilter* and *aIdFilter* let you specify what types of events you want to receive:

- *aTypeFilter* specifies what type of event objects you want to receive. The currently supported events are:
  - **di.ci.start** – Config Instance started
  - **di.ci.stop** – Config Instance stopped
  - **di.al.start** – AssemblyLine started
  - **di.al.stop** – AssemblyLine stopped
  - **di.eh.start** – EventHandler started
  - **di.eh.stop** – EventHandler stopped
  - **di.ci.file.updated** – Configuration file modified
  - **di.server.stop** – TDI Server shutdown

You can either specify a specific event type like `di.al.start` or you can specify a filter using the "\*" wildcard; for example `di.al.*` will register your listener for all Server events related to AssemblyLines, while a type filter of \* or NULL will register your listener for all events.

- `aldFilter` is only taken into account when `aTypeFilter` is not set to "" or NULL. It lets you filter events depending on the object related to the event – for AssemblyLines this is the AssemblyLine name, for EventHandlers this is the EventHandler name and for Config Instances this is the Config Instance ID. For example, if you register your listener with `addEventListener(myListener, "di.al.start", "MyAssemblyLine")` it will only be sent events when the "MyAssemblyLine" AssemblyLine is started and will not receive any other Server events.

If at some point you want to stop receiving event notifications from a listener already registered with the Server API, you need to unregister the listener. This is done through the same session object it was registered with by calling:

```
session.removeEventListener(myListener);
```

## Server shutdown event

A new Server API event notification has been added to signal Server shutdown events. This event is available to Server API clients and JMX clients, both in local and remote context. The event type is "di.server.stop" for both the Server API and JMX notification layers. As an additional user data the event object conveys the Server boot time.

## Custom Server API event notifications

New Server API functionality has been added for sending custom, user defined event notifications. The following new call has been added to the local and remote Server API Session objects and also to the `DIServer` MBean so that it can be accessed from the JMX context as well:

```
public void sendCustomNotification (String aType, String ald, Object aData)
```

The invocation of this method will result in broadcasting a new user defined event notification. The parameters that must be passed to this method have the same meaning as the respective parameters of standard Server API notifications. The `aType` parameter specifies the type of the event. The value given by the user will be prefixed with the `user.` prefix. For example if the type passed by the user is `process.X.completed` the type of the event broadcast will be `user.process.X.completed`. A client application can register for all custom events specifying a type filter of `user.*`. The `ald` parameter can be used to identify the object this event originated from. The standard Server API events use this value to specify a Config Instance, AssemblyLine or EventHandler. The `aData` parameter is where the user can pass on any additional data related to this event; if the event is expected to be sent and received in a remote context, this object has to be serializable.

## Getting access to log files

"Starting an AssemblyLine with a listener" on page 473 describes how listeners can be used to get AssemblyLine (or EventHandler) log messages in real time as they are produced.

The Server API provides another mechanism for direct access to log files produced by AssemblyLines or EventHandlers. This mechanism only provides access to the log files generated by the AssemblyLine or EventHandler SystemLog logger.

You don't need a reference to an AssemblyLine or EventHandler Server API object to get to the log file. Also you can access old logs of AssemblyLines/EventHandlers that have terminated.

First you need to get hold of the SystemLog object:

```
SystemLog systemLog = session.getSystemLog();
```

You can then ask for all the log files generated by an AssemblyLine:

```
String[] allLogFileNames = systemLog.getAllLogFileNames("C__Dev_TDI_rs.xml", "TestAL");
if (allLogFileNames != null) {
    System.out.println("Available AssemblyLine log files:");
    for (int i=0; i<allLogFileNames.length; i++) {
        System.out.println(allLogFileNames[i]);
    }
}
```

The `getAllLogFileNames(String aConfigId, String aALName)` method is passed the Config ID (see “Stopping a Config Instance” on page 471 for more details on the Config ID) and the name of the AssemblyLine. This will return an array with the names of all log files generated by runs of the specified AssemblyLine.

If you are interested in the last run of the AssemblyLine only, there is a Server API call that will give you the name of that log file only:

```
String lastALLogFileName = systemLog.getAllLastLogFileName("C__Dev_TDI_rs.xml", "TestAL");
System.out.println("AssemblyLine last log file name: " + lastALLogFileName);
```

When you have got the name of a log file you can retrieve the actual content of the log file:

```
String allLog = systemLog.getAllLog("C__Dev_TDI_rs.xml", "TestAL", lastALLogFileName);
System.out.println("TestAL AssemblyLine log: ");
System.out.println(allLog);
```

In cases where the log file can be huge, you might want to retrieve only the last chunk of the log. The sample code below specifies that only the last 10 kilobytes from the log file should be retrieved:

```
String allLog = systemLog.getAllLogLastChunk("C__Dev_TDI_rs.xml", "TestAL", lastALLogFileName, 10);
System.out.println("Last 10K of the TestAL AssemblyLine log: ");
System.out.println(allLog);
```

The same methods are available for EventHandler log files. Consult the JavaDoc of the `com.ibm.di.api.remote.SystemLog` or `com.ibm.di.api.local.SystemLog` interfaces for the signatures and description of the EventHandler methods.

The Server API also provides methods for cleaning up (deleting) old log files.

You can delete all log files (for all configurations and all AssemblyLines and EventHandlers) older than a specific date. The sample code below will delete all log files older than a week:

```
Calendar calendar = Calendar.getInstance();
calendar.add(Calendar.DATE, -7);
systemLog.cleanAllOldLogs(calendar.getTime());
```

Another criterion you can use for log files clean up is the number of log files for each AssemblyLine or EventHandler. You can specify that you want to delete all log files except the 5 most recent logs for all AssemblyLines and EventHandlers:

```
systemLog.cleanAllOldLogs(5);
```

You can also delete the log files for AssemblyLines only or for EventHandlers only or for a specific AssemblyLine or EventHandler. The same two criteria are available: date and number of log files but in addition you can specify the name of an AssemblyLine or EventHandler or use calls that operate on all AssemblyLines or all EventHandlers only. Consult the JavaDoc of the `com.ibm.di.api.remote.SystemLog` or `com.ibm.di.api.local.SystemLog` interfaces for the signatures and the descriptions of all log clean up methods.

## Server Info

Through the Server API you can get various types of information about the TDI Server itself like the Server version, IP address, operating system, boot time and information about what Connectors, Parsers, EventHandlers and Function Components are installed and available on the Server.

It is the `ServerInfo` object that provides access to this information. You can get the `ServerInfo` object through the session object:

```
ServerInfo serverInfo = session.getServerInfo();
```

You can then get and print out details of the Server environment:

```
System.out.println("Server IP address: " + serverInfo.getIPAddress());
System.out.println("Server host name: " + serverInfo.getHostName());
System.out.println("Server boot time: " + serverInfo.getServerBootTime());
System.out.println("Server version: " + serverInfo.getServerVersion());
System.out.println("Server operating system: " + serverInfo.getOperatingSystem());
```

You can also output a list of all Connectors installed and available on the Server:

```
String[] connectorNames = serverInfo.getInstalledConnectorsNames();
System.out.println("Connectors available on the Server: ");
for (int i=0; i<connectorNames.length; i++) {
    System.out.println(connectorNames[i]);
}
```

You can output more details for each installed Connector including its description and version:

```
String[] connectorNames = serverInfo.getInstalledConnectorsNames();
for (int i=0; i<connectorNames.length; i++) {
    System.out.println("Installed connector: ");
    System.out.println("    name: " + connectorNames[i]);
    System.out.println("    description: " + serverInfo.getConnectorDescription(connectorNames[i]));
    System.out.println("    version: " + serverInfo.getConnectorVersionInfo(connectorNames[i]));
    System.out.println();
}
```

Information for other components can be retrieved in a similar manner – `Parsers`, `Functional Components` and `EventHandlers`.

## Using the Security Registry

The Security Registry is a special Server API object that lets you query what rights a user is granted and whether he/she is authorized to execute a specific action. This is useful if an application is building an authentication and authorization logic of its own – for example the application is using internally a single admin user for communication with the TDI Server and it manages its own set of users and rights.

The Security Registry object is only available to users with the admin role. It is obtained through the session object:

```
SecurityRegistry securityRegistry = session.getSecurityRegistry();
```

You can then check various user rights. For example, `securityRegistry.userIsAdmin("Stan")` will return true if Stan is granted the admin role; `securityRegistry.userCanExecuteAL("User1", "rs.xml", "TestAL")` will return true only if Stan is allowed to execute AssemblyLine "TestAL" from configuration "rs.xml".

Check the JavaDoc of `com.ibm.di.api.remote.SecurityRegistry` for all available methods.

## Custom Method Invocation

You sometimes need to implement your own functionality and be able to access it from the Server API, both locally and remotely. This was supported by the Server API in TDI 6.0, but it needed to be simplified so that you can drop a JAR file of your own in the TDI classpath and then access it from the Remote Server API without having to deal with RMI.

Two methods are now available in the following interfaces:

- `com.ibm.di.api.remote.Session`

- `com.ibm.di.api.local.Session`

The two methods are:

```
public Object invokeCustom(String aCustomClassName, String aMethodName, Object[] aParams)
    throws DIException;
```

and

```
public Object invokeCustom(String aCustomClassName, String aMethodName,
    Object[] aParamsValue, String[] aParamsClass)
    throws DIException;
```

Both methods invoke a custom method described by its class name, method name and method parameters.

These methods can invoke only static methods of the custom class. This is not a limitation, because the static method of the custom class can instantiate an object of the custom class and then call instance methods of the custom class.

The main difference between the two methods is that the `invokeCustom(String, String, Object[], String[])` method requires the type of the parameters to be explicitly set (in the `paramsClass` `String` array) when invoking the method. This helps when you want to invoke a custom method from a custom class, but also want to invoke this method with a null parameter value. Since the parameter's value is null its type can not be determined and so the desired method to be called cannot be determined.

If the you need to invoke a custom method with a null value you must use the `invokeCustom(String, String, Object[], String[])` method, where the desired method is determined by the elements of the `String` array which represents the types and the exact order of the method parameters. If the user uses `invokeCustom(String, String, Object[])` and in the object array put a value which is null than an Exception will be thrown.

### Primitive types handling

These methods do not support the invocation of a method with primitive types of parameter(s). All primitive types in Java have a wrapper class which could be used instead of the primitive type.

### Custom methods with no parameters

If your need to invoke a method which has no parameters you must set the `paramsValue` object array to null (and the `paramsClass` `String` array if the other method is used).

### Errors

Several exceptions may occur when using these methods. Both local and remote sessions support these two methods, but the Server API JMX does not.

### Turning custom invocation on/off

The ability to use `invokeCustom()` methods can be turned on or off (the default is off). This can be done by setting a property in the `global.properties` file named `api.custom.method.invoke.on` to true or false. If the value of this property is set to true then users can use these methods.

### Specifying the classes allowed for custom invocation

There is a restriction on the classes which can be invoked by these Server API methods. In the `global.properties` file there is another property named `api.custom.method.invoke.allowed.classes` which specifies the list of classes which these methods can invoke. If these methods are used and a class which is not in the list of allowed classes is invoked then an exception is thrown. The value of this property is the list of fully qualified class names separated by comma, semicolon, or space.

### Examples

Here are some sample values for these properties:

```
api.custom.method.invoke.on=true
api.custom.method.invoke.allowed.classes=com.ibm.MyClass,com.ibm.MyOtherClass
```

The first line of this example specifies that custom invocation is turned on and thus the two `invokeCustom()` methods are allowed to be used. The second line specifies which classes can be invoked. In this case only `com.ibm.MyClass` and `com.ibm.MyOtherClass` classes are allowed to be invoked. If one of the two `invokeCustom()` methods is used to invoke a different class then an exception is thrown.

