



---

Produced in  
collaboration with:  **Redbooks®**

Content in this document was produced in collaboration with IBM® Collaboration Solutions and IBM® Redbooks®.

# Installing and Deploying IBM Connections

**Note:** This PDF document is the original text from the Installing and Deploying IBM Connections hosted in the online wiki. Always refer to the online wiki version for the latest updates.

# Contents

|  |    |
|--|----|
| <b>Preface</b> .....   | i  |
| Meet the authors .....   | ii |
| Special thanks to the following people for contributing to this effort. ....   | iv |
| Become an author .....   | v  |
| Comments welcome .....   | v  |
| Stay connected to IBM Redbooks .....   | vi |
| <br><b>Chapter 1. IBM Connections overview</b> .....                           | 1  |
| 1.1 The software components and their roles .....                              | 3  |
| 1.2 What is new in IBM Connections 4 .....                                     | 5  |
| 1.2.1 Overall .....  | 5  |
| 1.2.2 Installation .....   | 7  |
| 1.2.3 Administration .....   | 8  |
| 1.2.4 Customization .....  | 8  |
| 1.2.5 Security .....   | 8  |
| 1.2.6 Mobile access .....  | 8  |
| 1.3 Architecture Overview .....  | 8  |
| 1.3.1 Functional features .....  | 8  |
| 1.3.2 Operational architecture .....   | 10 |
| <br><b>Chapter 2. General deployment considerations and requirements</b> ..... | 13 |
| 2.1 Architecture considerations .....  | 13 |
| 2.2 Hardware requirements .....  | 15 |
| 2.3 Software requirements .....  | 16 |
| 2.4 Performance considerations .....   | 18 |
| 2.5 Deployment options .....   | 21 |
| 2.5.1 Small deployment .....   | 21 |
| 2.5.2 Medium deployment .....  | 22 |
| 2.5.3 Large deployment .....   | 24 |
| <br><b>Chapter 3. Planning the environment</b> .....                           | 29 |
| 3.1 LDAP .....   | 29 |
| 3.2 DNS and host names .....   | 30 |
| 3.3 Shared content storage location .....                                      | 30 |
| 3.4 LTPA and single sign on .....  | 30 |
| 3.5 SSL certificates .....   | 31 |
| 3.6 Multiple language content .....  | 32 |
| 3.7 Deployment checklist .....   | 32 |

|  |     |
|--|-----|
| <b>Chapter 4. Planning Profiles</b>                                  | 35  |
| 4.1 Photographs  | 35  |
| 4.2 Setting up Manager attributes                                    | 35  |
| 4.3 Cleaning up data sources   | 36  |
| 4.4 Designing profiles   | 36  |
| 4.5 Using profile types for custom profiles by user name             | 36  |
| 4.5.1 Default profile-type   | 37  |
| <b>Chapter 5. Preinstallation tasks</b>                              | 39  |
| 5.1 Verify software requirements                                     | 40  |
| 5.2 Setting up DNS and testing host names                            | 41  |
| 5.3 Setting up LDAP and testing LDAP for data quality                | 42  |
| 5.3.1 LDAP pre-requirements  | 42  |
| 5.3.2 Installing Domino  | 43  |
| 5.4 Populating photo repository                                      | 44  |
| 5.4.1 Populating photo repository                                    | 44  |
| 5.4.2 Enabling profile photo   | 45  |
| 5.5 Verifying operating system installation and disk space available | 47  |
| 5.5.1 Operating system requirements                                  | 47  |
| 5.5.2 Applying operating system patches                              | 48  |
| 5.5.3 Cognos requirements  | 48  |
| 5.5.4 Disk space   | 48  |
| <b>Chapter 6. Product deployment</b>                                 | 51  |
| 6.1 Setting up the Installation Manager                              | 52  |
| 6.2 Installing the database management system                        | 54  |
| 6.3 Installing Tivoli Directory Integrator                           | 63  |
| 6.3.1 Installing Tivoli Directory Integrator                         | 63  |
| 6.3.2 Applying Fix Pack  | 70  |
| 6.4 Installing WebSphere Application Server                          | 70  |
| 6.4.1 WebSphere Application Server deployment                        | 72  |
| 6.4.2 Configuring WebSphere to use LDAP repository                   | 90  |
| 6.4.3 Configuring security on ISC                                    | 95  |
| 6.5 Creating databases   | 97  |
| 6.6 Populating Profiles using population wizard                      | 98  |
| 6.6.1 Preparing to run profile populating wizard                     | 99  |
| 6.6.2 Running the profile population wizard                          | 99  |
| 6.7 Installing Cognos Business Intelligence                          | 102 |
| 6.7.1 Required software  | 102 |
| 6.7.2 Installing WebSphere Application Server for Cognos BI          | 102 |
| 6.7.3 Preparing database client for IBM Cognos BI Transformer        | 102 |
| 6.7.4 Preparing databases for Cognos BI Server                       | 103 |
| 6.7.5 Installing Cognos BI Server                                    | 103 |

|   |            |
|---|------------|
| 6.7.6 Federating Cognos BI Server to the Deployment Manager . . . . .                               | 106        |
| 6.7.7 Validating Cognos BI Server . . . . .   | 107        |
| 6.8 Installing IBM Connections applications . . . . .   | 108        |
| 6.9 Installing IBM HTTP Server . . . . .  | 117        |
| 6.9.1 Installing IBM HTTP Server . . . . .  | 117        |
| 6.9.2 Federating IBM HTTP Server on WebSphere Application Server . . . . .                          | 123        |
| 6.10 Post installation environment configuration . . . . .  | 127        |
| 6.10.1 Configuring IBM HTTP Server . . . . .  | 127        |
| 6.10.2 Setting the single sign-on domain for future integration . . . . .                           | 138        |
| 6.10.3 Secure Sockets Layer encryption . . . . .  | 140        |
| 6.10.4 Setting the Java Virtual Machine heap size . . . . .   | 143        |
| 6.10.5 Creating additional administrator with the WebSphere Integrate<br>Console Solution . . . . . | 145        |
| 6.10.6 Configuring Cognos Business Intelligence . . . . .   | 146        |
| 6.11 Post installation IBM Connections configuration . . . . .                                      | 159        |
| 6.11.1 Additional languages . . . . .   | 159        |
| 6.11.2 Media components . . . . .   | 161        |
| 6.11.3 Configuring and creating search indexes . . . . .  | 162        |
| <b>Chapter 7. High availability and disaster recovery . . . . .</b>                                 | <b>165</b> |
| 7.1 Database management systems . . . . .   | 165        |
| 7.2 Multiple LDAP servers . . . . .   | 166        |
| 7.3 Edge Components Caching Proxy Server . . . . .  | 167        |
| 7.3.1 Installing Edge Components Caching Proxy Server . . . . .                                     | 167        |
| 7.3.2 Configuring Edge Components Caching Proxy Server . . . . .                                    | 171        |
| 7.3.3 Configuring SSL support on Edge Components Caching Proxy Server<br>177                        |            |
| 7.3.4 Configuring disk cache on Edge Components Caching Proxy server .<br>187                       |            |
| 7.4 Role of load balancers . . . . .  | 189        |
| 7.4.1 Installing Load Balancer . . . . .  | 189        |
| 7.4.2 Configuring Load Balancer . . . . .   | 193        |
| <b>Chapter 8. Working with IBM Connections mobile . . . . .</b>                                     | <b>197</b> |
| 8.1 Setting up an IBM Connections mobile client . . . . .   | 198        |
| 8.2 Troubleshooting . . . . .   | 199        |
| <b>Chapter 9. IBM Connections metrics . . . . .</b>   | <b>201</b> |
| 9.1 Security for IBM Connections Metrics application . . . . .                                      | 201        |
| 9.1.1 Admin role . . . . .  | 201        |
| 9.1.2 Metrics-report-run role . . . . .   | 202        |
| 9.1.3 Community-metrics-run role . . . . .  | 202        |
| 9.1.4 Reader-role . . . . .   | 202        |
| 9.2 Using IBM Connection Metrics . . . . .  | 203        |



|  |            |
|--|------------|
| 9.2.1 People .....   | 203        |
| 9.2.2 Content .....  | 203        |
| 9.2.3 Participation .....  | 204        |
| <b>Chapter 10. IBM Connections mail .....</b>                        | <b>205</b> |
| 10.1 Features of IBM Connections mail .....                          | 205        |
| 10.1.1 Email .....   | 206        |
| 10.1.2 Calendar .....  | 206        |
| 10.2 Configuring Mail for IBM Connections .....                      | 207        |
| 10.2.1 Installing IBM Connections Mail .....                         | 207        |
| 10.2.2 Configuring access to IBM Connections Mail .....              | 210        |
| 10.2.3 Setting up Discovery service for IBM Connections Mail .....   | 211        |
| 10.2.4 Enabling help for IBM Connections Mail .....                  | 215        |
| <b>Chapter 11. Customizing IBM Connections user experience .....</b> | <b>217</b> |
| 11.1 Branding .....  | 217        |
| 11.2 Multiple language support .....                                 | 219        |
| 11.3 Profile types .....   | 219        |
| 11.4 Notification .....  | 220        |
| 11.5 Renaming Applications .....                                     | 220        |
| 11.6 Hiding Applications .....                                       | 221        |
| <b>Chapter 12. Integrating with other software .....</b>             | <b>223</b> |
| 12.1 WebSphere Portal .....  | 223        |
| 12.1.1 IBM Connections application portlets .....                    | 223        |
| 12.1.2 Installing and Configuring IBM Connections portlets .....     | 224        |
| 12.1.3 Test integration with WebSphere Portal .....                  | 224        |
| 12.2 Sametime .....  | 224        |
| 12.2.1 System requirement .....                                      | 225        |
| 12.2.2 Pre-requisite .....   | 225        |
| 12.2.3 Procedure .....   | 225        |
| 12.3 Quickr .....  | 226        |
| 12.4 FileNet .....   | 226        |
| 12.4.1 Configuring FileNet .....                                     | 227        |
| 12.4.2 Configuring IBM Connections .....                             | 227        |
| 12.4.3 Testing the integration with FileNet .....                    | 228        |
| 12.5 Microsoft .....   | 229        |
| <b>Chapter 13. Upgrading from previous versions .....</b>            | <b>231</b> |
| 13.1 Before you begin .....  | 231        |
| 13.2 Migration process .....   | 232        |
| 13.2.1 Saving existing customization .....                           | 232        |
| 13.2.2 Backing up your IBM Connections environment .....             | 232        |
| 13.2.3 In-place upgrades .....                                       | 232        |



|   |   |     |
|---|---|-----|
| 13.2.4  | Side-by-side upgrades   | 233 |
| 13.2.5  | Restoring customization   | 234 |
| <b>Chapter 14. Administering IBM Connections</b>                                |   | 234 |
| 14.1  | Introducing the Integrated Solutions Console                        | 234 |
| 14.2  | Working with servers  | 237 |
| 14.2.1  | WebSphere A . . . . .pplication Servers                             | 238 |
| 14.2.2  | Web Servers   | 239 |
| 14.3  | Finding and using server logs                                       | 240 |
| 14.4  | Working with enterprise applications                                | 243 |
| 14.4.1  | Manage Modules.   | 244 |
| 14.4.2  | Security Role to user and group mapping.                            | 245 |
| 14.5  | Using wsadmin to modify and update application settings             | 246 |
| 14.6  | Where is the IBM Connections data                                   | 247 |
| 14.6.1  | Databases.  | 247 |
| 14.6.2  | Local and shared data.  | 248 |
| 14.6.3  | Configuration information   | 249 |
| 14.7  | Backing up and protecting data.                                     | 249 |
| 14.7.1  | Databases.  | 249 |
| 14.7.2  | Local and shared data.  | 250 |
| 14.7.3  | Server configuration  | 250 |
| <b>Chapter 15. Performance tuning</b>   |   | 252 |
| 15.1  | Database server performance.  | 252 |
| 15.2  | LDAP performance  | 253 |
| 15.3  | DNS performance   | 254 |
| <b>Chapter 16. Troubleshooting IBM Connections</b>                              |   | 256 |
| 16.1  | What can be found in WebSphere Application Server logs.             | 256 |
| 16.2  | How to troubleshoot IBM Connections Applications                    | 258 |
| 16.3  | Adding additional tracing to the logs                               | 262 |
| 16.4  | Gathering information for support                                   | 264 |
| 16.5  | Using the IBM SWG Support Portal to upload files to a PMR.          | 266 |
| <b>Appendix A. IBM Greenhouse</b>   |   | 268 |
| A.1   | The IBM Greenhouse Collaborations Solutions Catalog                 | 269 |
| A.2   | Searching the IBM Greenhouse Collaboration Solutions Catalog        | 269 |
| A.3   | Downloading from the IBM Greenhouse Collaboration Solutions Catalog | 271 |
| <b>Appendix B. Working with Tivoli Directory Integrator for custom Profiles</b> |   | 274 |
| B.1   | What is customizable?   | 275 |
| B.1.1   | IBM Tivoli Directory Integrator                                     | 275 |
| B.1.2   | TDI solutions package   | 275 |