### Defaults

The default value of the `api.custom.method.invoke.on` property is `false`. This means that users are not allowed to use the two `invokeCustom()` methods and that an exception would be thrown if any one of these methods is invoked. The default value of the `api.custom.method.invoke.allowed.classes` is empty, in other words, no classes can be invoked. This means that even if custom invocation is turned on no classes can be invoked by the two `invokeCustom()` methods.

### A Full Example

Suppose the following class is packaged in a jar file, which is then placed in the 'jars' folder of TDI:

```
public class MyClass {
    public static Integer multiply(Integer a, Integer b) {
        return new Integer(a.intValue() * b.intValue());
    }
}
```

Suppose the global.properties TDI configuration file contains the following lines:

```
api.custom.method.invoke.on=true
api.custom.method.invoke.allowed.classes=MyClass
```

Then in a client application the 'multiply' method of 'MyClass' can be invoked in a Server API session like this:

```
Integer result = (Integer) session.invokeCustom(
    "MyClass",
    "multiply",
    new Object[] {new Integer(3), new Integer (5)});
```

---

## The JMX layer

The Server API provides a JMX layer. It exposes all Server API calls through a JMX interface locally and remotely (through the JMX Remote API 1.0).

Please refer to the "Remote Server" chapter in the *IBM Tivoli Directory Integrator 6.1.1: Administrator Guide* for information on how to switch on and setup the JMX layer of the Server API for local and remote access.

### Local access to the JMX layer

You can get a reference to the JMX MBeanServer object from the local Server JVM by calling

```
import com.ibm.di.api.jmx.JMXAgent;
import javax.management.MBeanServer;
```

```
...
```

```
MBeanServer jmxMBeanServer = JMXAgent.getMBeanServer();
```

The `getMBeanServer()` static method of the `com.ibm.di.api.jmx.JMXAgent` class will return an `MBeanServer` JMX object that represents an entry point to all MBeans provided by the JMX layer of the Server API. You can also register for JMX notifications with the `MBeanServer` object returned.

**Note:** The `getMBeanServer()` method will throw an Exception if it is called and the JMX layer of the Server API is not initialized.

## Remote access to the JMX layer

The remote JMX access to the Server API is implemented as per the JMX Remote API 1.0 specification.

You have to use the following JMX Service URL for remote access:

```
service:jmx:rmi://<TDI_Server_host>/jndi/rmi://<TDI_Server_host>:<TDI_Server_RMI_port>/jmxconnector
```

You need to replace `<TDI_Server_host>` and `<TDI_Server_RMI_port>` with the host and the RMI port of the TDI Server; for example, `service:jmx:rmi://localhost/jndi/rmi://localhost:1099/jmxconnector`

The sample code below demonstrates how a remote JMX connection can be established:

```
import javax.management.MBeanServerConnection;
import javax.management.remote.JMXConnector;
import javax.management.remote.JMXConnectorFactory;
import javax.management.remote.JMXServiceURL;

...

JMXServiceURL jmxUrl = new
    JMXServiceURL("service:jmx:rmi://localhost/jndi/rmi://localhost:1099/jmxconnector");
JMXConnector jmxConnector = JMXConnectorFactory.connect(jmxUrl);
MBeanServerConnection jmxMBeanServer = jmxConnector.getMBeanServerConnection();
```

Similarly to the local JMX access the `MBeanServerConnection` object is the entry point to all MBeans and notifications provided by the JMX layer of the Server API.

For example, you can list all MBeans available on the JMX Server:

```
Iterator mBeans = jmxMBeanServer.queryNames(null, null).iterator();
while (mBeans.hasNext()) {
    System.out.println("MBean: " + mBeans.next());
}
```

## MBeans and Server API objects

The JMX layer wraps the Server API objects in MBeans. The access to the MBeans is however straightforward - you can directly look up an MBean through the `MBeanServerConnection` object.

There is no session object in the MBean layer (the session and the security checks are managed through the RMI session). The methods for creating, starting and stopping Config Instances that exist in the Server API Session object can be found in the `DIServer` MBean in the JMX layer.

A list of the Server API MBeans available at some time on a TDI Server might look like this:

- `ServerAPI:type=ServerInfo,id=192.168.113.222`
- `ServerAPI:type=ConfigInstance,id=C__Dev_TDI_11_11_fp1_rs.xml`
- `ServerAPI:type=AssemblyLine,id=AssemblyLines/longal.618794016`
- `ServerAPI:type=DIServer,id=winserver`
- `ServerAPI:type=SystemLog,id=SystemLog`
- `ServerAPI:type=SecurityRegistry,id=SecurityRegistry`
- `ServerAPI:type=Notifier,id=Notifier`

Each Config Instance, AssemblyLine or EventHandler is wrapped in an MBean. When the Config Instance, AssemblyLine or EventHandler is started the MBean is created automatically and it is automatically removed when the Config Instance, AssemblyLine or EventHandler terminates.

Refer to the JavaDoc of the Java package `com.ibm.di.api.jmx.mbeans` for all available MBeans, their methods and attributes.

## JMX notifications

The JMX layer of the Server API provides local and remote notifications for all Server API events (see “Working with the System Queue” on page 477.)

You have to register for JMX notifications with the Notifier MBean.

The JMX notification types are exactly the same as the Server API notifications:

- `di.ci.start` – Config Instance started
- `di.ci.stop` – Config Instance stopped
- `di.al.start` – AssemblyLine started
- `di.al.stop` – AssemblyLine stopped
- `di.eh.start` – EventHandler started
- `di.eh.stop` – EventHandler stopped
- `di.ci.file.updated` – Configuration file modified
- `di.server.stop` – TDI Server shutdown

## JMX Example - TDI 6.1.1 and MC4J configuration

This example describes how MC4J and TDI can be set up so that MC4J can be used to access the Server API JMX layer from MC4J.

### TDI side

**Set up Remote Server API and JMX:** Set the following properties in `global/solution.properties` file:

```
## Server API properties
## -----
```

```
api.on=true
```

```
api.user.registry=serverapi/registry.txt
api.user.registry.encryption.on=false
```

```
api.remote.on=true
```

```
api.remote.ssl.on=false
```

```
api.remote.ssl.client.auth.on=true
```

```
api.remote.naming.port=1099
```

```
api.truststore=testserver.jks
```

```
{protect}-api.truststore.pass={encr}L79kdqak1afKdAyuCZBmi1GqY/DPfD1Ipo020CVAGx/0ROE2JBUTgZxLjqADXSZJgM3dHg2aW1CRwB+is/WQa+d
```

```
## Specifies a list of IP addresses to accept non SSL connections from (host names are not accepted).
```

```
## Use space, comma or semicolon as delimiter between IP addresses. This property is only taken into account
```

```
## when api.remote.ssl.on is set to false.
```

```
## api.remote.nonssl.hosts=
```

```
api.jmx.on=true
```

```
api.jmx.remote.on=true
```

**Note:** SSL is turned off for easy configuration.

**Start the TDI server from the command line:**

```
D:\TDI>ibmdisrv -d
```

```
CTGDKD435I Remote API successfully started on port:1099, bound to:'SessionFactory'. SSL and Client Authentication are disabled.
CTGDKD111I JMX Remote Server Connector started at: service:jmx:rmi:///localhost/jndi/rmi:///localhost:1099/jmxconnector.
```



## MC4J side

1. Download and install MC4J from <http://sourceforge.net/projects/mc4j/>.
2. Start the **Connect to server ...** wizard

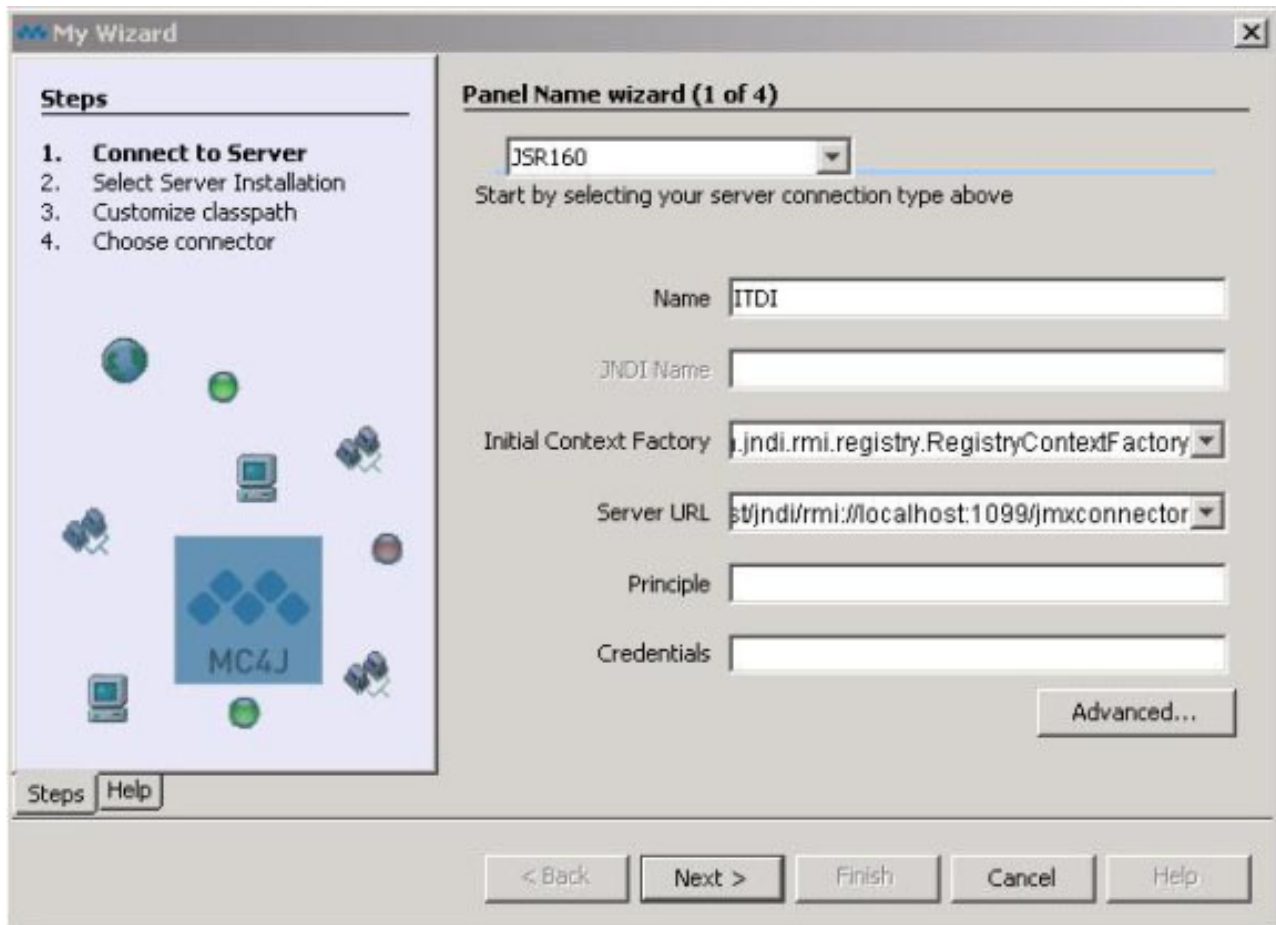


Figure 6.

3. Enter **TDI** in *Name* field.
4. In the **Server URL** text box paste the JMX connection URL dumped by the TDI server on startup

**Note:** If TDI and MC4J are on different machines replace localhost with the TDI machine IP address.

5. Select **Next**.

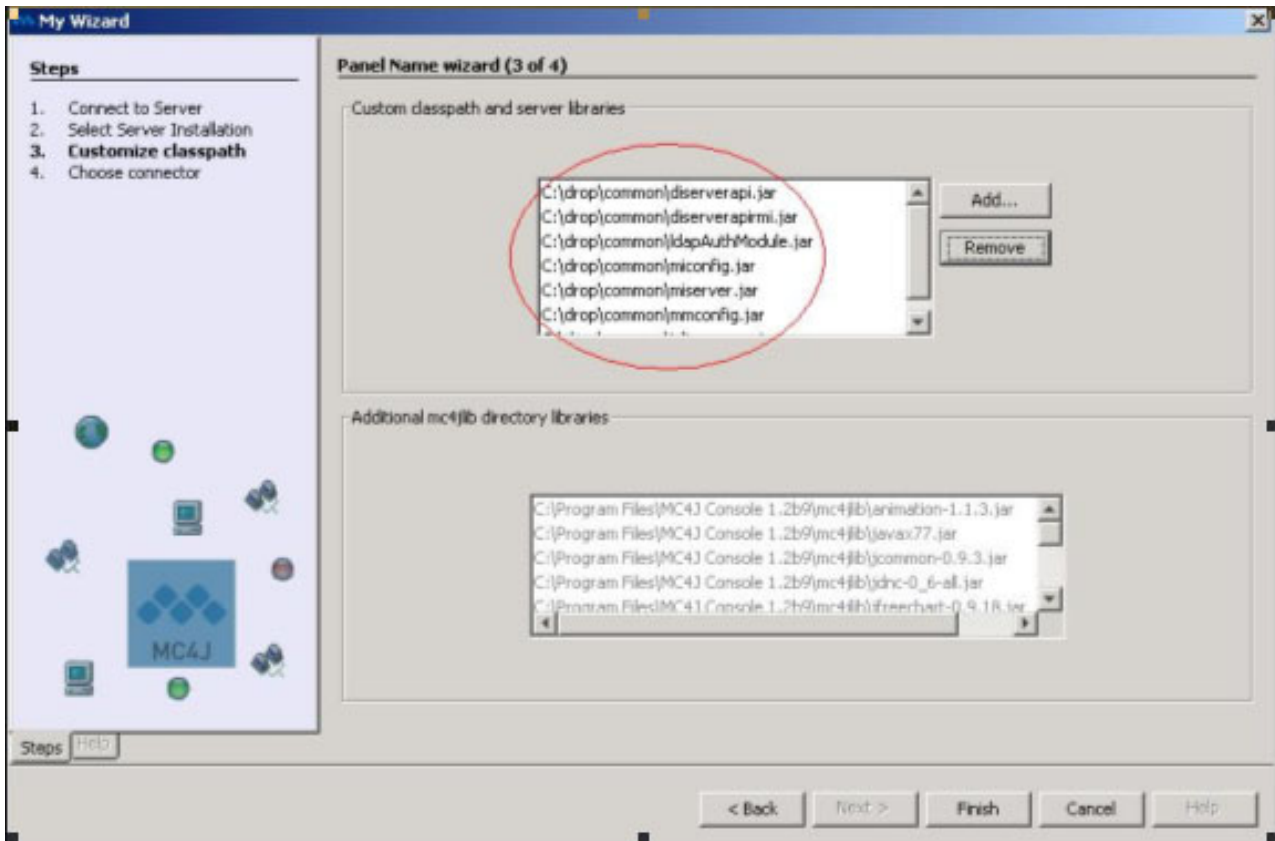


Figure 7.

6. In the **Custom classpath and server libraries** list, add all JAR files from the `<TDI_HOME>\jars\common` folder.
7. Add these three jars as well:
  - `<TDI_home>\jars\3rdparty\others\log4j-1.2.8.jar`
  - `<TDI_home>\jars\3rdparty\IBM\icu4j_3_4_1.jar`
  - `<TDI_home>\jars\3rdparty\IBM\ITLMToolkit.jar`
  - Select **Finish**.

Now MC4J is connected to the TDI server.

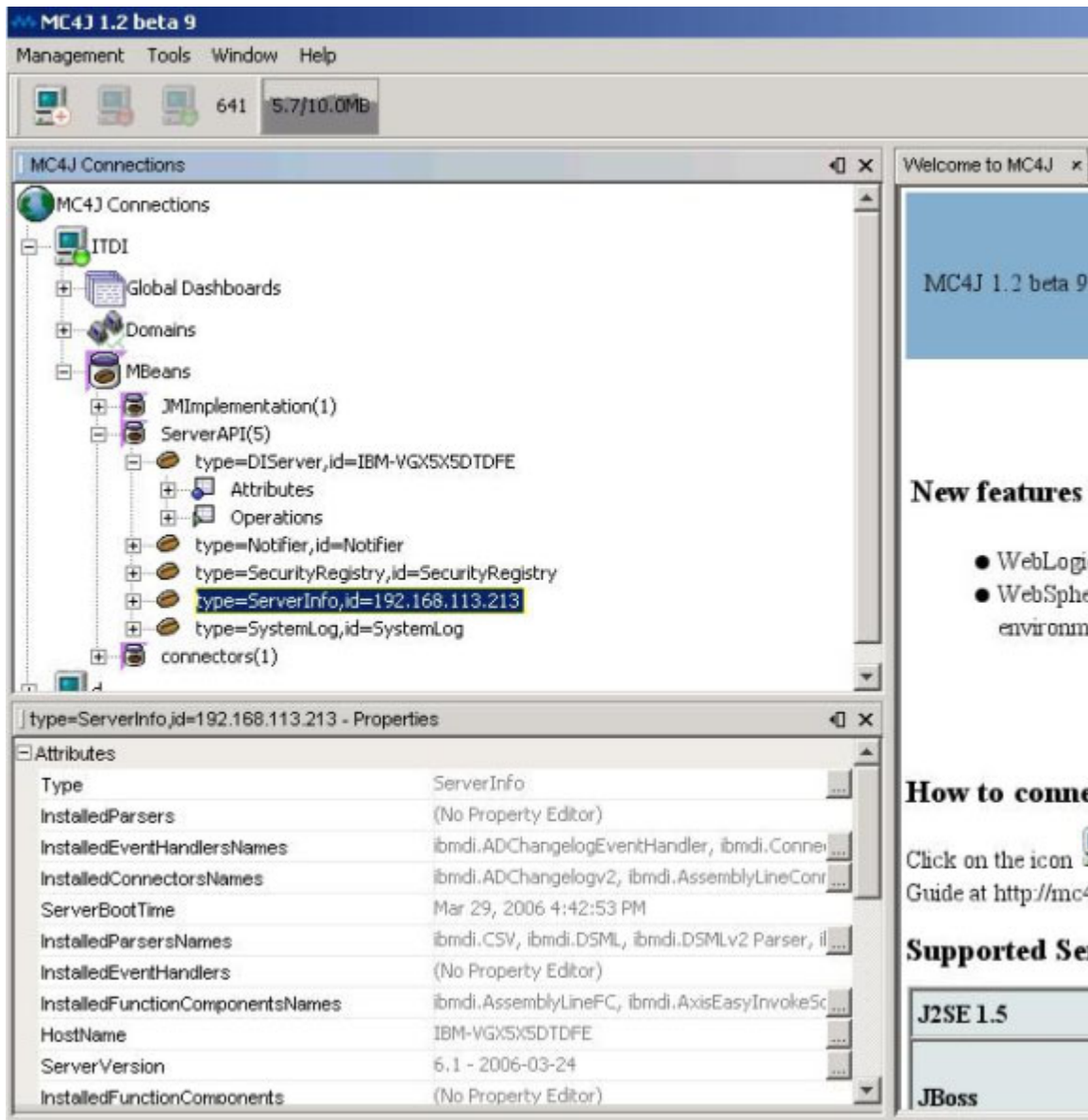


Figure 8.

## Backward compatibility

### Scenarios overview

While upgrading your TDI 6.0 installation to TDI 6.1.1, you may find yourself in one of the following scenarios:

Table 47. Compatibility matrix

| TDI Server version►<br>Client version▼ | 6.0  | 6.1   |
|--|--|---|
| 6.0                                    | OK   | In most cases porting the client to 6.1 is required – see the <i>““Guidelines for porting a TDI 6.0 Server API client to use a TDI 6.1.1 server””</i> section |
| 6.1                                    | OK with some caveats – see the <i>““Guidelines for implementing a Server API client capable of working with both TDI 6.0 and TDI 6.1.1 servers””</i> section | OK  |

## Guidelines for porting a TDI 6.0 Server API client to use a TDI 6.1.1 server

**When is porting required:** Probably the most significant change in the TDI 6.1.1 Server API is the way configurations are edited. For more information on editing configurations in TDI 6.1.1 see the *“Using the Server API -> Editing Configurations”* section.

Server API changes in TDI 6.1.1 relevant to porting a TDI 6.0 Server API client:

- There is a slight behavior change to a configuration editing related method described in *“Table 50 on page 498 - Changed Methods”*.
- If a TDI 6.0 client uses some of the method calls listed in *“Table 51 on page 498 - Deprecated methods”* it needs to be reworked to use the new TDI 6.1.1 methods instead.

Another reason to rework a TDI 6.0 client is to benefit from the functionality introduced in TDI 6.1.1:

- There are several interfaces introduced in TDI 6.1.1 described in *“Table 48 on page 496 – New Server API interfaces”*.
- Some TDI 6.0 interfaces have been added new methods. A list of the new methods can be found in *“Table 49 on page 496 - New methods”*.

Another important consideration while porting a TDI 6.0 client is the usage of serializable classes. More details can be found in the *““Using serializable classes” on page 495”* section. A major part of the serializable classes used by the Server API are the TDI config interface classes. New serializable classes are listed in *“Table 52 on page 498 - New Serializable classes/interfaces”*. A complete reference of the config interfaces can be found in the JavaDocs provided with TDI.

**When is porting optional:** If the TDI 6.0 client does not use config editing and there is no requirement to use the new TDI 6.1.1 Server API features the TDI 6.0 client does not need to be modified.

## Guidelines for implementing a Server API client capable of working with both TDI 6.0 and TDI 6.1.1 servers

Since the enhancements in the Server API are done in a backward compatible manner it is possible a Server API client application to use all TDI 6.0 features against a TDI 6.0 Server and also use all new TDI 6.1.1 features against a TDI 6.1.1 Server. This can be accomplished by having the Server API client check the TDI server version and then execute the appropriate version specific code accordingly. An example is available in the *““Checking the TDI server version” on page 495”* section.

There are two primary ways of sharing data between the Server API client and the TDI server:

- Using RMI remote objects
- Using serializable classes

**Using RMI remote objects:** In this case the Server API client will use remote object stubs generated from the TDI 6.1.1 version of the remote classes. These stubs contain all methods existing in the TDI 6.0 version of the remote classes as well as the methods introduced in TDI 6.1.1 (as they are described in “Table 49 on page 496 - New Methods”):

- The methods introduced in TDI 6.1.1 cannot be used against a TDI 6.0 server. It is the responsibility of the client Server API application not to use these new methods against a TDI 6.0 server by checking the server version beforehand.
- The methods described in “Table 51 on page 498 - Deprecated methods” can only be used with a TDI 6.0 server. If a deprecated method is invoked on a TDI 6.1.1 server an exception will be thrown.

**Using serializable classes:** The Server API serializable classes as well as the TDI serializable classes have evolved from TDI 6.0 to TDI 6.1.1. Thus these classes are different in TDI 6.0 and in TDI 6.1.1. Nevertheless these classes have evolved in a backward compatible way from a serialization perspective. This means that the TDI 6.0 serializable classes can interoperate with the TDI 6.1.1 serializable classes through the Java RMI engine.