|  |  |            |
|--|--|------------|
| B.1.3  | How user data is load to Profiles database .....                 | 276        |
| B.2  | Creating and using custom functions to manipulate data .....     | 277        |
| B.2.1  | Create a function that maps the city for timezone .....          | 277        |
| B.2.2  | Adding function to profile_functions.js .....                    | 278        |
| B.2.3  | Map function within the file map_dbrepos_from_source.properties  | 278        |
| B.2.4  | Synchronize the data .....                                       | 278        |
| B.3  | Creating custom mapping .....                                    | 278        |
| B.3.1  | How extension attributes are stored in Profiles (PEOPLEDDB) .... | 279        |
| B.3.2  | Adding a custom mapping .....                                    | 279        |
| B.4  | Setting up Tivoli Directory Integrator properties files .....    | 283        |
| B.4.1  | PROFILES_TDI.PROPERTIES file .....                               | 283        |
| B.4.2  | MAP_DBREPOS_FROM_SOURCE.PROPERTIES file .....                    | 285        |
| <b>Appendix C. Downloading the software from Passport Advantage and PartnerWorld .....</b> |  | <b>286</b> |



# Preface

## Meet the authors

This book is produced by a team of specialists from around the world.

|  |   |
|--|---|
|   | <p><b>Enio Rubens Basso</b> is an IT Specialist for IBM Software Group in Brazil. He has more of 16 years as IT Professional and joined IBM in 2009, starting as a Client Technical Professional at IBM Collaboration Solutions (ICS) brand. Enio is currently part of Accelerate Value Program (AVP) team in one of the Biggest Banks in Brazil, focusing in Collaboration Software and Portals. Enio holds a degree in Computer Science from Universidade Federal de Uberlandia. He is a Certified System Administrator for IBM Connections, IBM Sametime, Lotus Domino and WebSphere Portal Server and is also a certified in Linux LPI Level 1 and DB2 Associate.</p>   |
|  | <p><b>Gabriella Davis</b> – Technical Director, The Turtle Partnership -is a highly respected member of IBM's technical community and an IBM Champion for Collaboration Solutions 2011-2013. With her focus on design, development, deployment and administration of global infrastructures, she has established herself and her firm as experts within the messaging/collaborative space. Besides enjoying the challenge of learning new technologies and thriving in environments of constant change, Gabriella enjoys sharing her love of collaborative technologies and promoting women in technology (via NerdGirls). She can often be found presenting at user groups, conferences and industry events around the world on the topics of administration, infrastructure, collaboration and NerdGirl-related topics. In addition to her Technical Director, speaker and presenter roles, Gabriella is also a successful author – authoring IBM Lotus exams, acting as Technical Editor for The View and co-authoring the recently published IBM Lotus Sametime 8.5.2 Administration Guide and Connections101.Net website</p> |

|   |   |
|---|---|
|    | <p><b>Alan Hamilton</b> a passionate believer in the use of social collaboration tools to enhance the way people work. He demonstrates how these tools can enhance the communication, collaboration, and capture of information in organizations of all sizes. Alan has nearly 20 years experience of helping to solve customer problems through the implementation of collaborative systems and has turned many customer relationships into long term friendships. Alan encourages you to be social by tweeting him(<a href="https://twitter.com/alanghamilton">https://twitter.com/alanghamilton</a>), linking with him on LinkedIn (<a href="http://uk.linkedin.com/in/alanghamilton">http://uk.linkedin.com/in/alanghamilton</a>), or posting comments.</p> |
|   | <p><b>Abhishek Jain</b> is working with IBM India Software Labs since 2004 and has been in the industry for 10 years. He is currently working as an IT Specialist with IBM Collaboration Services and is skilled on various Lotus products. He is a Certified Lotus Professional, Certified Lotus Administrator, and a Certified Lotus Instructor on both Lotus Domino Administration and Development. Abhishek has been a part of earlier RedWikis Customizing Quickr 8.1 and Best Practices for Building Web Applications for Domino 8.5.1. He has also published developerWorks articles Integrating IBM Lotus Forms with IBM Lotus Domino and Auto-zipping Lotus Notes Attachments.</p>   |
|  | <p><b>Marcelo Makiuchi</b> is a Senior IT Specialist working for Global Technology Services at IBM Brazil. Marcelo majored in Systems Analysis at Universidade Mackenzie. He has 14 years experiences in middleware platforms including WebSphere Application Server, Web Server, Messaging, LDAP, Security, and Operating Systems.</p>   |

|   |   |
|---|---|
|  | <p><b>Chris Miller</b> is the Director of Messaging &amp; Collaboration at Connectria, a three time IBM Lotus Beacon Award winner. Connectria is the leader in hosted and remotely managed IBM environments. He is better known as IdoNotes across the social networks and the founder of Spiked Studio.</p>  |
|  | <p><b>Chander Ponnusamy</b> is working as a CTO at ReactiveBus Business Solutions Pvt Ltd, Bangalore, India. He has around 12 years of experience and worked on various IBM WebSphere, IBM Lotus and IBM Security Products. ReactiveBus is an IBM Business partner which provides services in IBM WebSphere Portal, IBM Connections, IBM FileNet P8, IBM Vivisimo Search and IBM Security products.</p> |
|   | <p><b>Evan Tepsic</b> is a Staff Software Engineer working for IBM Software Group on the IBM Connections and SmartCloud products since 2011. He holds a Bachelors degree in Computer Engineering Technology and over seven years of industry experience in Information Technology.</p>  |
|   | <p><b>Whei-Jen Chen</b> is a Project Leader at the International Technical Support Organization, San Jose Center. She has extensive experience in application development, database design and modeling, and DB2® system administration. Whei-Jen is an IBM Certified Solutions Expert in Data Management, and an IBM Certified IT Specialist</p>   |

## Special thanks to the following people for contributing to this effort

The authors express their deep gratitude for the technical consultation and direction from the following members:

- ▶ **David Byrd** is an Executive I/T Architect for IBM Collaboration Solutions.
- ▶ **Charles Price** is an Advisory Software Engineer for IBM Collaboration Solutions

We wish to acknowledge a special thank you to the following sponsors and key stakeholders from the Lotus Forms Development, Product Management, and Lotus IDC Teams:

- ▶ **Amanada Bauman** - ICS Wikis Program Manager
- ▶ **Dana Liburdi** - Information Architect for Lotus products
- ▶ **David Byrd** - Executive I/T Architect for IBM Collaboration Solutions.
- ▶ **Michael Wanderski** - Senior Software Engineer of IBM Connections
- ▶ **Scott Prager** - Distinguished Engineer - Social Software and Lotus Connections
- ▶ **Therese Barrett** - IBM Connections Release Manager

## Become an author

Join us for a two- to six-week residency program! Share your knowledge with peers in the industry and learn from others. Help create content about specific products or solutions, while getting hands-on experience with leading-edge technologies. You will have the opportunity to team with IBM technical professionals, Business Partners, and Clients. Your efforts will help increase product acceptance and customer satisfaction. As a bonus, you will develop a network of contacts in IBM development labs, and increase your productivity and marketability.

Find out more about the residency program, browse the residency index, and apply online at: <http://www.ibm.com/redbooks/residencies.html>

## Comments welcome

Your comments are important to us!

We want the content in this wiki and all our wikis to be as helpful as possible. Provide us your comments in one of the following ways:

- ▶ Use the commenting feature with in the wiki. Login and add comments, located at the bottom of each page.
- ▶ Provide feedback in the Web form located at:  
<http://www-12.lotus.com/1dd/doc/cct/nextgen.nsf/feedback?OpenForm>



## Stay connected to IBM Redbooks

- ▶ Find us on Facebook: <http://www.facebook.com/IBMRedbooks>
- ▶ Follow us on Twitter: <http://twitter.com/ibmredbooks>
- ▶ Look for us on LinkedIn:  
<http://www.linkedin.com/groups?home=&gid=2130806>
- ▶ Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:  
<https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm>
- ▶ Stay current on recent Redbooks publications with RSS Feeds:  
<http://www.redbooks.ibm.com/rss.html>

# IBM Connections overview

IBM Connections is an enterprise class social software platform. It features applications that any size business can leverage for collaboration. Whether internal or externally accessible, content can be created and shared with dynamic networks of colleagues in features such as Communities, Blogs, Activities, or Wikis.

IBM Connections provides the following features and benefits:

- ▶ Accessible from a variety of devices ranging from a PC web-browser to mobile devices.
- ▶ Fosters innovation through cultivation of critical information from co-workers, colleagues, partners, and customers.
- ▶ Numerous points of integration with other products which can realize an infinite number of possible ways to create and consume multi-media content.
- ▶ Highly scalable to meet the demands of tens to hundreds of thousands of Users.
- ▶ Customizable and brandable to deliver an experience unique to your company.

IBM Connections includes the following applications:

- ▶ **Activities**

Activities is a project-oriented application that allows you to create, assign, organize, and prioritize activities with to achieve goals. Such activities or any of the information which it is comprised of can then be referenced and re-used throughout the entire IBM Connections platform.

Activities are comprised of Entries, To-Do items, and Sections. Entries within an Activity are designed to store rich-content. Whether to be used as information resources or containing the final product or goal of the Activity itself, Entries are flexible structures. Activity Entries can also be tagged so that they can easily surface within other applications of IBM Connections.

To-Do items are structures within an Activity that organize tasks, assignments, and assignees. You can also assign To-do items priorities, due dates, members, bookmarks, files, and custom fields.

Sections are expandable and collapsible structures within an Activity that bring organization to an Activities Entries and To-do items. A section can contain multiple entries and to-do items. You can relocate a section within an Activity easily.

In addition to the elements of an Activity, IBM Connections also provides a way to create an Activity Template either from scratch or an existing Activity. This feature facilitates the reuse or creation of structure within an Activity.

- **Blogs**

Functioning as a journal, Blogs provides a tool with which users can create and deliver rich-content from a personal perspective that other users can consume, reference, and even participate in the growth of ideas an author writes about. IBM Connections offers essentially three types of Blogs, a Personal Blog, Community Blog, and Ideation Blog. The functionality of Personal and Community Blogs is virtually the same, except for who can read and provide feedback on the Blog Entries.

An Ideation Blog is a special type of Blog that can only exist within a Community. Its purpose is to generate ideas on a specific topic and also collect feedback from IBM Connections users. Users can create ideas for the given topic in a fashion similar to a thread-based forum. Other users can then vote on or comment on those ideas. When the ideas have enough support from the Community of users determined either on votes or feedback, that idea can then be graduated; an option to create an Activity from the Graduated Idea is also available to continue developing the idea. In addition, Owners of the Ideation Blog can manage several different aspects to ensure that the final goal of the best idea can be realized. Whether limiting the number of votes users can cast, to freezing the creation of ideas, to ultimately preventing the creation of new ideas while allowing voting and commenting on existing to continue, many aspects of an Ideation Blog can be controlled.

- **Bookmarks**

This application provides a way for users to store references to content in or outside the IBM Connections platform, organizing the references with social technologies such as Tags, Comments, and Popularity.

- **Communities**

In ways similar to a company intranet web-site, this application provides a way which users can organize teams to share information and interact with each other using Community Activities, Files, Forums, Bookmarks, Feeds, and so on .

- **Files**

Acting as a repository, this application provides users with a concentric location to store multimedia in multiple formats. That data can then be shared within Communities, across dynamic networks of users, or publically.

- **Forums**

Topics of discussion can be held within Forums to brainstorm and cultivate information that can then be transformed into content that comprises Activities, Blogs, or even Wikis. Similar to an Internet Message-board, this application provides the ability to archive messages rather than leave them volatile, for future reference, in a hierarchal or tree-like structure.

- **Homepage**

Similar to Communities, this application provides a launchpad-like website specific to a given user that allows them to easily consume notifications of information and content which they have followed or are a member of. Features like the Activity Stream provide users with an easy way to provide feedback on notifications of events generated from other applications within IBM Connections or establish a status that other users can be aware of.

- **Metrics**

Statistics that surface the usage of the IBM Connections platform and provide real-world numbers that users, administrators, and management alike can leverage.

- Profiles

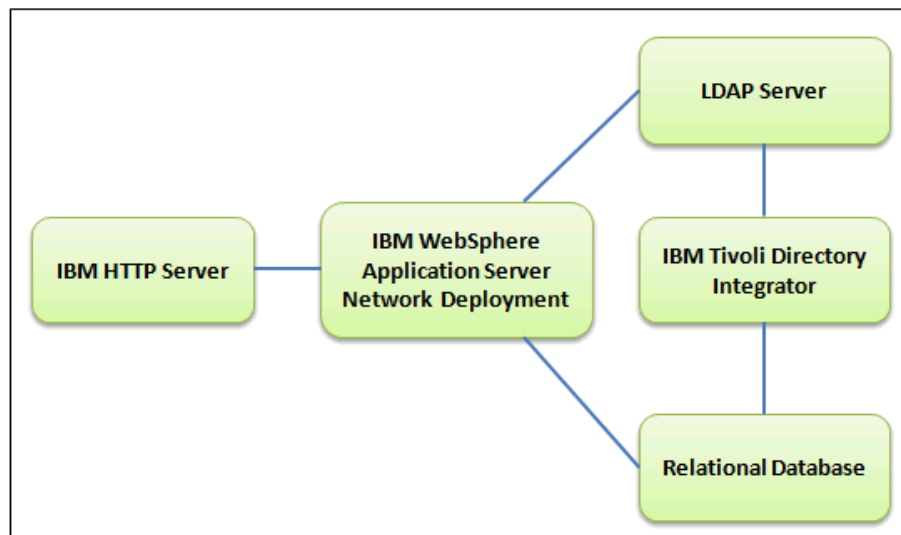
A directory of the users both within and external to your IBM Connections platform, this application delivers user-friendly tools that can be leveraged to easily locate and communicate with co-workers, colleagues, & customers.

- Wikis

This application provides tools that a user, team, or even Community members, can leverage to create and store information. Pages comprising a wiki can be organized in a hierarchy, with changes of those pages tracked, comments to improve the content with, and recommendations that other users can leverage to find the right information.

## 1.1 The software components and their roles

The following figure shows the major software components in an IBM Connections 4 deployment:



### IBM HTTP Server

The IBM HTTP Server is a front-end web server that provides the HTTP connection between the browser and the application server. A plug-in, generated by IBM WebSphere Application server, is deployed to the HTTP server to provide dynamic linking of the content.

Using an HTTP server instead of the one built into IBM WebSphere provides you options for off loading the processing, caching, and horizontal scaling.

### IBM WebSphere Application Server Network Deployment

IBM WebSphere Application Server Network Deployment (ND) provides the functionality for application deployment and management across multiple physical and logical nodes. Using WebSphere Application Server ND is the best approach to provide future scalability of the solution onto other servers. It also allows the deployment to be split across multiple physical servers, but still be managed by a single user interface.

## **Relational database environment**

The relational database systems (IBM DB2, Microsoft SQL Server, and Oracle) is the primary data store for the indexes and content displayed when the user works with IBM Connections. Note that it is not the only data store but is the primary one that the application talks to directly.

## **Tivoli Directory Integrator**

Tivoli Directory Integrator (TDI) provides the essential linkage between the Profiles in IBM Connections, the LDAP directory, and other sources of information. TDI pulls the details about the authorized users from the LDAP V3-compliant system, such as IBM Domino or Microsoft Active Directory, and creates and manages records in the Profiles database in the database server. When the user logs in, the system looks for a Profile for the user being authenticated. It then uses that information for business card lookups, reporting chain management, and so on.

TDI is usually scripted to run automatically using a Scheduled Service or a cron job so that changes in the corporate directory are reflected in the IBM Connections environment. You can set the frequency of running updates based on your business need.

You can use TDI to integrate many different data sources into the Profiles environment. For example, you might want to pull in human resource information from a SAP environment and pick up employee photos from a file system. You can use TDI to create a scheduled workflow for this.

## **LDAP**

LDAP is not included in the IBM Connections installation but is a requirement in an IBM Connections deployment. IBM Connections uses an LDAP directory to authenticate user requites. It also uses LDAP directories to populate and manage the Profiles.

The LDAP integration is performed within IBM WebSphere Application Server as a "federated repository" and the WebSphere Application Server administration console provides all the tools and features to set this up and test it.

If your organization has a large LDAP directory, you might want to restrict the people who can authenticate and gain access to the IBM Connections environment. This is normally done by creating a group in the LDAP environment (such as an Active Directory group, or an Access Control group in Domino) and then setting up Federated Repositories to query against that group when the user tries to log in. The Active Directory or Domino administrator can then control access to Connections simply by adding and removing people from the group.

## **SMTP**

An SMTP server is recommended in an IBM Connections environment. This can be any standard SMTP server. It is used to send and receive notifications about new documents and other events in IBM Connections.

There is an important post-configuration step in the install which requires the changing of the sender email address so that it matches your organizations standards. It is also possible to customize the format and content of the email notifications. For more detail, see IBM developerWork article Customizing IBM Lotus Connections 3.0 email digests and notification(<http://www.ibm.com/developerworks/lotus/documentation/lc3notifications/>)

## 1.2 What is new in IBM Connections 4

IBM Connections V4.0 provides advanced social software features and functions for business that helps enable you to access the right people and internal and external content in your professional networks and communities. Here we cover the new features introduced in IBM Connections 4.

### 1.2.1 Overall

- ▶ You can now share a status update or file from anywhere in IBM Connections. Log in and then click the Share link in the header.
- ▶ The activity stream displays an aggregated view of the latest updates from people or events that you are following and people in your network.
- ▶ Introduction of an enhanced Metrics application employing the analytic capabilities of the IBM Cognos Business Intelligence server, which is provided as part of the IBM Connections installation. Administrators and designated users can work with interactive displays of global metrics by clicking Server Metrics in the footer. Community owners can view non-interactive reports for their communities by clicking Metrics in the navigation pane.
- ▶ The rich text editor has been upgraded to CKEditor 3.6.3 in this release.
- ▶ Profiles has been updated to include the activity stream, which shows the profile owner's latest updates from across IBM Connections.
- ▶ When viewing your search results, you can filter the results from Profiles to exclude inactive profiles by selecting Exclude Inactive People from the Show menu on the Profiles Search Results page.
- ▶ The social analytic widgets now recommends private as well as public content, based on your existing relationships with public and private content in IBM Connections.
- ▶ The Trending widget displays a list of the hot topics that are trending in your organization. The widget displays when you filter your search results using the Status Updates option.
- ▶ Status updates and microblogging content are now included in the analysis of the relationships that are used to recommend content and people in the social analytics widgets.

#### Activities

- ▶ Activity members are now displayed in a Members view within the activity.
- ▶ Standard activity owners can go to the Members view to make an activity public.
- ▶ Titles and descriptions in activity entries are automatically saved to prevent data loss.
- ▶ In an activity entry, you can link to files and folders in the Files application.
- ▶ Activity owners can convert an entry into a To-do item.

#### Blogs

- ▶ Improved UI.

#### Bookmarks

- ▶ Improved UI.

- ▶ When you install the Add Bookmark browser button, you also have the option to install a Discuss This and Related Community browser buttons for posting web pages to an IBM Connections forum or linking together related communities.

## Communities

- ▶ Community owners can share information about upcoming events with the rest of the community.
- ▶ For deployments that make use of owner moderation of communities, owners can disable content approval and content flagging on individual communities.
- ▶ Ability to suggest communities for colleagues to join.
- ▶ You can now share status with members of your community.
- ▶ The Recent Updates view provides a centralized place to see what is new in a community.
- ▶ LDAP groups can now be added as members of a community.

## Files

You can now :

- Upload multiple files at the same time.
- Download all of the files in a view.
- Add files to a folder during upload.
- Select and perform actions on multiple files at one time.
- Delete a file version.
- Share folders with communities.
- Give community members access to edit files you own.
- Move files uploaded to a community to trash; from trash you and others can restore or delete the files.
- Stop sharing a file in one action, including removing the file from any shared folders and communities.
- Stop sharing files that were shared with you.
- ▶ A file's owners and editors can lock and unlock the file.
- ▶ The *Recommend* file option has been changed to a *Like* file option.
- ▶ For files that you are adding or have added to a folder, you can give access to those files to anyone who has access to the folder.
- ▶ The summary page and tabs have been redesigned to provide more information.
- ▶ The Communities Files view displays files that are you can access through communities.
- ▶ Files that are referenced in one or more status updates are noted as such.

## Forums

- ▶ When a user is notified by email that someone has added a topic to a forum, the user can click a Reply to this topic link in the email. This creates a response email the user can add content to and send. This create a new forum topic as a response to the topic they were notified about in the email. Attachments in the email are added to the response topic.
- ▶ You can add content from any web page or IBM Connections source to a forum topic by clicking a button in your browser tool bar. Click Bookmark or Discuss This, and then follow the steps for installing the Discuss This button. Then navigate to any web or IBM Connections page, click Discuss This, and select a forum to post the content to.

## Home Page

- ▶ Improved UI.
- ▶ The improved microblogging experience allows you to gather information in a meaningful way and act on it in context. You can now attach files to your status updates, and use hashtags to tag your updates and make them easier for other users to find. You can re-post status updates to share information with the people who are following you, or click Like to recommend an update. You can also preview images and download files to work on them locally.
- ▶ The Events widget helps you to keep track of upcoming community events that you are attending and that you are following. The widget is available from the activity stream views.

## Profiles

- ▶ The Board tab has been replaced with the Recent Updates tab on the user's profiles page.
- ▶ The Recent Posts tab on the Profiles page has been removed. Recent posts appear under the profile owner's Recent Updates tab.
- ▶ You can use the Recent Updates area on your profile page to post a status message.
- ▶ The business card has been redesigned for improved layout and access.
- ▶ On the Invite to My Network page, the Also Follow option is enabled by default.
- ▶ You can now accept a network invitation from the inviter's profile page.
- ▶ The Network Contact or Pending Invitation indicator label now displays next to the person's name on their profile page.
- ▶ You can now accept an invitation to join a person's network from that person's profile page.

## Wikis

- ▶ All views are now together in the same list instead of separate tabs.
- ▶ See wikis you are following by clicking I am Following.
- ▶ Pages can be removed from a wiki by moving them to the trash. From the trash, pages can be deleted or restored to the wiki.
- ▶ You can now download a version of a page from the page comparison view, as an HTML file.
- ▶ The wiki editor has two new features: the editor area expands downward as you add content. As your editing space expands, a toolbar displays even if scrolling is required.