The Java RMI engine determines whether serializable classes are compatible by checking the class serial version UID – if the class serial version UID of two classes are identical then the RMI engine considers these two classes compatible. The serial version UIDs of the serializable classes in TDI can be found in “Table 53 on page 499 – serialVersionUID for serializable classes”. Since the TDI 6.1.1 serializable classes are compatible with the TDI 6.0 serializable classes the serial version UIDs of these classes have not changed.

“Table 52 on page 498 - New Serializable classes/interfaces” lists classes and interfaces introduced in TDI 6.1.1. Since these classes and interfaces are not available in TDI 6.0 they cannot be used against a TDI 6.0 server. The TDI JavaDocs should be referred to for more detailed information on method signature changes of serializable classes in both releases. Methods which are not available in TDI 6.0 cannot be used against a TDI 6.0 server.

If the Server API client uses third party or custom user serializable classes then the best approach would be to ensure that these classes are identical on the server and on the client. If for any reason the serializable classes are different (but compatible) versions of the same class then the client still can work if both versions are set the same serialVersionUID. More information on maintaining and evolving serializable classes can be found at:

<http://java.sun.com/j2se/1.5.0/docs/api/java/io/Serializable.html>

<http://java.sun.com/j2se/1.5.0/docs/guide/serialization/spec/serialTOC.html>

[http://www-03.ibm.com/developerworks/blogs/page/woolf?entry=serialization\\_and\\_serial\\_version\\_uid](http://www-03.ibm.com/developerworks/blogs/page/woolf?entry=serialization_and_serial_version_uid)

**Config Editing:** Config editing in TDI 6.1.1 is very different from config editing in TDI 6.0. That is why special care must be taken when coding editing TDI configs for both TDI 6.0 and TDI 6.1.1 servers. This code is TDI version-specific. That is why the code needs to be branched by checking the TDI server version as described in the ““Checking the TDI server version”” section.

**Authentication mechanisms:** The username/password based authentication mechanism and the LDAP authentication mechanism are not supported on TDI 6.0. That is why the createSession (String aUserName, String aPassword) method of the com.ibm.di.api.remote.SessionFactory interface will fail if invoked against a TDI 6.0 server.

**Checking the TDI server version:** Usually most of the Server API client code will be common for TDI 6.0 and TDI 6.1.1 servers. Sometimes, however, TDI 6.0- or TDI 6.1.1-specific code could be needed. These version-specific portions of code require checking the server version. Below is a code sample which demonstrates how the TDI server version can be retrieved and used.

```
import com.ibm.di.api.remote.Session;
import com.ibm.di.api.remote.ServerInfo;
```

```

...
ServerInfo serverInfo = session.getServerInfo();
if (serverInfo == null) {
    throw new Exception("Server version information is not available!");
}

String serverVersion = serverInfo.getServerVersion();
if (serverVersion.startsWith("6.1")) {
    // TDI 6.1 specific code
}
else if (serverVersion.startsWith("6.0")) {
    // TDI 6.0 specific code
}
else {
    throw new Exception("Unsupported TDI server version: " + serverVersion);
}

```

## Server API changes in TDI 6.1.1

Table 48. New Server API interfaces

| Name             | Description                          |
|------------------|--------------------------------------|
| SystemQueue      | Server API access to SystemQueue     |
| TDIProperties    | Wrapper for External Property Stores |
| TombstoneManager | Access to Tombstones read and delete |

Table 49. New Methods

| Name   | Description   |
|--|---|
| <b>AssemblyLine</b>  |   |
| String getGlobalUniqueID ()                                      | Returns AssemblyLine GUID. The GUID is a string value that is unique for each component ever created by a particular TDI Server.        |
| <b>ConfigInstance</b>  |   |
| String getGlobalUniqueID ()                                      | Returns the Config Instance GUID. The GUID is a string value that is unique for each component ever created by a particular TDI Server. |
| String[] getConnectorPoolNames ()                                | Returns the names of all Connector Pools in the Config Instance.  |
| int getConnectorPoolSize (String aConnectorPoolName)             | Returns the size of the specified Connector Pool.   |
| int getConnectorPoolFreeNum (String aConnectorPoolName)          | Returns the number of free Connectors in the specified Connector Pool.  |
| PoolDefConfig getConnectorPoolConfig (String aConnectorPoolName) | Returns the Connector Pool configuration object.  |
| int purgeConnectorPool (String aConnectorPoolName)               | Unused Connectors will be released so that the Pool is shrunk to its minimum size.  |
| TDIProperties getTDIProperties()                                 | Returns the TDIProperties object associated with the current configuration.   |
| <b>EventHandler</b>  |   |
| String getGlobalUniqueID ()                                      | Returns EventHandler GUID. The GUID is a string value that is unique for each component ever created by a particular TDI Server.        |
| <b>Session</b>   |   |
| void shutDownServer (int aExitCode)                              | Shuts down the TDI Server with the specified exit code.   |

Table 49. New Methods (continued)

| Name   | Description   |
|--|---|
| TombstoneManager getTombstoneManager ()  | Returns the TombstoneManager object. Tombstones can be queried and cleared through this object.   |
| boolean isSSLon ()   | Checks if current session is over SSL.  |
| boolean releaseConfigurationLock(String aRelativePath)   | Administratively releases the lock of the specified configuration. This call can be only executed by users with the admin role.   |
| boolean undoCheckOut(String aRelativePath)   | Releases the lock on the specified configuration, thus aborting all changes being done. This call can only be executed from a user that has previously checked out the configuration and only if the configuration lock has not timed out.  |
| ArrayList listConfigurations(String aRelativePath)   | Returns a list of the file names of all configurations in the specified folder. The configurations file paths returned are relative to the Server configuration codebase folder.  |
| ArrayList listFolders(String aRelativePath)  | Returns a list of the child folders of the specified folder.  |
| ArrayList listAllConfigurations()  | Returns a list of the file names of all configurations in the directory subtree of the Server configuration codebase folder. The configurations file paths returned are relative to the TDI Server configuration codebase folder.   |
| MetamergeConfig checkOutConfiguration (String aRelativePath)                                       | Checks out the specified configuration. Returns the MetamergeConfig object representing the configuration and locks that configuration on the Server.   |
| MetamergeConfig checkOutConfiguration (String aRelativePath, String aPassword)                     | Checks out the specified password protected configuration. Returns the MetamergeConfig object representing the configuration and locks that configuration on the Server.  |
| ConfigInstance checkOutConfigurationAndLoad (String aRelativePath)                                 | Checks out the specified configuration and starts a temporary Config Instance on the Server.  |
| ConfigInstance checkOutConfigurationAndLoad (String aRelativePath, String aPassword)               | Checks out the specified configuration and starts a temporary Config Instance on the Server.  |
| void checkInConfiguration (MetamergeConfig aConfiguration, String aRelativePath)                   | Saves the specified configuration and releases the lock. If a temporary ConfigInstance has been started on check out, it will be stopped as well.   |
| void checkInAndLeaveCheckedOut (MetamergeConfig aConfiguration, String aRelativePath)              | Checks in the specified configuration and leaves it checked out. The timeout for the lock on the configuration is reset.  |
| void checkInConfiguration (MetamergeConfig aConfiguration, String aRelativePath, boolean aEncrypt) | Encrypts and saves the specified configuration and releases the lock. If a temporary Config Instance has been started on check out, it will be stopped as well.   |
| MetamergeConfig createNewConfiguration (String aRelativePath, boolean aOverwrite)                  | Creates a new empty configuration and immediately checks it out. If a configuration with the specified path already exists and the aOverwrite parameter is set to false the operation will fail and an Exception will be thrown.  |
| ConfigInstance createNewConfigurationAndLoad (String aRelativePath, boolean aOverwrite)            | Creates a new empty configuration, immediately checks it out and loads a temporary Config Instance on the Server. If a configuration with the specified path already exists and the aOverwrite parameter is set to false the operation will fail and an Exception will be thrown. |

Table 49. New Methods (continued)

| Name   | Description   |
|--|---|
| boolean isConfigurationCheckedOut (String aRelativePath)   | Checks if the specified configuration is checked out on the Server.   |
| void sendCustomNotification (String aType, String aId, Object aData)   | Sends a custom, user defined notification to all registered listeners.  |
| SystemQueue getSystemQueue()   | Gets the remote Server API SystemQueue representation object  |
| String getConfigFolderPath()   | Gets the value of the api.config.folder property in the remote server as a complete path. If not set, then returns an empty string. |
| Object invokeCustom (String aCustomClassName, String aMethodName, Object[] aParams)                            | Invokes the specified method from the specified class.  |
| Object invokeCustom (String aCustomClassName, String aMethodName, Object[] aParamsValue,String[] aParamsClass) | Invokes the specified method from the specified class.  |
| <b>SessionFactory</b>  |   |
| Session createSession (String aUserName, String aPassword)   | Creates a session object with the specified username and password.  |

Table 50. Changed Methods

| Name   | Description   |
|--|---|
| <b>ConfigInstance</b>                                  |   |
| void setConfiguration (MetamergeConfig aConfiguration) | In TDI 6.1.1 this method can be invoked only if a particular client has already checked out same config with temporary config instance. |

Table 51. Deprecated methods (these are methods which are not to be used against a TDI 6.1.1 server; it is perfectly OK to use these methods against a TDI 6.0 server)

| Name   | Description                         |
|--|-------------------------------------|
| <b>ConfigInstance</b>  |                                     |
| void saveConfiguration ()  | Use CheckIn methods instead of save |
| void saveConfiguration (boolean aEncrypt)  | Use CheckIn methods instead of save |
| void setExternalProperties (ExternalPropertiesConfig aExPropConfig)              | Use TDIProperties                   |
| void setExternalProperties (String aKey, ExternalPropertiesConfig aExPropConfig) | Use TDIProperties                   |
| void saveExternalProperties ()   | Use TDIProperties                   |

Table 52. New Serializable classes/interfaces

| Name  | Description           |
|---|-----------------------|
| com.ibm.di.api.Tombstone                        | 5178569311755396746L  |
| com.ibm.di.api.CIEvent                          | 5178569311755396746L  |
| com.ibm.di.config.interfaces.NamespaceEvent     | -1857414661726671152L |
| com.ibm.di.config.interfaces.OperationConfig    | 2715909691453046036L  |
| com.ibm.di.config.interfaces.PoolDefConfig      | -1252371938517765606L |
| com.ibm.di.config.interfaces.PoolInstanceConfig | 5594919717769030291L  |



Table 52. New Serializable classes/interfaces (continued)

| Name   | Description           |
|--|-----------------------|
| com.ibm.di.config.interfaces.PropertyManager     | 4280805548502266432L  |
| com.ibm.di.config.interfaces.PropertyStoreConfig | -2620929677558833640L |
| com.ibm.di.config.interfaces.ReconnectConfig     | -7935628947261477628L |
| com.ibm.di.config.interfaces.TDIProperties       | -3361471837888677277L |
| com.ibm.di.config.interfaces.TDIPropertyStore    | 198251115520372634L   |
| com.ibm.di.config.interfaces.TombstonesConfig    | -3260102686391332434L |