## 1.2.2 Installation

- ▶ The installation wizard is now based on IBM Installation Manager 1.4.4.
- ▶ You can install and configure IBM Cognos Business Intelligence, obtained separately, by using the scripts, models, and specifications that are included with IBM Connections.
- ▶ Console Mode is available. Use this character based interface to install, modify, or uninstall the product when you do not have access to the graphical interface.
- ▶ Silent installation has been extended so that you can install both IBM Connections and IBM Installation Manager in silent mode.
- ▶ The initial configuration of administrators for Home page and Blogs is now handled automatically during installation. However, to configure widgets, you still need to assign a Home page administrator.



### 1.2.3 Administration

- ▶ Preview mode for running Profiles synchronization commands.
- ▶ New Metrics interface.
- ▶ New commands and properties files for different features.
- ▶ Improved and enhanced Search APIs.

### 1.2.4 Customization

- ▶ Changes in Customization paths.
- ▶ Support for customized Sprited images.
- ▶ Ability to over-ride a JavaScript file used by IBM Connections.
- ▶ Ability to extend the deployment using JSTL tags.
- ▶ Ability to customize notifications.

### 1.2.5 Security

- ▶ OAuth Support. Also, users can report a malicious application to an administrator who can remove it from the list of applications enabled for OAuth.
- ▶ Users can allow applications access to their Connections data without sharing credentials, and revoke that access at any time.

### 1.2.6 Mobile access

- ▶ New and enhanced APIs for improved performance and introduction of a new database and configuration file.

## 1.3 Architecture Overview

IBM Connections is a product from IBM that uses a set of J2EE-based social collaboration services tailored to support the needs of the enterprise. It consists of lightweight, independent features designed to allow for incremental implementation and adoption by the business, while at the same time providing a simple and extensible integration framework that allows the individual features to interact when they are deployed together in an organization.

### 1.3.1 Functional features

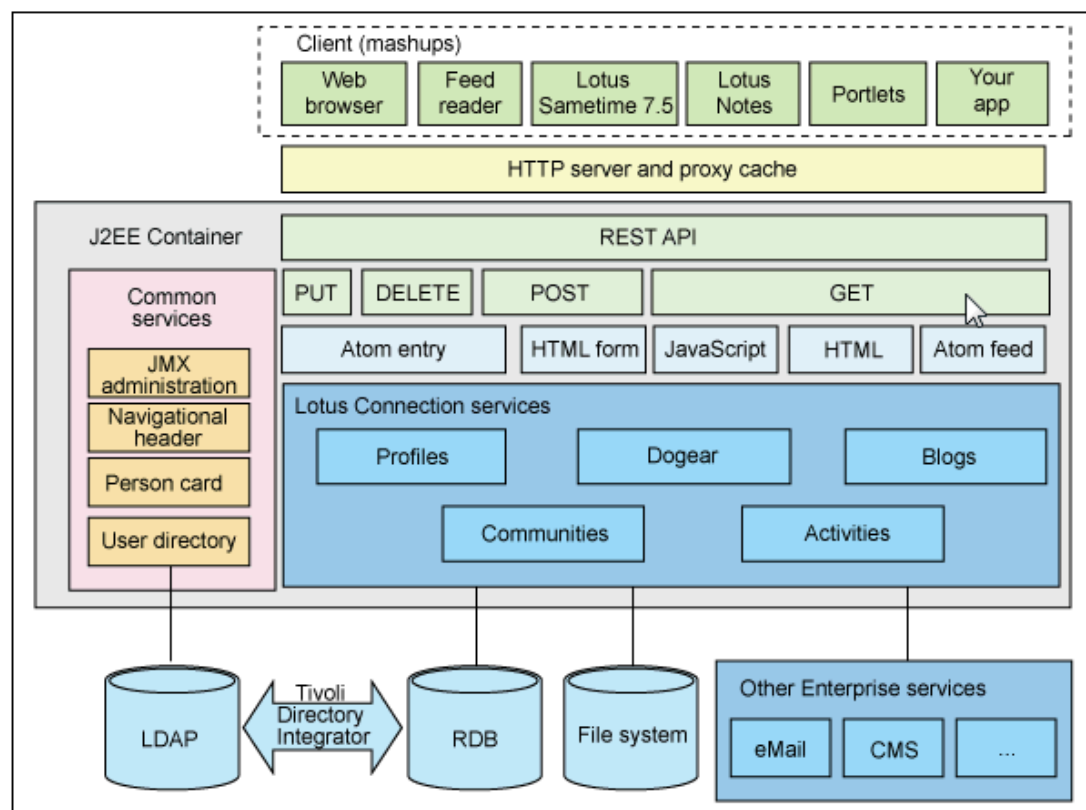
The functional features of IBM Connections include the following:

- ▶ *Profiles*: Provide quick access to information about people in the organization, including the ability to search across the organization using keywords that help identify expertise, current projects, and responsibilities.
- ▶ *Communities*: Provide a facility for creating communities of common interest, responsibility, or areas of expertise that people across the organization can join.
- ▶ *Blogs*: Provide a weblog service available to individuals or groups to share points of view and to get feedback from others.

- ▶ **Bookmarks:** Provides a facility to save, organize, and share bookmarks to valued online resources and a means to discover bookmarks that have been shared by others.
- ▶ **Activities:** Provide a means for individuals and groups to organize work, to plan and save process steps for reuse, and to collaborate easily on everyday deliverables.

The following figure illustrates the logical architecture of IBM Connections features. It consists of the following:

- ▶ Clients used to access the features
- ▶ HTTP transport and proxy caches
- ▶ J2EE container that hosts and controls access to all IBM Connections features and data
- ▶ Backend systems for use by those features for authentication, data storage, and integration with external messaging systems



IBM Connections provides features to various types of clients over standard Web ports through an API based on the REST protocol and the Atom standard. While several means of accessing the features are provided natively, such as browser access and application plug-ins for IBM Sametime or IBM Notes, the API is designed to allow customers to create, update, query, and manage IBM Connections information from their own custom applications.

Because the IBM Connections REST API is similar in structure to HTTP (in fact, HTTP is a REST-based protocol), and because it uses the same transport layer as standard Web servers, calls to the features are compatible with standard Web servers and proxy servers.

The API allows information to be entered and managed using POST, PUT, and DELETE methods with the service data encapsulated in an HTML form or an XML Atom document. Information can be retrieved using the GET method and rendered either as an HTML or an XML Atom document, depending upon the needs of the requesting client.

In addition to the functional features that are accessed by clients, IBM Connections provides four additional common utility modules:

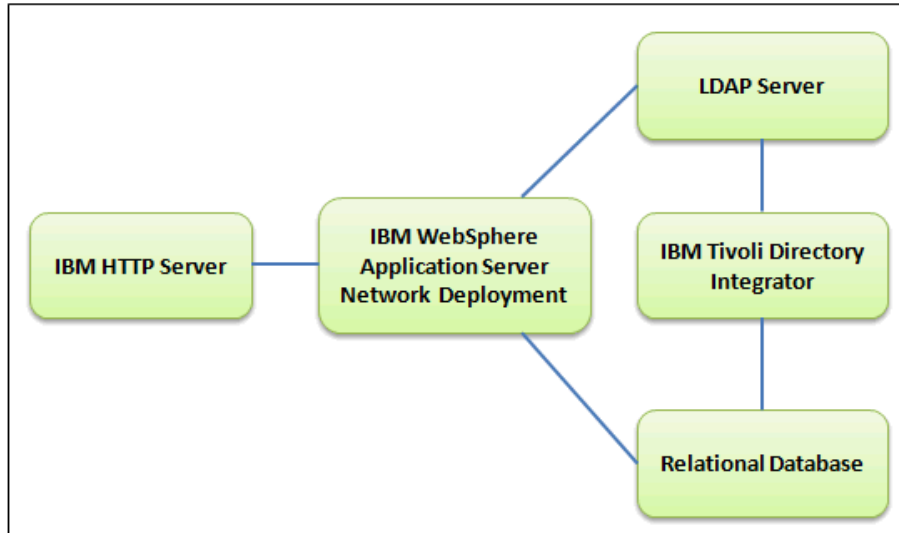
- ▶ *JMX administration*: Used to configure and manage the IBM Connections environment. Most administration functions are managed using the WebSphere wsadmin command, but others are exposed through a Web interface.
- ▶ *Navigation header*: Allows all installed features to be aware of one another and to provide consistent Web navigation to users. Extensible to include links to other external services.
- ▶ *Business card*: Displays consistent business card information when a person's basic Profile information is requested from within each of the features. Requires the Profiles feature.
- ▶ *User directory*: Interfaces to the directory used by IBM Connections for authentication, authorization, and query features.

IBM Connections also relies on several key backend services:

- ▶ *LDAP*: Provides authentication and authorization services to IBM Connections and serves as the primary data source for person information used by the Profiles feature.
- ▶ *Relational database*: Stores databases and tables needed by the IBM Connections features. Each functional feature has its own data store.
- ▶ *Data integration* (IBM Tivoli Directory Integrator): Extracts person information from enterprise data sources, such as the LDAP directory, and pushes that information to the Profiles feature's database tables. Can also be configured to push updates made to Profiles entries back to the original data source. Used only with the Profiles feature.
- ▶ *File system*: Stores service indexes, as well as service-specific data, such as file attachments uploaded to blogs or activities.
- ▶ *Outbound SMTP*: IBMConnections leverages an organization's existing messaging infrastructure to transmit notification messages. This can be any mail system that can accept and forward an SMTP message packet.

### 1.3.2 Operational architecture

The following figure illustrates the primary deployment components that make up IBM Connections. These are the minimum required components. In some instances, components might be co-located on the same physical server. For example, while it is normally deployment best practice to install an HTTP server on a separate physical unit from the IBM WebSphere Application Server, it might be appropriate to install them on the same physical unit in some low-usage scenarios, such as a development or test server, or for a small proof-of-concept or pilot deployment.



IBM Connections requires WebSphere Application Server running on a supported operating system. A single functional feature can be installed, or multiple features can be deployed into separate application servers on the same physical instance. In addition, you can deploy features across several physical servers that are part of a network deployment cluster if a company requires a highly available environment or if IBM Connections must scale to support deployment to a large user population.

IBM Connections databases can be hosted on either IBM DB2, Microsoft SQL Server or Oracle. On DB2, each service's data is stored in a separate database. On Oracle, Profiles and Activities data are stored in separate database instances, while Blogs, Communities, and Dogear data are stored in separate tables that share a single database instance. With most deployments, the Tivoli Directory Integrator application that is used to populate the Profiles database is co-located with the database server.

As mentioned previously, certain data is stored outside of databases in the file system that is accessible by the IBM Connections features. These file system components, such as indexes and file attachments, must be stored on drives attached to WebSphere Application Server. If you are deploying in a clustered WebSphere Application Server environment, each cluster instance must have access to a file share on common file servers or enterprise network storage devices.