Table 53. serialVersionUID for serializable classes

| Name   | Status   | serialVersionUID      |
|--|--|-----------------------|
| com.ibm.di.api.ALEvent                                   | backward compatible                                      | 5631772256973692972L  |
| com.ibm.di.config.base.ALMappingConfigImpl               | backward compatible                                      | 2712493657450710788L  |
| com.ibm.di.server.ALState                                | backward compatible                                      | 669938312260868491L   |
| com.ibm.di.config.base.AssemblyLineConfigImpl            | backward compatible                                      | 2715909691453046036L  |
| com.ibm.di.entry.Attribute                               | backward compatible                                      | 6675881744901860329L  |
| com.ibm.di.config.base.AttributeMapConfigImpl            | backward compatible                                      | -2619015538178665684L |
| com.ibm.di.entry.AttributeValue                          | backward compatible                                      | 100100L               |
| com.ibm.di.config.base.BaseConfigurationImpl             | known issue – see the “Known issues” on page 500 section | -7316979979253125005L |
| com.ibm.di.config.base.BranchConditionImpl               | backward compatible                                      | -4091773233583817912L |
| com.ibm.di.config.base.BranchingConfigImpl               | backward compatible                                      | -1013588884381133944L |
| com.ibm.di.config.base.CallConfigImpl                    | backward compatible                                      | -4697458497835329096L |
| com.ibm.di.config.base.CallParamConfigImpl               | backward compatible                                      | 5788021154714741767L  |
| com.ibm.di.config.base.CheckpointConfigImpl              | backward compatible                                      | -8342369881523468483L |
| com.ibm.di.config.base.ConfigCache                       | backward compatible                                      | -3311255731504174416L |
| com.ibm.di.config.base.ConfigStatistics                  | backward compatible                                      | -1271645457384911249L |
| com.ibm.di.config.base.ConnectorConfigImpl               | backward compatible                                      | 4093376456212230000L  |
| com.ibm.di.config.base.ConnectorSchemaConfigImpl         | backward compatible                                      | 930161291800752910L   |
| com.ibm.di.config.base.ConnectorSchemaItemConfigImpl     | backward compatible                                      | -1665598194757295769L |
| com.ibm.di.config.base.ContainerConfigImpl               | backward compatible                                      | -4134004409592694052L |
| com.ibm.di.config.base.DeltaConfigImpl                   | backward compatible                                      | -7250128484588024017L |
| com.ibm.di.api.DIEvent                                   | backward compatible                                      | -8664533477452491219L |
| com.ibm.di.api.EHEvent                                   | backward compatible                                      | -1690270461263918159L |
| com.ibm.di.entry.Entry                                   | backward compatible                                      | -5961424529378625729L |
| com.ibm.di.config.base.EventHandlerActionConfigImpl      | backward compatible                                      | -1798497078340945864L |
| com.ibm.di.config.base.EventHandlerActionItemConfigImpl  | backward compatible                                      | 7669745504897906857L  |
| com.ibm.di.config.base.EventHandlerConditionConfigImpl   | backward compatible                                      | 1427205408043312536L  |
| com.ibm.di.config.base.EventHandlerConfigImpl            | backward compatible                                      | -4274035078726148643L |
| com.ibm.di.config.interfaces.ExternalPropertiesDelegator | known issue – see the “Known issues” on page 500 section | 7725187425731381660L  |

Table 53. serialVersionUID for serializable classes (continued)

| Name   | Status              | serialVersionUID      |
|--|---------------------|-----------------------|
| com.ibm.di.config.base.ExternalPropertiesImpl            | backward compatible | -5837658758525300221L |
| com.ibm.di.config.base.FormConfigImpl                    | backward compatible | -8761349695805705052L |
| com.ibm.di.config.base.FormItemConfigImpl                | backward compatible | -7825109041707716857L |
| com.ibm.di.config.base.FunctionConfigImpl                | backward compatible | 5778585850194005910L  |
| com.ibm.di.config.interfaces.GlobalRef                   | backward compatible | 366178307603105225L   |
| com.ibm.di.config.base.HookConfigImpl                    | backward compatible | -1300997546910640256L |
| com.ibm.di.config.base.HooksConfigImpl                   | backward compatible | -9160883008989377612L |
| com.ibm.di.config.interfaces.InheritanceLoopException    | backward compatible | -5977834080357995975L |
| com.ibm.di.config.base.InheritConfigImpl                 | backward compatible | 9015532163983199487L  |
| com.ibm.di.config.base.InstanceConfigImpl                | backward compatible | -7052997089129596762L |
| com.ibm.di.config.base.LibraryConfigImpl                 | backward compatible | -6737181973806281819L |
| com.ibm.di.config.base.LinkCriteriaConfigImpl            | backward compatible | -9206856536172011821L |
| com.ibm.di.config.base.LinkCriteriaItemImpl              | backward compatible | -952539248920610452L  |
| com.ibm.di.config.base.LogConfigImpl                     | backward compatible | 3371411072185625170L  |
| com.ibm.di.config.base.LogConfigItemImpl                 | backward compatible | 6299750464788808971L  |
| com.ibm.di.config.base.LoopConfigImpl                    | backward compatible | -8174541074510481418L |
| com.ibm.di.config.base.MetamergeConfigImpl               | backward compatible | -3363695330685967904L |
| com.ibm.di.config.xml.MetamergeConfigXML                 | backward compatible | -4403169711579029765L |
| com.ibm.di.config.base.MetamergeFolderImpl               | backward compatible | 6107586753523140220L  |
| com.ibm.di.config.base.NamespaceConfigImpl               | backward compatible | 986964857890827079L   |
| com.ibm.di.config.base.ParserConfigImpl                  | backward compatible | 5497221494799800099L  |
| com.ibm.di.config.base.PropertyConfigImpl                | backward compatible | -2620929677558833640L |
| com.ibm.di.config.base.RawConnectorConfigImpl            | backward compatible | 8439049716964119460L  |
| com.ibm.di.config.base.SandboxConfigImpl                 | backward compatible | -399320124155373314L  |
| com.ibm.di.config.base.SchemaConfigImpl                  | backward compatible | 1778816095104785134L  |
| com.ibm.di.config.base.SchemaItemConfigImpl              | backward compatible | 5168801947811376566L  |
| com.ibm.di.config.base.ScriptConfigImpl                  | backward compatible | -7747686242551793890L |
| com.ibm.di.api.remote.impl.rmi.SSLRMIClientSocketFactory | backward compatible | 5083017546031420384L  |
| com.ibm.di.server.TaskCallBlock                          | backward compatible | 115072761837771375L   |
| com.ibm.di.server.TaskStatistics                         | backward compatible | 2098518046376889585L  |
| com.ibm.di.api.remote.impl.rmi.RMISocketFactory          | backward compatible | -3200652858929712303L |

## Known issues

### com.ibm.di.config.interfaces.ExternalPropertiesDelegator

The `com.ibm.di.config.interfaces.ExternalPropertiesDelegator` class is the implementation class of the `com.ibm.di.config.interfaces.ExternalPropertiesConfig` interface. The `com.ibm.di.config.interfaces.ExternalPropertiesDelegator` class also extends the `com.ibm.di.config.base.BaseConfigurationImpl` class.

Server API client code deals with interfaces and not classes, that is why the `ExternalPropertiesDelegator` class is not directly referenced in the Server API client source code. The limitation is that while a TDI 6.0

client can retrieve an `ExternalPropertiesConfig` object from a TDI 6.0 server, this client cannot modify the external properties on the server by calling the `setExternalProperties(String aKey, ExternalPropertiesConfig aExPropConfig)` or the `setExternalProperties(ExternalPropertiesConfig aExPropConfig)` on a config instance object (`com.ibm.di.api.remote.ConfigInstance`). If one of these methods is invoked from a TDI 6.1.1 client against a TDI 6.0 server it will fail.

### **com.ibm.di.config.base.BaseConfigurationImpl**

The same issue as the above one discussed for `com.ibm.di.config.interfaces.ExternalPropertiesDelegator` applies to `com.ibm.di.config.base.BaseConfigurationImpl` as well. (The former is an extension of the latter.)



---

## Appendix D. Implementing your own Components

This chapter is intended for developers that are tasked with creating new Connectors or Function Components for IBM Tivoli Directory Integrator (TDI). They should have a firm understanding of TDI operations as well as experience in developing with the Java language.

This material does not describe how to develop parsers, and assume that parsing logic is implemented in the component itself. A separate document will be provided to cover this theme.

TDI currently also supports a component type called an EventHandler; however, this type of component is being phased out and replaced by Connectors in Server mode. You should therefore not attempt to implement your own EventHandler, as the framework supporting this type of component may be removed in future versions of TDI.

---

### Support materials for Component development

The `DirectoryConnector.java` file contains Java code which is a helpful examples when reading this tutorial. The file is located in the `root_directory/examples/connector_java` directory.

All java docs for the core TDI classes cited in this chapter are located in the `"/docs/api"` folder of your TDI installation. You can view this documentation by selecting **Help>Low Level API** from within the Config Editor.

---

### Developing a Connector

#### Implementing the Connector's Java source code

All TDI Connectors implement the `"com.ibm.di.connector.ConnectorInterface"` Java interface. This interface provides a number of methods to implement addressing all the possible ways of using a Connector within TDI. Usually the Connectors you write will not require all the options provided by TDI and you will actually need to implement only a subset of the methods presented in the `"ConnectorInterface"` interface. It is the `"com.ibm.di.connector.Connector"` class that makes this possible.

`"com.ibm.di.connector.Connector"` is an abstract class implementing `"ConnectorInterface"` that contains core Connector functionality (for example processing of Connector's configuration) and also provides empty or default implementation to many of the methods from `"ConnectorInterface"`. This allows you to start implementing your Connector by subclassing `"com.ibm.di.connector.Connector"` and focusing on (implementing) only those methods from `"ConnectorInterface"` that provide value in your case, and that are actually necessary for your Connector.

Listed below are the `"ConnectorInterface"` methods that build the backbone of a real Connector, and which you will usually need to implement:

#### Connector's constructor

Required for all Connector modes.

In the constructor you will usually set the name of your Connector (using the `"setName(...)"` method) and define what modes – Iterator, Lookup, AddOnly, Server, etc. – that your Connector supports (using the `"setModes(...)"` methods). For an example of a Connector implementation, look at the `"DirectoryConnector.java"` Connector included in this package.

### **public void initialize (Object object)**

This method is called by the AssemblyLine before it starts cycling. In general anybody who creates and uses a Connector programmatically should call *"initialize(...)"* after constructing the Connector and before calling any other method.

Usually the *"initialize(...)"* method reads the Connector's parameters and makes the necessary preparations for the actual work (creates a connection, etc.) based on the parameter values specified.

### **public void selectEntries ()**

Required for Iterator mode. This method is called only when the Connector is used in Iterator mode, after it has been initialized.

Place in *"selectEntries(...)"* any code you need to execute prior to actually starting to iterate over the Entries. When the Connector operates on a database, that code could be an **SQL SELECT** query that returns a result set; when the Connector operates on an LDAP directory, that code could be a search operation that returns a result set. The result of the *"selectEntries(...)"* (result set, etc.) is later used by the *"getNextEntry(...)"* method to return a single Entry on each call/AssemblyLine iteration. Of course you might not need any preparation to iterate over the Entries (as in the case with the FileSystem Connector) in which case there is no need to implement *"selectEntries(...)"*. By subclassing *"com.ibm.di.connector.Connector"* you will inherit its default implementation that does nothing.

### **public Entry getNextEntry ()**

Required for Iterator mode. This is the method called on each AssemblyLine's iteration when the Connector is in Iterator mode.

It is expected to return a single Entry that feeds the rest of the AssemblyLine.

There are no general guidelines for implementing this method – it all depends on the information this Connector is supposed to access. This method retrieves data from the connected data source and must create an Entry object and populate it with Attributes. For example, a database Connector would read the next record from a table/result set and build an Entry object whose Attributes correspond to the record's fields.