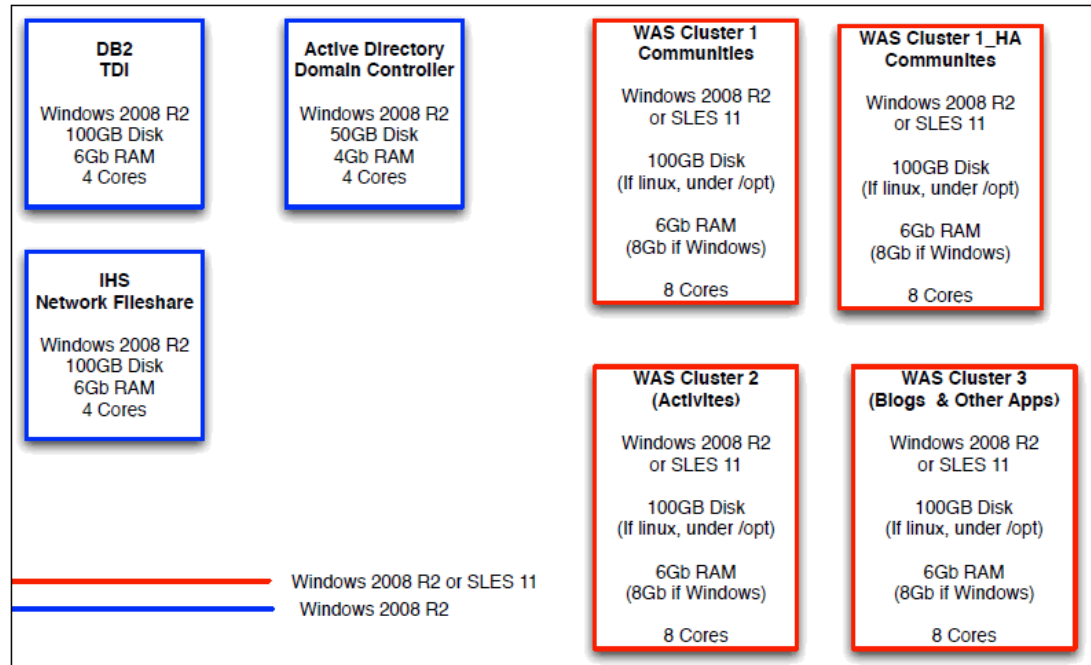
# General deployment considerations and requirements

In this section, we describe the considers and requirements for a successful IBM Connections deployment. We cover the following topics:

- ▶ 2.1, “Architecture considerations” on page 13
- ▶ 2.2, “Hardware requirements” on page 15
- ▶ 2.3, “Software requirements” on page 16
- ▶ 2.4, “Performance considerations” on page 18
- ▶ 2.5, “Deployment options” on page 21

## 2.1 Architecture considerations

The IBM Connections product manual provides a detailed description of the deployment options([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Deployment\\_options\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Deployment_options_ic40&content=pdcontent))and considerations in planning an IBM Connections deployment. In this section, we describe the planning considerations for our lab environment (see the figure below) which is a slightly modified small deployment scenario.



While this is the easiest of the deployment scenarios to build, the basic architecture permits scaling horizontally or vertically into the larger style deployments should it be necessary. Using IBM WebSphere Application Server Network Deployment allows future scaling to be performed and hence can act as a good starting point for your own deployment.

A network deployment can consist of a single server that hosts all IBM Connections applications or two or more sets of clustered servers that share the workload. You must configure an additional system with WebSphere® Application Server Network Deployment Manager. IBM Cognos® Business Intelligence is an optional component in the deployment. If used, Cognos must be federated to the same Deployment Manager as the IBM Connections servers. However, Cognos servers cannot be configured within an IBM Connections cluster. A network deployment provides the administrator with a central management facility and it ensures that users have constant access to data. It balances the workload between servers, improves server performance, and facilitates the maintenance of performance when the number of users increases. The added reliability also requires a larger number of systems and experienced administrative personnel who can manage them.

It is important to distinguish between the physical needs of the IBM Connections server and the ability of WebSphere to allow you to scale the IBM Connections applications themselves horizontally or vertically. To be clear by "physical needs", we mean:

- ▶ The presence of a database management system such as DB2 or Oracle;
- ▶ The presence of an HTTP server, in our case IBM HTTP Server
- ▶ The ability of the system to connect to one or more LDAP servers to authenticate users and create profiles.
- ▶ The number and location of WebSphere Application Servers.

With these physical needs addressed, the individual IBM Connections applications can be scaled across multiple WebSphere Application Servers (WAS). A single WAS can also run more than one application (and frequently does - in a standard "Small Deployment" one where the WebSphere Application Server server runs all the applications). By "application" we mean Activities, Blogs, Communities, Wikis, Profiles, and so on. Each of these in

WebSphere Application Server terms are applications in their own right and by chance or design, they happen to share the same databases and look and feel.

For example, suppose you have an existing Enterprise Content Management solution which manages your organization's files. The need for the Files application in IBM Connections would be restricted to the mandatory requirements of the wikis, activities, and so forth. The need to provide a highly-scalable Files solution has already been solved through the ECM system. Thus, you might choose to run the Files application on a single WebSphere Application Server node. Similarly, however, it might be that the Profiles application is one of the main aspects of your deployment and as such needs, to be highly-responsive. You would choose in that situation to cluster the Profiles application across two or more WAS nodes.

In our deployment, we have chosen to use a modified small deployment where the applications are split between two WAS servers. We are not clustering applications (that is, running the same application in a synchronized manner across multiple nodes), but simply dividing the total number of applications we are deploying across more than one node.

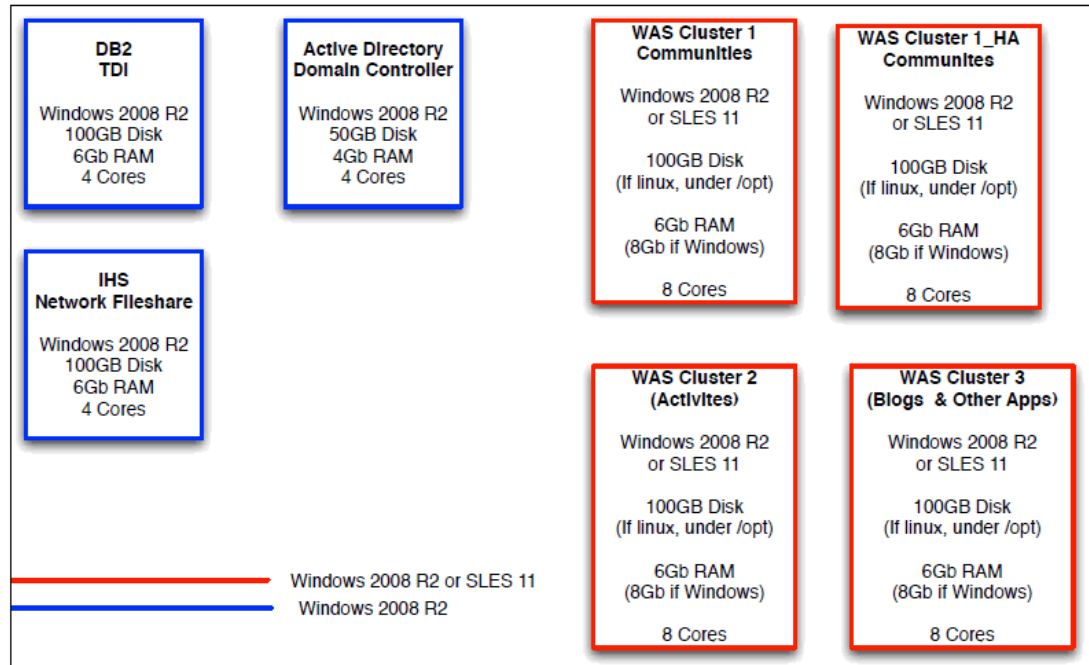
## 2.2 Hardware requirements

The hardware requirements for IBM Connections are very much dependent on the type of implementation you are going with. It is also affected by the operating system that you choose. Typically, Windows server deployments requires more available memory than Linux due to the overheads of the operating system. Both operating systems require broadly the same amount of disk space. Compute cores and processors have a strong influence on the performance of IBM Connections, as does the configuration and tuning of the Java Virtual Machines which IBM Connections runs in through WebSphere.

Choosing a 64-bit operating system is a good first step because you can allocate more memory to the JVMs. Using more processors can improve performance when you have maximized the use of the JVMs. Be aware that you have to check your licensing situation with IBM when it comes to adding cores and processors as you might be licensed on a Processor Value Unit basis.

As a rule of thumb, for a small deployment serving up to 1000 users, the hardware configuration we chose was as follows:





## 2.3 Software requirements

IBM Connections 4 can be installed on a wide range of software and hardware including Microsoft Windows and a number of Linux distributions. The table below summarizes the supported combinations.

Before start your installation, you have to check if your environment is fully compatible with the IBM Connections software requirements, listed below:

| Operating System                            | Version             | Hardware     |
|---|---------------------|--------------|
| AIX   | 6.1 and 7.1         | POWER System |
| Red Hat Enterprise Linux (RHEL)             | Advanced Platform 5 | System Z     |
| Red Hat Enterprise Linux (RHEL)             | Desktop Edition 5   | x86-32       |
| Red Hat Enterprise Linux (RHEL)             | Server 5            | X86-64       |
| Red Hat Enterprise Linux (RHEL) Client      | 6                   | X86-32       |
| Red Hat Enterprise Linux (RHEL) Server      | 6                   | System Z     |
| Red Hat Enterprise Linux (RHEL) Server      | 6                   | x86-64       |
| Red Hat Enterprise Linux (RHEL) Workstation | 6                   | X86-32       |
| SUSE Linux Enterprise Desktop (SLED)        | 11.0                | X86-32       |
| SUSE Linux Enterprise Server (SLES)         | 11                  | System Z     |
| SUSE Linux Enterprise Server (SLES)         | 11                  | X86-64       |

| Operating System    | Version               | Hardware          |
|---------------------|-----------------------|-------------------|
| Windows 7           | Professional          | X86-32 and x86-64 |
| Windows Server 2008 | Datacenter Edition    | X86-64            |
| Windows Server 2008 | Datacenter Edition R2 | X86-64            |
| Windows Server 2008 | Enterprise Edition    | X86-64            |
| Windows Server 2008 | Enterprise Edition R2 | X86-64            |
| Windows Server 2008 | Standard Edition      | X86-64            |
| Windows Server 2008 | Standard Edition R2   | X86-64            |
| Windows Vista       | Enterprise            | X86-32            |
| Windows XP          | Professional          | X86-32            |

| Name       | Version         |
|------------|-----------------|
| Android    | 2.3 3.0 and 4.0 |
| Blackberry | 6.0 and 7.0     |
| IOS        | 5               |

| Product  | Version |
|--|---------|
| WebSphere Application Server Network Deployment<br>(Mandatory) | 7.0     |

| Product                               | Version         |
|---------------------------------------|-----------------|
| IBM Sametime                          | 8.0.2           |
| Lotus Quickr for Domino               | 8.5.1           |
| Lotus Quickr for WebSphere Portal     | 8.5             |
| Lotus Sametime Advanced               | 8.5             |
| Lotus Sametime Standard               | 8.5.1 and 8.5.2 |
| Microsoft Sharepoint Server           | 2007 and 2010   |
| Microsoft Windows SharePoint Services | 3.0             |

| Product                                 | Version           |
|---|-------------------|
| DB2 Enterprise Server Edition           | 9.7               |
| Microsoft SQL Server Enterprise Edition | 2005 SP3 and 2008 |
| Oracle Database 10g Enterprise Edition  | Release 2         |

| Product                                | Version   |
|--|-----------|
| Oracle Database 11g Enterprise Edition | Release 2 |

| Product           | Version               |
|-------------------|-----------------------|
| Lotus Notes       | 8.5.1 8.5.2 and 8.5.3 |
| Microsoft Outlook | 2007 and 2010         |

| Product                     | Version |
|-----------------------------|---------|
| Tivoli Directory Integrator | 7.1     |

| Product                          | Version       |
|----------------------------------|---------------|
| Lotus Domino                     | 8.0.2 and 8.5 |
| Tivoli Directory Server          | 6.2           |
| Microsoft Active Directory       | 2003 and 2008 |
| Novell eDirectory                | 8.8           |
| Sun Java System Directory Server | 6.3 and 7.0   |

| Product                 | Version       |
|-------------------------|---------------|
| Websphere Portal Server | 6.1.5 and 7.0 |

| Product          | Version       |
|------------------|---------------|
| Microsoft Office | 2007 and 2010 |

| Product                      | Version |
|------------------------------|---------|
| Cognos Business Intelligence | 10.1.1  |

| Product                             | Version |
|-------------------------------------|---------|
| Tivoli Acess Manager for e-business | 6.1     |
| CA SiteMinder                       | 6.0     |

## 2.4 Performance considerations

The performance of IBM Connections is largely dependent on the following variables:

- The amount of memory allocated to the Java virtual machines used by WebSphere Application Server

- ▶ The number of processors available for processing
- ▶ The speed of connectivity between the application server and the database
- ▶ The speed of the underlying disk infrastructure

With this number of variables, there is no hard-and-fast rule to maximizing the performance of an IBM Connections environment. At the outset of your project, however, if you consider your system to be likely to grow in scale after successful deployment, you should consider ensuring you have the knowledge and skills to horizontally and vertically scale IBM WebSphere Application Server through its Network Deployment tools so that you can balance the load.