### **public Entry findEntry (SearchCriteria search)**

Required for Lookup, Update and Delete modes. It is called once on each AssemblyLine iteration when the Connector performs a Lookup operation.

This method finds matching data in the connected system based on the "Link Criteria" specified in the Config Editor GUI. For example, a database Connector would execute a **SELECT** query with the appropriate **WHERE** clause based on Link Criteria and then build an Entry from the database record, in the same way as *"getNextEntry()"* does. Please consult the Java Docs for the structure of the SearchCriteria input parameter.

- When the specified link criteria succeeds in finding exactly one Entry, it should return that Entry.
- When the specified link criteria results in either zero or multiple Entries found (that is, anything but a single match), the method should return **NULL**. However, in the case of a multiple entry match, it must still provide the entries found so that they can be accessed from the "On Multiple Entries" Hook.

Use the following implementation pattern to achieve the above required Connector behavior: for each Entry found call Connector's *"addFindEntry(...)"* method. When finished, call *"getFindEntryCount(...)"* to get the number of Entries you have found – if it is 1, return the value returned by *"getFirstFindEntry(...)"* , otherwise return **NULL**.

For example: In a database Connector, *"modEntry(...)"* executes an **SQL UPDATE** query, using the Attributes of the entry parameter as database fields and the SearchCriteria in the search parameter to build the **WHERE** clause.

**public void putEntry (Entry entry)**

Required for AddOnly and Update modes. It is called once on each AssemblyLine iteration when the Connector is used in AddOnly mode, or for Update mode when no matching entry is found in the connected data source.

The goal of this method is to add/save/store the Entry object (passed in as parameter to this method) into the Connector's data source. So, a database Connector would execute an **INSERT SQL** statement using the Entry's Attributes' names and values and table fields names and values.

**public void modEntry (Entry entry, SearchCriteria search, Entry old)**

—or—

**public void modEntry (Entry entry, SearchCriteria search)**

Required for Update mode.

Before discussing the "*modEntry(...)*" method, a short clarification of the Update mode is necessary: When the AssemblyLine encounters a Connector in Update mode, it will first execute Connector's "*findEntry(...)*" method using the specified Link Criteria. If "*findEntry(...)*" finds no matching Entry, then the Connector's "*putEntry(...)*" method is called to add the Entry to the data source. If "*findEntry(...)*" finds exactly one Entry, the Connector's "*modEntry(...)*" method is called. Finally, if the "*findEntry(...)*" method finds more than one Entry, the "On Multiple Entries" hook is executed and depending on what the user specified either no Connector's calls are invoked or one of "*putEntry(...)*", alternatively "*modEntry(...)*" methods is invoked.

As seen above there are two variants of the "*modEntry(...)*" method – one with three and one with two input parameters. The two parameters that you get in both cases are: *entry*, the output mapped *conn* Entry, ready to be written to the data source; and *search*, the SearchCriteria to be used to make the modify call to the underlying system. When this method is invoked by the Update mode logic (the "*update(...)*" method of an AssemblyLineComponent), this will reference the actual SearchCriteria built from the Link Criteria (after evaluation of Attribute values, etc.).

The extra parameter is *old*. This is the original Entry in the data source as it looks right now, before the modification is applied. This information might be useful in certain cases like "rename" operations when you need the old name to perform the rename.

It is up to you to decide which of these methods to use. Of course you could implement both of them. One of them is sufficient for your Connector to support Update mode.

Following the analogy with the database Connector, "*modEntry(...)*" would execute an **SQL UPDATE** query, using the Attributes of the entry parameter as database fields and the data from the search parameter to build the **WHERE** clause of the SQL query.

**public Entry queryReply (Entry entry)**

Required for CallReply mode. It is called once on each AssemblyLine iteration when the Connector is used in CallReply mode.

This mode is appropriate when your Connector participates in some kind of request-response communication. The output mapped *entry* parameter contains the data necessary to perform the "call" or "request" part of the operation. For example, the Web Service Connector builds and transmits a SOAP call based on the Attributes in *entry*. The method then must build and return an Entry object from the reply/response data.

**public void deleteEntry (Entry entry, SearchCriteria search)**

Required for Delete mode.

Delete mode will cause the Connector to perform a "*findEntry(...)*" to try and locate the Entry to be deleted. If the "*findEntry(...)*" method returns exactly one Entry, the "*deleteEntry(...)*" method is called with this Entry and the Link Criteria used in the Lookup as parameters. If "*findEntry(...)*" returns zero or more than one Entries the corresponding Connector hooks are called. Depending on what the user specified in the script code, either nothing more is executed or the "*deleteEntry(...)*" method is called with the Entry specified by the user script via the

AssemblyLineComponent method *setCurrent( entry )*. Unless the current entry is set in the On Multiple Found hook, nothing more happens, and control passes down the AssemblyLine.

Back to our database Connector example, *deleteEntry()* would execute an SQL DELETE statement.

### **public ConnectorInterface getNextClient()**

The *getNextClient()* method is used for Connectors in Server mode to accept a client request. This method usually blocks until a client request arrives. When a request is received it creates and returns a new instance of itself. This new instance is then handed over to the AssemblyLine that spawns a new AssemblyLine thread for that Connector instance. The AssemblyLine then calls the *getNextEntry()* method on this new Connector instance in the new thread until there are no more Entries for processing. Right after the *getNextClient()* method returns and the AssemblyLine spawns a new thread to handle the client request, the AssemblyLine calls again *getNextClient()* to accept the next client request.

Since Connectors in Server mode handle client requests which require a response, the AssemblyLine will call the *replyEntry(...)* Connector method at the end of the AssemblyLine. Use this method to place your code that returns response to the client. In case your Connector might need to return multiple responses on a single request you can code the *putEntry(...)* method so that it returns an individual response Entry. In this case it will be the responsibility of the AssemblyLine developer to call the *putEntry(...)* method of the Connector by scripting and this fact has to be documented in the Connector's documentation.

When implementing a Connector in Server mode, you also have to take care about terminating the Connector on external request. Place your termination code in the *terminateServer()* method. Take into consideration that this method can be called on the master Connector instance that accepts client requests and also on a child Connector instance processing a client request. In both cases proper termination should happen: it is usually a good termination practice to stop accepting new requests from the master Server Connector instance but let all child Connectors finish their processing. The *terminateServer()* method usually sets some flag that is checked by the *getNextClient()* method of the master Server Connector instance – if termination is requested the *getNextClient()* method will return NULL. This is a signal to the AssemblyLine that this Server Connector has terminated and the AssemblyLine will not call anymore its *getNextClient()* method.

### **public void terminate ()**

The *terminate(...)* method is called by the AssemblyLine after it has finished cycling and before it terminates. You would put here any cleanup code, that is, release connections, resources that you created in the *initialize(...)* method or later during processing.

The methods listed above are the core *ConnectorInterface* methods that bring life to your Connector. And remember, you only need to implement the methods corresponding to the Connector modes that your Connector will support.

*ConnectorInterface* also provides other methods that address aspects of the possible use of a Connector and which you might want to implement. One example is *querySchema(...)*. This method returns the schema of the connected data source. If you implement it, the Config Editor presents the returned values as the Connector's Schema.

These return values are stored as a Vector of Entry objects, one for each column/attribute in the schema. For example, a database Connector would return one Vector for each column in the connected database table.

Each Entry in the Vector returned should contain the following attributes:

|               |   |
|---------------|---|
| <b>name</b>   | The name of the attribute (column, field, etc.)   |
| <b>syntax</b> | The syntax (like <b>VARCHAR</b> or <b>TIMESTAMP</b> ) or expected value type of this attribute. |



|      |   |
|------|---|
| size | If specified, this will give the user a hint as to how long the field may be. |
|------|---|

Specified by: *querySchema* in ConnectorInterface

Parameters: *source* - The object on which to discover schema. This may be an Entry or a string value

Returns: A vector of *com.ibm.di.entry.Entry* objects describing each entity, or in the case of error, a *java.lang.Exception* is thrown.

## Using a Parser in your Connector

If your connector extends the base implementation of the TDI connector (*com.ibm.di.connectors.Connector*), you can invoke the *initParser()* method to initialize the associated parser:

```
/**
 * Initialize the connector's parser with input and output streams. If the parser
 * has not been loaded then an attempt is made to load it. The input and output objects
 * may be Stream objects (InputStream,OutputStream), java.io.Reader object, String object,
 * java.net.Socket, byte and character array objects.
 *
 * @param is The input object.
 * @param os the output object.
 * @exception Any exception thrown by the parser
 * @see #getParser
 */
public void initParser (Object is, Object os) throws Exception;
```

You have to provide the input and/or output streams the parser will use for its read/write operations. The mode of your connector typically determines which way the flow goes (note that your *initialize(Object obj)* connector method will have the connector mode in the "obj" object). You are not required to initialize the parser at the time of connector initialization, but you should do so unless there is a good reason to initialize it elsewhere. In any case you should invoke the *initParser()* method to properly initialize the parser with logging objects, debug flags and other standard TDI objects/behaviors.

The parser can be chosen either by the user or you can hide the parser selection and either provide the configuration in your "idi.inf" file or programmatically configure the parser in your connector (or both).

### 1. Let the user choose the parser.

In this case you must define a parameter in your connector's "idi.inf" file that activates the "Parser Config" tab in the configuration editor. Once this field is defined the selection of the parser is delegated to the user through a standard user interface (note that you can prefill the parserConfig section of your idi.inf file with a default parser). Here is a snippet from the FileSystem connector's "idi.inf" file showing "parserOption" as "Required", which means the connector requires a parser (that is, an error is thrown if none is defined in the configuration):

```
[connectors ibmdi.FileSystem]
connectorConfig {
  connectorType:com.ibm.di.connector.FileConnector
  parserOption:Required
  filePath:
  fileAwaitDataTimeout:
  etc .....
```

The value for the "parserOption" parameter can be "Required" or "Useless" (no parser allowed).

### 2. Use a predefined parser using the "idi.inf" file.

You can include the parserConfig section in your "idi.inf" file if you always use the same parser:

```
[connectors myconnector]
parserConfig {
  parserType:<name of parser class>
  <custom parameters>
```

```

    etc...
}
connectorConfig {
    connectorType:<name of connector class>
    parserOption:Required
    <custom parameters>

```

or as an alternative you can reuse the system library of parsers using the "inheritFrom" keyword:

```

[connectors myconnector]
parserConfig {
    inheritFrom:system:/Parsers/ibmdi.CSV
    <optional/additional parameters to make the parser functional (e.g. field separator etc)>
}

```

### 3. Configure the parser at runtime.

Your connector has access to the ConnectorConfig object via the *Connector.getConfiguration()* method. Through the ConnectorConfig object you can obtain the ParserConfig interface object for the connector. Use that object to configure the parser before you invoke the *initParser()* method:

```

import com.ibm.di.config.interfaces.ConnectorConfig;

public void initialize(Object obj) throws Exception {

    // Check mode
    String mode = "" + obj;
    boolean isIterator = mode.equals(ConnectorConfig.ITERATOR_MODE);

    ConnectorConfig cc = (ConnectorConfig)getConfiguration();

    // Get the parser config object
    ParserConfig parser = cc.getParserConfig();

    // -- use the csv parser and set the column separator parameter
    parser.setParameter("parserType", "com.ibm.di.parser.CSVParser");
    parser.setParameter("csvColumnSeparator", "\t");

    if(isIterator)
        initParser(inputStream, null);
    else
        initParser(null, outputStream);
}

```

Once the parser has been initialized you can invoke the *readEntry()* and *writeEntry()* methods to translate com.ibm.di.entry.Entry objects to and from the stream format defined by the parser. You typically invoke the *readEntry()* method in your *getNextEntry()* method and the *writeEntry* method from your *putEntry* method. You obtain the parser interface handle through the *getParser()* method.

### 4. Optional parser and dynamic reinitialization

If your connector can function with or without a parser you can invoke the *hasParser()* method to determine whether a parser is configured or not:

```

if(hasParser())
    doSomething();

```

If you use multiple instances of the parser during the life time of your connector you should close the parser interface to ensure data is written to the outputstream and that system resources are released. The methods used to re-initialize a parser can differ based on which parser you use but the following method calls should be sufficient for most parsers:

```

// Close parser to release system resources
if(getParser() != null)
    getParser().closeParser();

// assuming you just got a new input stream ... reinitialize the parser
initParser(inputStream, null);

```

When your connector is terminated it will automatically invoke the *closeParser()* method if one is in use by the connector.

## Logging from a Connector

The **com.ibm.di.connector.Connector** class that your Connector will be extending, has a number of methods to enable you to log messages to the AssemblyLine's configured log files. The simplest way of logging is using one of the following methods:

```
/**
 * Log a message to the connector's log. The message is prefixed by the connector's
 * name.
 *
 * @param msg The message to write to the log
 */
public void logmsg(String msg)

/**
 * Log a debug message to the connector's log
 *
 * @param msg The message to write to the log
 */
public void debug(String msg)
```

You can call these methods with code like

```
logmsg("initializing my connector");
```

This will cause your string to be issued to the AssemblyLine's configured log appenders, at INFO level. If you want to do more advanced logging, the **com.ibm.di.connector.Connector** class also has this field:

```
/**
 * The log object for logging messages
 */
protected com.ibm.di.server.Log myLog;
```

This **com.ibm.di.server.Log** class has many methods for logging. You could therefore use the *myLog* object to do logging like this:

```
myLog.logerror("Something very bad happened");
```

This issues a message to the log(s) at ERROR level. There are corresponding methods for logging at different levels, like *loginfo()* and *logfatal()*.

## Building the Connector's source code

When building the source code of your Connector, set up your CLASSPATH to include the jar files from the "jars/common" folder of the IBM Tivoli Directory Integrator installation. At minimum you would need to include "miserver.jar" and "miconfig.jar".

**Note:** When integrating your Java code with IBM Tivoli Directory Integrator, pay attention to the collection of pre-existing components that comprise IBM Tivoli Directory Integrator, notably in the *jars* directory. If your code relies upon one of your own library components that overlap or clash with one or more that are part of the TDI installation there will most likely be loader problems during execution.

## Implementing the Connector's GUI configuration form

### Introduction

When you create a custom TDI component you also have to provide an additional file that describes your component to TDI. This file is located at the root of your jar file and is named *idi.inf*. The syntax and contents of this file is described in this document. Localized versions of this file are provided by inserting the locale identifier in the file name (e.g. *idi\_en.inf*, *idi\_fr.inf* etc).

The first part of this section explains the format of this file and also shows the minimum requirements for a component inf-file.

The second part of this section focuses on the form definition and the various options you have when you define a form. This form definition is used by the TDI configuration editor to let the user configure your component. While the UI options in the form definition are basic and somewhat limited, you can still perform advanced operations using your own custom java based UI components as well as associating scripts with form events.

### idi.inf file format

The ".inf" files are created in the original (that is, IDI 4.6) configuration file format (that is, not XML). The format is a very simple key/value pair file with hashtables and array constructs. These are organized into a tree structure (all lines are trimmed before interpretation) that is used internally by the MetamergeConfig drivers (MetamergeConfigImpl).

The file syntax can be summarized by the following:

- All sections must start with a main section definition and end with a main section terminator

```
[connectors connectorName] Connector main section
```

```
[parsers parserName] Parser main section
```

```
[functions functionName] Function main section
```

```
[end] Main section terminator
```

- If the line ends with an opening curly brace it denotes a named Hashtable
- If the line ends with an opening bracket it denotes an array of values
- Otherwise, it is expected to be a *keyword:value* pair. Keyword/value pairs cannot span lines (e.g. there is no line-continuation character) so you have to add a "\n" if you need a newline in the text.

An example:

```
[connectors CustomConnector]
  connectorConfig {
    connectorType:pub.test.CustomConnector
    options [
      First Value
      Second Value
      Third Value
    ]
    subsection {
      anotherKey:anotherValue
    }
    paramWithNewlines:line 1\nline 2\n line3
  }
[end]
```

The above constructs a Hashtable with one key ("connectorConfig") that contains three named items (mode, options and subsection). This hashtable is added as a connector named CustomConnector to the current configuration (MetamergeConfig object). The specific parameters for your component appear inside the connectorConfig/functionConfig/parserConfig sections. In the above example options, subsection and *paramWithNewlines* are all component specific parameters.

**Basic Component Definitions:** When you first create your inf-file you add the main sections for the components your jar file contains. For each component you add a section where you as a minimum define java class. The syntax is as follows for the three main components:

Table 54.

| Component Type | Minimum Section Contents   |
|----------------|--|
| Connector      | <pre>[connectors CustomConnector] connectorConfig {   connectorType:pub.test.CustomConnector } } [end]</pre>                             |
| Parser         | <pre>[parsertypes CustomParser] parserConfig {   class:com.ibm.di.parser.FixedRecordParser } } [end]</pre>                               |
| Function       | <pre>[functions ibmdi.ComplexTypesGenerator] functionConfig {   javaclass:com.ibm.di.fc.webservice.ComplexTypesGenerator } } [end]</pre> |

In addition you should always include a form definition for each of your components. This is to prevent the configuration editor to report errors of missing forms. If your component has no configurable parameters you should include a form that says so.

**Note:** The current configuration object that the *FormUI* refers to is always the *connectorConfig/parserConfig/functionConfig* object. If you need to access the main component's parameters you should use the "*config.getParent()*" method to obtain for example the ConnectorConfig interface for the configuration.

**Install Location:** When you start either the configuration editor or the server there is a component called the TDI Loader that runs through its configured jar directories looking for \*.jar/\*.zip files that contain an "idi.inf" file at its root level. All these files are concatenated into a single configuration file known as the system templates (the system namespace in configuration terms).

The locations of these files are:

- <TDI\_INSTALL\_DIRECTORY>/jars and any subdirectory therein
- Any files/directories specified by the com.ibm.di.loader.userjars property (etc/global.properties)

When you put your jar file in either of these directories your component will show up in the configuration editor with the name you chose as part of the system namespace.

**Note:** Adding your jar file to the CLASSPATH or PATH alone does not include it in the system templates and hence will not be visible to the user.

## Form description

The form description is used to provide custom input panels for components. While most of the user interface in the configuration editor is static (defined in standard\_templates.cfg / miadmin.jar), most components need specific user interfaces to let the user define its behaviour.

**Component/Form Association:** The form definition defines the input fields and labels that the configuration editor will build when you open the configuration for a component. The binding between the component (e.g. connector, parser) and its form is through the java class of the component. Using the example above, the connectorConfig has a "connectorType" parameter that defines the implementing class for the component (pub.test.CustomConnector). When a component of this type is presented to the user, the configuration editor will look for a form with the same name as the implementing java class.

**Form/Configuration Binding:** When the form has been created it also has a binding object for each parameter to the configuration object. These binding objects will set the initial value of the input field (using the default value provided by the form if the configuration object returns null for the value) and also function as the controller between the input field and the configuration object. When the input field changes its value the binding will update the configuration object and vice versa. The configuration object is read and updated using the primitives of the configuration object (e.g. `BaseConfiguration.getParameter/setParameter`). It is possible to have the binding object invoke specific methods rather than using the primitives, but for component developers this is rarely needed.

**Form Definition:** Forms are defined the same way as components are defined. Below is an example of a form with three input fields and one event handler trapping changes to one of the parameters.

```
[form pub.test.CustomConnector]

title:This is the title/heading that appears at the top of the form

formevents:function firstParameter_changed() { form.alert("First param modified"); }
parameterlist [
  firstParameter
  secondParameter
  $GLOBAL.debug
]
parameters {
  firstParameter {
    label:First Param Label
  }
  secondParameter {
    label:Second Param Label
  }
}
[end]
```

*Form - top level keywords:* At the top level of the form definition you define the overall characteristics of the form.

Table 55.

| Keyword       | Description  |
|---------------|--|
| title         | The heading text for the form.   |
| width/height  | If the form is presented in its own frame (e.g. modal dialog etc) these fields define the size of the frame.   |
| parameterlist | This array defines which parameters are included in the form and order in which they appear. Parameters starting with "\$GLOBAL." refers to commonly used parameter settings, which is defined in the "standard_forms.cfg" resource (miadmin.jar). For each parameter listed here there must be a corresponding subsection in the parameters section.  |
| parameters    | This section contains the specific configurations for each parameter. See parameter definitions next.  |
| formevents    | This keyword lets you define javascript functions that are called when parameter values change. The function name is constructed using the parameter name plus a "_changed" suffix. So to intercept changes to "firstParameter" you would add a function called "firstParameter_changed()". In the function you have access to the "form" object which is the instance of the <code>com.ibm.di.admin.ui.FormUI</code> class shown in the configuration tab of the component. |
| tablist       | This parameter lets you create a multi-form form. The value of the tablist specifies the name of each form which will be created and added as a separate pane to the main form. Each sub-form shares the same configuration object.<br><br>When this parameter is present only the sub-forms are created. That means that any parameterlist/parameters sections are ignored for this form definition.  |

Table 55. (continued)

| Keyword                        | Description   |
|--------------------------------|---|
| <form>.title<br><form>.tooltip | When <i>tablist</i> is specified these parameters define the title and tool tip for each sub-form. If <i>tablist</i> contains the form "A" you can define "A.title" and "A.tooltip" to customize the tab header in the main form. |

*Parameter Definitions:* Each parameter has its own section within the parameters section. In this section you define the characteristics for each parameter.

Table 56.

| Keyword                     | Description   |
|-----------------------------|---|
| label                       | The label appearing in the left column of the form (e.g. LDAP URL)  |
| description                 | The tooltip for the parameter   |
| default                     | Default value for the parameter. The preferred way of providing a default value is in the component configuration itself (in the <i>idi.inf</i> file). This default value will only be set if the user uses the CE to view/modify the configuration for the component.  |
| script<br>script2           | Specifying this parameter adds a button to the right of the input field. When the button is clicked, the named JavaScript function is executed.<br><br><i>Script2</i> allows for a second button to the right of the first one.   |
| scriptLabel<br>scriptLabel2 | The button text   |
| scriptHelp<br>scriptHelp2   | Tooltip for the script button   |
| syntax                      | Specifies the syntax of the parameter. This also affects the choice of UI control used to represent the value. See the syntax section for more info.  |
| values                      | Array of values used to populate dropdown lists. The values can be static or dynamic. Dynamic values are values that the FormUI will gather from configuration objects or from java objects passed to the FormUI when it was instantiated (this is typically config editor specific and not used much by 3rd party devs). See section below for possible macros for dynamic value lists.                                  |
| localizedValues             | Array of <i>display</i> values. This field is only used when the values parameter is provided. Instead of showing the user the text from the values parameter the corresponding value in this array is shown instead (index based). This is often used to provide localized values and/or human readable text for numeric/technical configuration values.   |
| readonly                    | If present and set to "true" the input field is not editable.   |
| reflect                     | If present the binding will use this method to get/set the parameter value. The binding will prepend "get" or "set" accordingly to this value (e.g. specify Name to invoke getName and setName). This is only used when the configuration object performs specific logic when getting/setting a parameter value. For component developers this is rarely needed as component configurations only have get/set primitives. |
| reflectClass                | Optional – in case there are several versions of the reflect method Specifies the conversion class (e.g. java.lang.Boolean) to be used when setting the parameter value (e.g. setValue(boolean) vs setValue(string)).   |
| minValue<br>maxValue        | Used when the parameter syntax is Number. The fields specify the minimum and maximum numeric value.   |
|                             |   |

*Dynamic Values:* The *values* array can contain static and dynamic values. The dynamic values are expanded and added to the array at runtime to populate the dropdown list.