The Connections team prepared an excellent document for version 3 which describes the many facets of performance tuning - Click

[http://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM\\_Lotus\\_Connections\\_3.0\\_Performance\\_Tuning\\_Guide](http://www-10.lotus.com/ldd/lcwiki.nsf/dx/IBM_Lotus_Connections_3.0_Performance_Tuning_Guide)

In the system we built for this guide, we have split the burden of providing the communities functionality across two servers (WAS Cluster 1 and WAS Cluster 2). Activities resides on its own server and all other applications reside on the fourth server. This design was arrived at because we expect that Communities will be the most heavily-used application and splitting them provided greater resilience and greater throughput. Bookmarks, Wikis, and so on are used less and can be safely combined onto a single server.

Tuning IBM Connections server improves performance of the applications and it requires tuning various components till the desired results are achieved. The following topics give some generic performance considerations for IBM Connections server :

- ▶ *Avoiding co-location*

The system hosting the IBM Connections server should not have database server installed on the same server . Separating the database server to a dedicated server improves performance for IBM Connections server and can be tuned independently. There are multiple read and write operations performed on a database server and hence not to place database server on the server that host the IBM Connections.

- ▶ *RDBMS server performance*

IBM Connections server applications make extensive calls to database server to provide its functionality. In larger deployment scenario, consider creating a dedicated database server instance per database. The database server must have 8GB of memory in small deployment scenario and 16GB of memory in larger deployment scenario. The database storage disk should be a dedicated disk subsystem and able to handle heavy workload for read and write operations.

- ▶ *LDAP performance and directory size*

IBM Connections server caches the user information locally in the respective database. The profile application extensively uses LDAP server to retrieve user information through Tivoli Directory Integrator (TDI) and stored locally in the profiles database. By indexing the LDAP server search filter attribute and login attribute helps faster lookup and improves the performance of IBM Connections server. Any search taking more than 100 milliseconds need to be corrected.

- ▶ *64-bit architecture for WebSphere, TDI, and RDBMS*

IBM Connections server 4.0 supports only 64-bit architecture. 64- bit architecture gives better performance through more effectively using the process power of the system. . Setting large heap size is possible in the 64- bit systems, which provide more inflight transactions and higher throughput. A general recommendation is to use 64- bit system for WebSphere, TDI and RDBMS for better performance.

► *Placing IHS on a separate server*

IBM HTTP Server is the entry point for all IBM Connections applications and must be placed on the separate server. Configuring Files and Wikis applications data directories accessible by web server helps performance improvement and the request is served from the web server itself instead of WebSphere Application Server. This off loads the traffic going to WebSphere Application Server and improves the overall performance of the applications.

► *Identifying heavy-use applications*

In a large deployment scenario, IBM Connections applications are installed into dedicated application server cluster. Depending upon the usage of application, additional node can be added into the application cluster for that application to provide better performance results.

► *Monitoring disk space usage*

In a large deployment scenario, IBM Connections applications are installed into multiple nodes with a dedicated application cluster. Additional nodes can be added to the application cluster to provide scalability and high throughput. Monitor the disk space usage of IBM Connections server nodes, shared content store, temporary directory, and log directory locations to ensure that there is sufficient disk space or current operations and plan for future growth.

► *Dedicated resources*

IBM Connections 4.0 provides metrics application to utilize the analytic capabilities of Cognos Business Intelligence (BI) server. IBM Cognos BI server and database server should be installed on a dedicated server. IBM Cognos server must be federated into IBM Connections server deployment manager to enable Single Sign on (SSO) features. We recommend to use the same IBM HTTP Server as IBM Connections application.

► *Networking routing for IBM Connections requests*

IBM Connections applications serve mainly static content, Java script, and images. In a large deployment scenario, we recommend to cache the content of the applications. . IBM WebSphere Edge component proxy caches the content and improves the client-side performance. By using reverse caching proxy of IBM WebSphere Edge component, the workload is reduced on the server and improves the server-side performance.

► *JVM*

The heap size of the JVM should be less than the physical memory of the system and larger heap size is required for cluster setup when memory-to-memory replication is enabled. We recommend to set minimum and maximum heap size as same to avoid heap fragmentation. For small and medium deployment, the recommended heap size would be 2506 MB. For the large deployment, the recommended heap size is shown is .

| Application Name | Max Heap Value |
|------------------|----------------|
| Blogs            | 1024           |
| Bookmarks        | 1024           |
| Communities      | 1280           |
| Files            | 768            |
| Forums           | 1024           |
| Homepage         | 768            |
| Metrics          | 1024           |

| Application Name | Max Heap Value |
|------------------|----------------|
| Mobile           | 102            |
| Moderation       | 512            |
| News             | 1280           |
| Profiles         | 1280           |
| Search           | 1280           |
| Wikis            | 1024           |

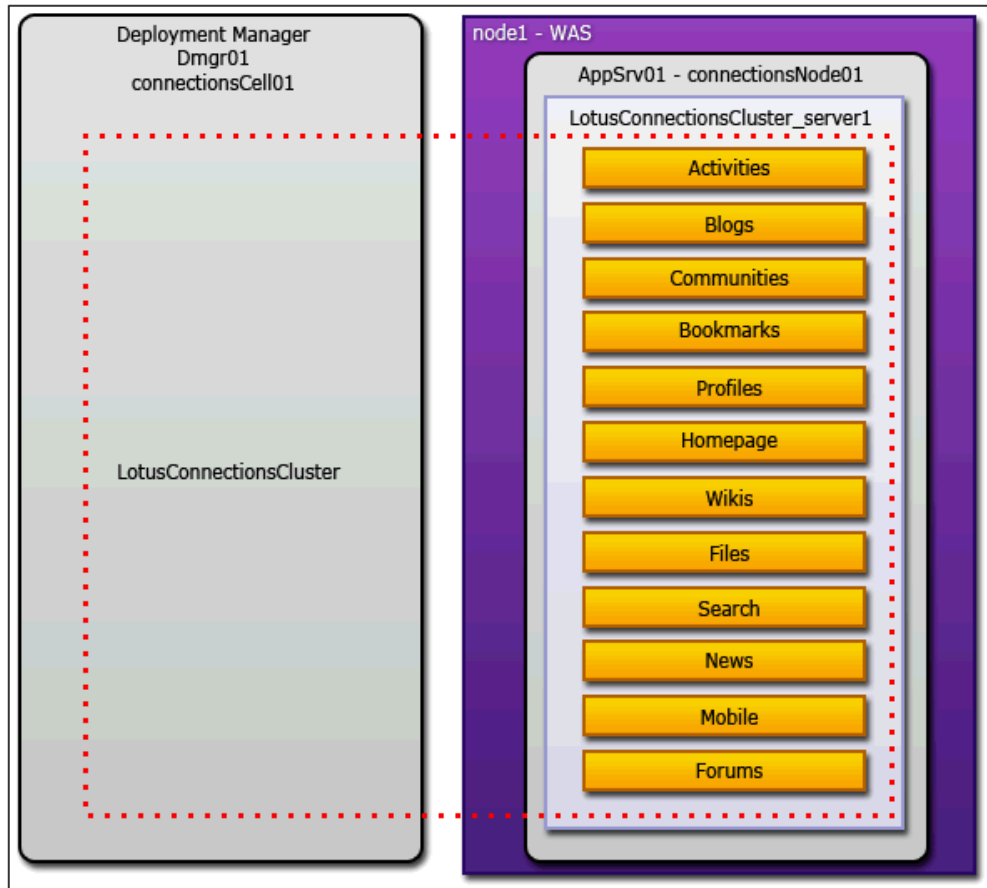
## 2.5 Deployment options

To make planning easier IBM has categorized three different sizes of deployment of IBM Connections. Additional guidance can be found at [http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Determining\\_the\\_best\\_deployment\\_topology\\_for\\_IBM\\_Connections\\_4.0](http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Determining_the_best_deployment_topology_for_IBM_Connections_4.0). The scenarios are as follows:

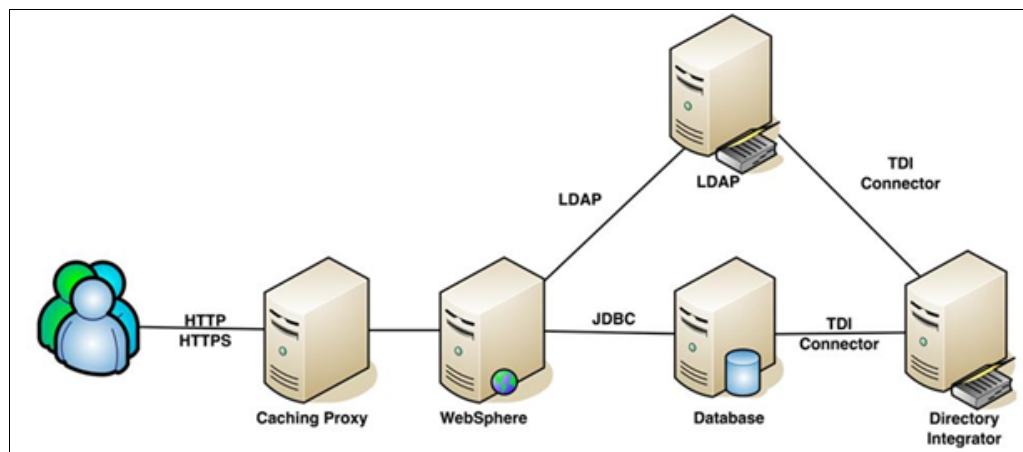
- ▶ Small deployment
- ▶ Medium deployment
- ▶ Large deployment

### 2.5.1 Small deployment

This option installs all applications in a single cluster on a single node and so is the simplest deployment. However, it has limited flexibility and does not allow you to scale up individual applications. For each node within the cluster, all applications run within a single JVM. The following figure shows a one node small deployment architecture.