Table 57.

| Value             | Description   |
|-------------------|---|
| @ASSEMBLYLINES@   | Adds all known AssemblyLines to the array   |
| @CONNECTORS@      | Adds all known connectors to the array  |
| @PARSERS@         | Adds all known parsers to the array   |
| @USER.PROPERTIES@ | Adds all known property values to the array   |
| @CONFIG.param     | Retrieves the value for param from the current configuration object and adds it to the array. |

*Syntax:* The syntax for a parameter can be any of the following.

Table 58.

| Value                | Description   |
|----------------------|---|
| String               | This is the default syntax. A one line text field is created for text input.  |
| Password             | A password field is created for text input. Be aware that if the user has configured a password store then FormUI will not insert the value in the configuration object but insert a property reference. The actual value is then stored in the password store.<br><br>If you modify this parameter via script or java code make sure to invoke <i>BaseConfiguration.setProtectedParameter()</i> instead of <i>BaseConfiguration.setParameter()</i> . The <i>setProtectedParameter</i> will automatically create a new property if there isn't one in place already. If the password store is not configured <i>setProtectedParameter</i> will simply invoke <i>setParameter</i> instead. |
| Boolean              | A checkbox is created for true/false values   |
| Droplist<br>Dropedit | Dropdown with values from the values parameter. Dropedit is the editable version where the user also has a text field to specify a custom value. See Dynamic Values for special values.   |
| Fontlist<br>Fontedit | Creates a dropdown list of available fonts  |
| Color                | Creates a Color selection dialog  |
| List                 | Creates a JList showing all values with the selection as the current value  |
| TextArea             | Creates a text area control for multi-line text input   |
| Script               | Creates a button that invokes a script  |
| Static               | Creates a text label for viewing only (same as string w/readonly=true)  |
| Number               | Creates a single-line text input field with validation. Validation includes verifying the input is a valid numeric string in the range defined by <i>minValue</i> and <i>maxValue</i>   |
| EditorWindow         | This syntax causes the form to be a tabbed pane. The non-editorwindow parameters appear in the left most tab whereas each editorwindow parameter has its own tab with an editor input control. Used when you need the complete display area for input (e.g. scripts)  |



Table 58. (continued)

| Value     | Description   |
|-----------|---|
| Component | <p>This enables you to provide your own UI component if you need complex input mechanisms or otherwise want more control over the UI. Specify the java class name in the component keyword that you want inserted into the form:</p> <p><i>syntax:component</i><br/> <i>component:pub.test.CustomUI</i></p> <p>The class is instantiated by FormUI at runtime and should be an AWT or Swing subclass (something that can be added to a JPanel). Also, it must have a constructor as shown in this example:</p> <pre>package pub.test;  import com.ibm.di.admin.ui.FormUI; import com.ibm.di.config.interfaces.BaseConfiguration;  public class CustomUI extends JPanel {     /*      * form – the FormUI object      * config – the config object being modified      * paramname – the parameter of config being edited      */     public CustomUI(FormUI form, BaseConfiguration config,         String paramname) {     } }</pre> |

**Form Scripts:** In your form definitions you can add calls to script functions. These functions execute in the form’s script engine. The form’s script engine provides the following predefined objects:

- **form** Represents the com.ibm.di.admin.ui.FormUI instance managing this form
- **config** A handle to the configuration objects this form operates on (e.g. the connection configuration for a connector, parser config for parser etc)
- **button** The JButton that triggered the script to be invoked
- **util** An instance of the com.ibm.di.admin.ui.Util class
- **system** An instance of the com.ibm.di.function.UserFunctions class

**Multi-Form Definition:** Your component’s inf-file can define more than one form. Often, it is advisable to break a form into several parts (like common, advanced etc) instead of having one form with too many input fields. To accomplish this you basically create a separate form definition for each part and bring them together in the main form. You are free to choose the name of your sub-forms but to avoid name collisions with other components you should use your main form name as base. Here is an example of a multi-form with two sub-forms.

```
[form pub.test.CustomConnector]
  tablist:pub.test.CustomConnector.common, pub.test.CustomConnector.advanced

  pub.test.CustomConnector.common.title:Common Parameters
  pub.test.CustomConnector.common.tooltip:This tab contains the most commonly used params

  pub.test.CustomConnector.advanced.title:Advanced Parameters
  pub.test.CustomConnector.advanced.tooltip:This tab contains special parameters
[end]

[form pub.test.CustomConnector.common]
  (form definition)
[end]
```

```
[form pub.test.CustomConnector.advanced]
(form definition)
[end]
```

## Examples

Look at TDI's components in the configuration editor to find an example you find suitable. Use a zip/jar tool (e.g. winzip, unzip) and extract the "idi.inf" file from the component's jar file (<tdi\_installdir>/jars/components subdirectory).

Also, the "examples/connector\_java" folder of this package contains the "idi.inf" file of the Directory Connector.

## Packaging and deploying the Connector

Now that we have the Connector source code compiled and supplied the "idi.inf" file, we are ready to package and deploy the Connector.

What you need to do is create a jar file (typically with the same name as that of the Connector) and include in it:

1. The class file(s) of the Connector
2. The "idi.inf" file, in the root of the jar file. (You might also include "idi.inf" files for different languages naming them in the standard Java internationalization schema – for example "idi\_de.inf" for German, "idi\_fr.inf" for French, etc.)

After you have created the jar file of the new Connector, you need only drop that jar file in the "jars/connectors" folder of the IBM Tivoli Directory Integrator installation. The next time the system starts up, it will automatically load the new Connector and make it ready for use.

---

## Developing a Function Component

Implementing a Function Component (FC) follows absolutely the same pattern of developing a Connector. A Function Component is actually easier to implement because of fewer dependencies on the AssemblyLine workflow.

### Implementing Function Component Java source code

Similar to the Connector foundation classes, we have "*com.ibm.di.fc.FunctionInterface*" and the "*com.ibm.di.fc.Function*" abstract class that implements the interface (the Java sources of both classes are included in the "fc" folder of this package).

You will usually implement your FCs by subclassing the "*com.ibm.di.fc.Function*" class. These are the most important methods you will usually need to implement:

#### **public void initialize (Object obj)**

Put any initialization code here – reading FC's parameters, allocating resources, etc. When the FC is placed into an AssemblyLine, the AssemblyLine will call the "*initialize(...)*" method once, on startup.

When the FC is created and used programmatically the "*initialize(...)*" method must be called right after constructing the FC object and setting its parameters, and before calling its "*perform(...)*" method.

#### **public Object perform (Object obj)**

The "*perform(...)*" method is the actual implementation of the business logic of your FC. In contrast to the Connector where you have different Connector modes and different methods to implement for each of them (*getNextEntry()*, *findEntry()*, etc.) all that a FC is supposed to do is implemented in the "*perform(...)*" method.

The general contract for the *"perform(...)"* method is that it receives some data on input and based on that input it produces some output data. There are no other assumptions. As you will see below it is not even necessary that your FC works with Entry objects.

When the FC is placed into an AssemblyLine, the AssemblyLine calls its *"perform(...)"* method on each iteration. In the AssemblyLine context the *"perform(...)"* method will be given an Entry object as input parameter (this is the Entry object constructed by the Output Attribute Mapping process). And it is supposed to return an Entry object as well. the AssemblyLine will feed the returned Entry object to the Input Attribute Mapping process, the result of which is applied to the AssemblyLine's work Entry. If you want to enable your FC to be placed into an AssemblyLine, you need to support this "Entry on input – Entry on output" behavior.

You might also code the *"perform(...)"* method so that it receives non-Entry objects on input and returns non-Entry objects on output. This could facilitate the process of programmatically creating and calling an FC. No Attribute Mapping will be done if you use this method.

#### **public void terminate()**

The FC's *"terminate(...)"* method is called by the AssemblyLine after it has finished cycling and before it terminates. You would put here any cleanup code, that is, release connections, resources that you created in the *"initialize(...)"* method or later during processing.

When using an FC programmatically, you must call the *"terminate(...)"* method after you have finished using that FC instance.

#### **public java.awt.Component getUI()**

The *"getUI(...)"* method allows you to build custom graphical user interface for the configuration form of your FC instead of using the standard configuration forms described in "idi.inf" files.

This however is an option. In most cases the standard GUI provided by forms that you can describe in "idi.inf" will be sufficient. It is up to you to decide how to implement it, what visual controls to include and how they map to the FC's parameters

## **Building the Function Component source code**

When building the source code of your Connector, include in your CLASSPATH the jar files from the "jars" folder of the IBM Tivoli Directory Integrator installation. At minimum you would need to include "miserver.jar" and "miconfig.jar".

**Note:** When integrating your Java code with IBM Tivoli Directory Integrator, pay attention to the collection of pre-existing components that comprise IBM Tivoli Directory Integrator, notably in the *jars* directory. If your code relies upon one of your own library components that overlap or clash with one or more that are part of the TDI installation there will most likely be loader problems during execution.

## **Implementing the Function Component GUI configuration form**

You have two options for implementing the FC GUI – use the standard syntax of "idi.inf" file or code your own GUI by implementing the *"getUI(...)"* method.

If you choose to use the standard "idi.inf" mechanism, you describe the FC configuration form by using the same syntax as used for Connectors.

Remember that even if you code a custom GUI by implementing the *"getUI(...)"* method, you still need the "idi.inf" file in the jar file of your FC. The presence of this file tells TDI that this component is an FC and must be loaded.

## Packaging and deploying the Function Component

Packaging and deploying an FC is just like packaging and deploying a Connector:

You need a jar file that contains:

1. The class file(s) of the Function Component
2. "idi.inf" file placed in the root of the jar file (and optionally "idi\_?.inf" files if you want to support different languages)

After you have created the jar file of the new Function Component, you only need to drop that jar file in the "jars/functions" folder in the IBM Tivoli Directory Integrator installation. The next time the IBM Tivoli Directory Integrator is started it will automatically load the new Function Component and it will be ready for use.

---

### See also

Appendix C, "Server API," on page 465

---

## Appendix E. Notices

This information was developed for products and services offered in the U.S.A. IBM might 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 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:

IBM World Trade Asia Corporation Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106-0032, 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 may 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 information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information 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  
Department MU5A46  
11301 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.

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 softcopy, the photographs and color illustrations may not appear.

---

## Third-Party Statements

### ICU License - ICU 1.8.1 and later

#### COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1995-2006 International Business Machines Corporation and others

All rights reserved.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation.

---

## Trademarks

The following terms are trademarks of International Business Machines Corporation in the United States, or other countries, or both:

|         |          |        |            |
|---------|----------|--------|------------|
| IBM     | Tivoli   | AIX®   | Lotus      |
| Notes   | pSeries® | DB2    | WebSphere  |
| OS/390® | Domino   | iNotes | Cloudscape |

Java, JavaScript and all Java-based trademarks and logos are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

Microsoft, Windows, Windows NT and the Windows logo are registered trademarks of Microsoft Corporation.

Intel™ is a trademark of Intel 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.

Linux is a trademark of Linus Torvalds in the U.S., other countries, or both.

This product includes software developed by the Apache Software Foundation (<http://www.apache.org/>).

Other company, product, and service names may be trademarks or service marks of others.









Printed in USA

SC32-2566-01