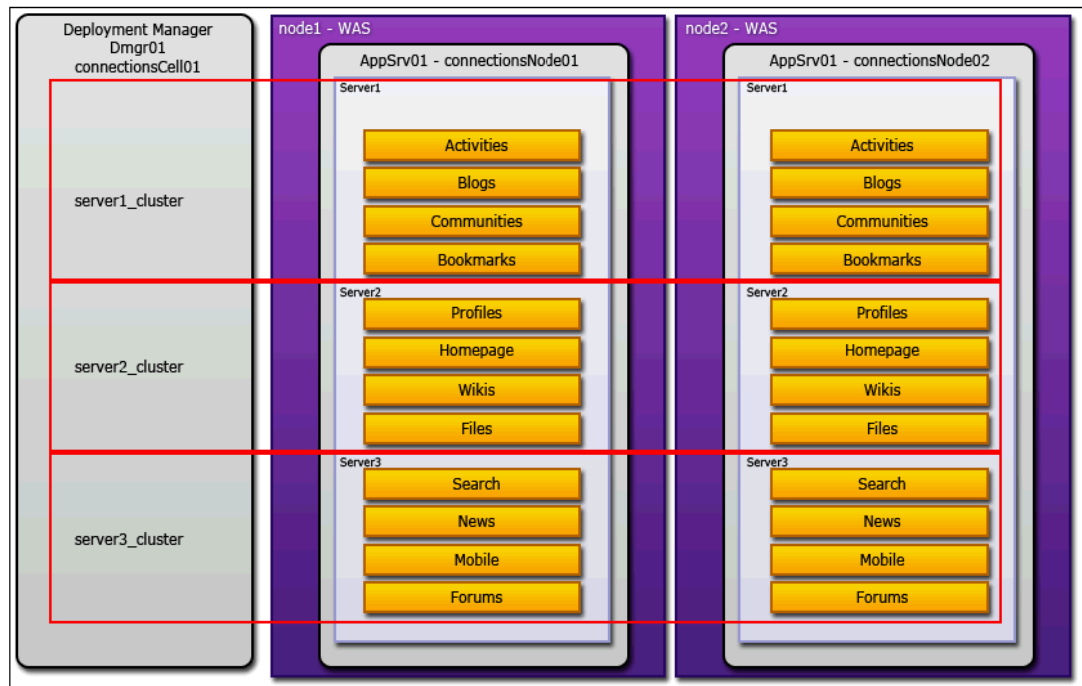
The following figure shows one of the simplest deployments of IBM Connections, where each component is running on its own machine. This option does not provide any workload or disaster recovery, but it does provide simplicity to small organizations looking to run IBM Connections.



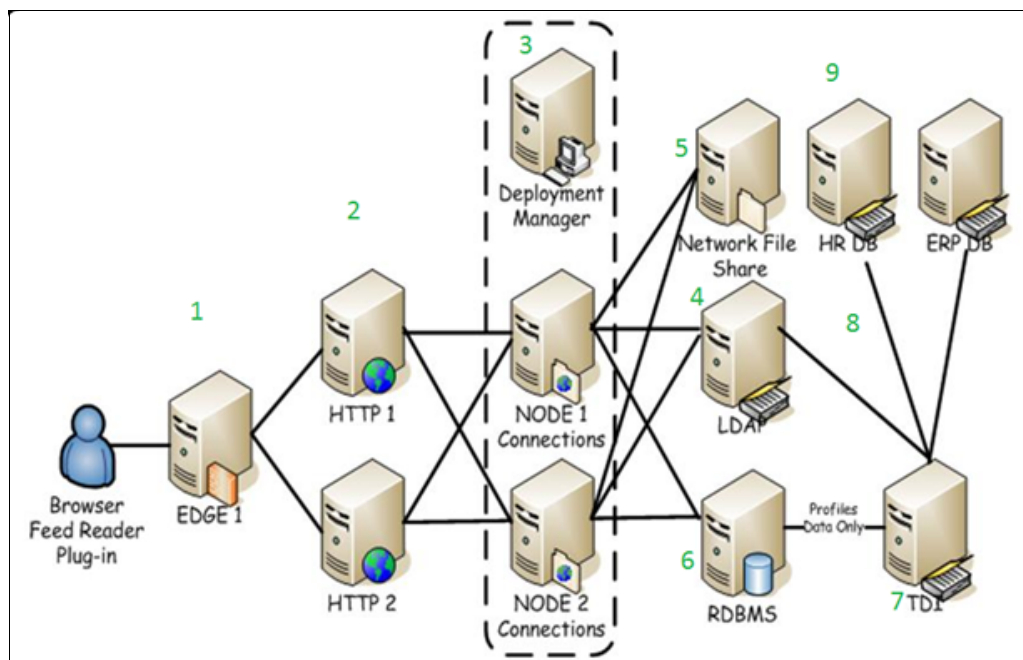
## 2.5.2 Medium deployment

This option installs a subset of applications in separate clusters. IBM Connections 4 provides three predefined cluster names shared among all applications. This option is used to distribute applications according to usage expectations and allows you to maximize the use of

available hardware and system resources to suit specific needs. The following figure illustrates a medium IBM Connections deployment architecture.



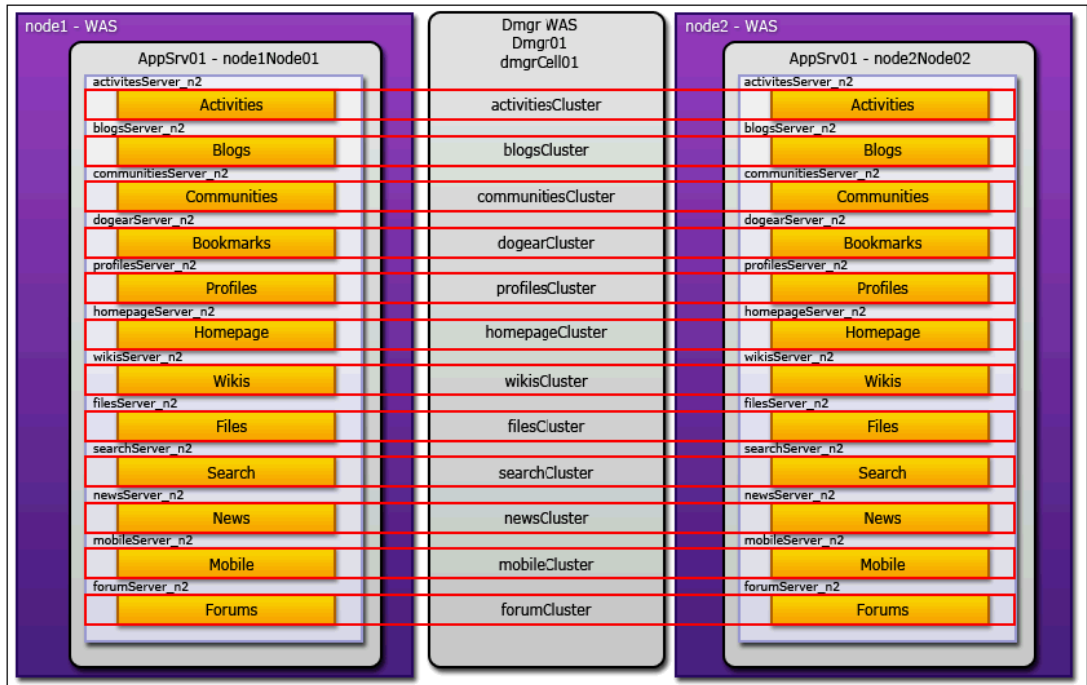
The following figure shows a typical medium deployment of IBM Connections. A two-node cluster is used for IBM Connections, with two HTTP servers in front handling all requests coming from the edge server. This approach also shows you how you can use IBM Tivoli® Directory Integrator (TDI) to merge data coming from multiple sources into the Lightweight Directory Access Protocol (LDAP) server and IBM DB2® database.



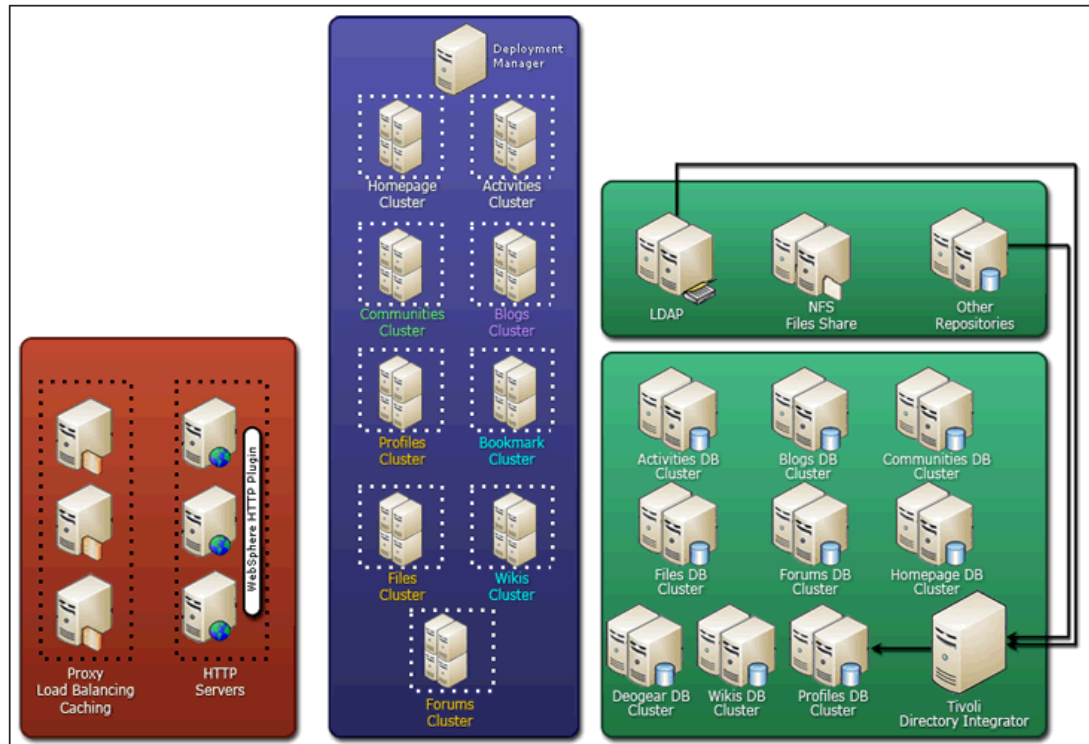


## 2.5.3 Large deployment

This option installs each application in its own cluster, and IBM Connections 4 provides a predefined cluster name for each application. This option provides the best performance in terms of scalability and availability options, but it also requires more system resources. The figure below illustrates a large architecture, with multiple nodes and clusters.



With a basic understanding of all the deployment options, you reach a decision point regarding all the additional servers and components that IBM Connections uses. The figure below shows a complex environment with multiple nodes, HTTP and proxy servers, and database clusters for each feature of IBM Connections (blogs, home pages, and more). Large organizations with strict service level agreements should consider deployments that include high availability and disaster recovery as well as sufficient resources to support the workload.



For large IBM Connections deployment, high availability considerations include:

- Clustering for Connections applications

Deploying IBM Connections applications in dedicated cluster provides better performance, scalability, and availability. This deployment requires more system resources and additional maintenance.

- LDAP

Lightweight Directory Access Protocol (LDAP) server is used to store user repository information for WebSphere application server. When the LDAP server fails, WebSphere cannot access directory data, such as security data, and hence fails to service client requests. Therefore, consider building a highly available LDAP as a part of the highly available WebSphere system. The LDAP high availability configuration and setup varies from vendor to vendor. As a general rule, place WebSphere Edge Component load balancer in front of LDAP server and access the LDAP server through cluster IP address. If any one of the LDAP server fails, request will route to another LDAP servers.

- Load balancing

A load balancer distributes load across a number of systems. If you have more than one HTTP server, you must use a load balancer. For moderately sized deployments, use a software-based load balancer, such as WebSphere Edge Component. For larger deployments, which support a large number of concurrent users, use a hardware-based load balancer such as F5 or Cisco ACE.

- Clustering for WebSphere - horizontal and vertical clusters

Horizontal clustering, sometimes referred to as scaling out, is adding physical machines to increase the performance or capacity of a cluster pool. Vertical clustering, sometimes referred to as scaling up, is adding WebSphere Application Server instances to the same machine. WebSphere clustering is a logical group of application servers that hosts the IBM Connections server applications either vertically or horizontally and provides the load

balancing and high availability capabilities. Vertical clustering is not supported on IBM Connections 4.

- ▶ WebSphere Edge caching proxy

WebSphere Edge Caching Proxy Server is a proxy Server which can be used to cache content from backend so that the servers are relieved from high load. This in turn helps faster response from the server and improves user experience. You can configure WebSphere Edge Server for high availability by using additional WebSphere Edge Server as a backup server. When the primary WebSphere Edge Server fails, the user requests are sent to the backup server.

- ▶ Relational database management systems

IBM Connections applications supports IBM DB2, Oracle, and SQL server for storing application related data. Each database systems provides high availability features and can be used for IBM Connections data.

- IBM DB2

DB2 supports a number of software and hardware offerings from IBM and other vendors that you can use with DB2 to strengthen high availability in your environment.

IBM offers the following high availability configurations. The options for implementing high availability and disaster recovery solutions with DB2 include:

- High availability disaster recovery

DB2 high availability disaster recovery (HADR) feature provides a high availability solution for both partial and complete site failures. HADR protects against data loss by replicating data changes from a source database, called the primary database, to one or more target databases, called the standby databases.

- Tivoli System Automation

Tivoli System Automation (TSA) clustering software is installed on TSA server, primary, and standby DB2 servers. Both the DB2 servers are monitored through heartbeat node installed on TSA server. In the event of primary database failure, TSA automatically fail back to standby node.

- Clustering with IBM PowerHA SystemMirror for AIX (formerly known as High Availability Cluster Multi-Processing for AIX or IBM HACMP™) or Microsoft Cluster Server for Windows.

- SQL Server

SQL Server provides the following options for creating high availability solutions:

- AlwaysOn Failover Cluster Instances

AlwaysOn Failover Cluster Instances leverages Windows Server Failover Clustering (WSFC) functionality to provide local high availability through redundancy at the server-instance level—a failover cluster instance (FCI).

- AlwaysOn Availability Groups :AlwaysOn Availability Groups is an enterprise-level high-availability and disaster recovery solution introduced in SQL Server 2012 to enable you to maximize availability for one or more user databases. AlwaysOn Availability Groups requires that the SQL Server instances reside on Windows Server Failover Clustering (WSFC) nodes

- Database mirroring : Database mirroring is a solution to increase database availability by supporting almost instantaneous failover. Database mirroring can be used to maintain a single standby database, or mirror database, for a corresponding production database that is referred to as the principal database. This feature is deprecated and not recommended for high availability solutions

- Log Shipping: Like AlwaysOn Availability Groups and database mirroring, log shipping operates at the database level. You can use log shipping to maintain one or more warm standby databases (referred to as secondary databases) for a single production database that is referred to as the primary database
- Oracle
  - Oracle database built-in high availability capabilities are as follows:
  - Real Application Clusters (RAC)
  - Data Guard
  - Automatic Storage Management (ASM)
  - Flashback, Recovery Manager (RMAN)
  - Online Reorganization
  - Edition-based Redefinition



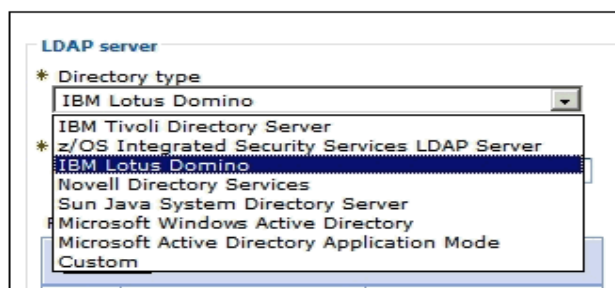
## Planning the environment

This sections describes the planning required for IBM Connections before installation.

### 3.1 LDAP

LDAP (lightweight directory access protocol) is a protocol used by most Enterprise directories for talking to each other in a common language. In an IBM Connections environment, the WebSphere servers must be able to talk to a corporate directory to both authenticate users who are accessing the system and to import and manage user profiles.

In the IBM Connections pre-installation step, it is a requirement that the WebSphere Application Server server be configured to access one or more LDAP servers. It is very common to tell the WebSphere server of a host name that directs requests through a load balancer to multiple LDAP servers. Many LDAP servers are pre-configured in the WebSphere server including Microsoft Active Directory, IBM Domino, and IBM Tivoli Directory Servers, however, any LDAP compatible directory is supported.



LDAP performance and stability is critical for IBM Connections to work at all.

## 3.2 DNS and host names

Domain Naming System (DNS) is a distributed database management system for managing host names and their associated Internet Protocol (IP) addresses. In an enterprise environment, the host names are registered in DNS server, so that the user can query the system by host name instead of typing the IP address.

IBM Connections server uses the DNS server to query the database server, directory server, mail server and application server. The host name of the IBM Connections server must be defined as fully qualified name, for example, "connections.ibm.com".

SMTP Notifications server

IBM Connections applications uses Simple Mail Transfer Protocol (SMTP) server to send notifications to the users. The SMTP sever must be installed separately in the same network or different network.

## 3.3 Shared content storage location

IBM Connections server uses shared content directory to store application contents. The content directory resides in a shared repository that provides read and write accessible to the WebSphere Deployment manager and all nodes. Network File Share (NFS) V4 is recommended for UNIX and Linux platform. The following table summarizes the usage of disk space for each application in enterprise environment.

| Feature Name      | Disk Space |
|-------------------|------------|
| Activities        | 10 GB      |
| Files             | 10 GB      |
| Wikis             | 10 GB      |
| Search            | 15 GB      |
| Blogs             | 10 GB      |
| Communities       | 3 GB       |
| Homepage          | 100 MB     |
| Message stores    | 6 GB       |
| Bookmarks(Dogear) | 600 MB     |

## 3.4 LTPA and single sign on

IBM Connections uses single sign-on (SSO) to secure the transfer of user ID and password information that users provide to be authenticated. The authentication is done once per session and then the users can switch to different applications without needing to be authenticated again.

SSO is automatically enabled when IBM Connections is installed on a single WebSphere Application Server profile or when different profiles are federated into the same cell.

IBM Connections supports several methods to implement SSO for you to choose based on how your environment was planned.

If you already have an Intranet that requires authentication, you can share the credential with your IBM Connections. For example, you have an Intranet hosted on a Domino Web Server,

you can shared the credential with the IBM Connections using SSO for Domino ([http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Enabling\\_single\\_signon\\_for\\_Domino\\_ic40](http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Enabling_single_signon_for_Domino_ic40)).

If you already have a Tivoli Access Manager environment, you can use WebSphere cookie-based lightweight third-party authentication (LTPA) as an SSO solution to authenticate your IBM Connections environment. You can read the uses of the SSO at IBM Connections Wiki

([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Configuring\\_single\\_signon\\_ic40&content=pdfcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Configuring_single_signon_ic40&content=pdfcontent)).

On our lab environment, we use SSO domain name. For the installation details, 6.10, “Post installation environment configuration” on page 127.

## 3.5 SSL certificates

On your architecture environment, you must identify what are the components that provide sensible data to secure the communication using SSL to protect the data traffic .

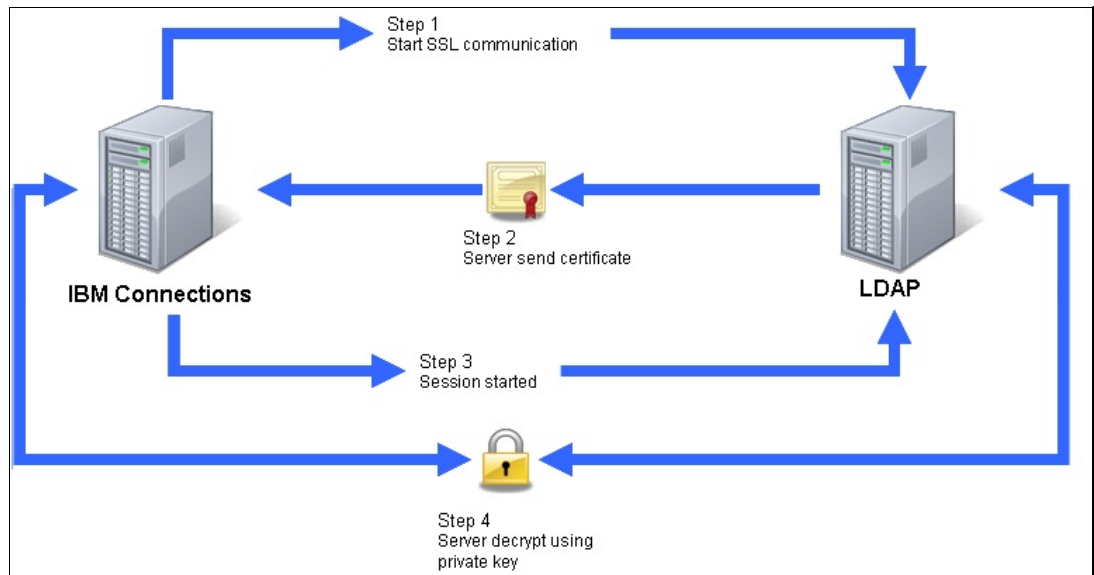
For example:

- ▶ You can use SSL to secure the LDAP communication during the authenticating user name and password.
- ▶ To secure IBM Connections communications, you can use Secure Sock Layer (SSL) between the IBM Connections and user web browser.

The figure below represents an SSL communication between IBM Connections and LDAP server:

- ▶ Step 1 - IBM Connections server requests a SSL communication using LDAP protocol (TCP Port 636).
- ▶ Step 2 - LDAP servers sent a certificate to IBM Connections server, this certificate checks the validation of the certificate, if it is signed by some Certificate Authority and the Full Qualified Domain Name (FQDN) used to access the server.
- ▶ Step 3 - If the IBM Connections has the certificate on the Trust store, the session can be started, if not, you must to import the certificate on the IBM Connections
- ▶ Step 4 - All data are encrypted using the certificate sent on step 2, and the LDAP server can decrypt the information using the private key.





The process to import the certificate on IBM Connections is detailed on 6.10, “Post installation environment configuration” on page 127.

## 3.6 Multiple language content

IBM Connections applications support multiple pre-defined languages. By default, the default language of the browser is chosen for the current user session. The customer has to consider the default language and prioritize the order of other languages for IBM Connections applications.

## 3.7 Deployment checklist

IBM Connections applications communicate with various backend applications. Make sure that the following conditions are met prior to starting the IBM Connections server installation.

- ▶ For IBM Connections 4.0, we recommend to use 64-bit operating system server for better performance.
- ▶ If the registered user is less than 1000, consider choosing a small deployment scenario, where all the applications and databases are installed in same machine. Separating the database server from IBM Connections server provides the better performance and is recommended.
- ▶ If the registered user is less than 10 000, consider choosing a medium deployment scenario, where IBM Connections applications are grouped together and installed into multiple clusters.
- ▶ If the registered user is higher than 10 000, consider choosing a large deployment scenario, where each application is installed into dedicated application server cluster.
- ▶ 50 GB of available space required for installing IBM Connections.
- ▶ We recommend to use IBM WebSphere Application Server Edge components to cache the content data for IBM Connections applications.

- ▶ The location of shared content storage directory must be accessible to Deployment manager and all the nodes.
- ▶ Select the language used by registered users to access the IBM Connections applications. List the SMTP server details to enable notification for IBM Connections applications.
- ▶ LDAP server details required prior to starting IBM Connections server installation.
- ▶ Cognos Business Intelligence server can be installed prior or after to IBM Connections server
- ▶ IBM Connections server supports IBM DB2, Oracle, and Microsoft SQL database server to store application data. Setup any one of the database server on dedicated server.
- ▶ Populate users from the LDAP repository to the Profiles database for IBM Connections applications.
- ▶ For small and medium deployment, the maximum heap size was set to 2048 MB during the installation. For large deployment the default heap size is set to 256 MB. For larger deployment, the sum of heap size of the entire application server should be less than physical memory of the server.
- ▶ Configure IBM HTTP Server and add certificates to the WebSphere trust store.
- ▶ By default, Common and Widget container applications are installed with News application on News Cluster. We recommend to uninstall Common and Widget container applications from News cluster and install it on a dedicated cluster.



## Planning Profiles

Planning for Profiles usually takes most time and is the most challenging of all the features of IBM Connections because it utilizes data imported from the organization LDAP. This data can contain information such as user names, email, uid, and so on.

Some points to take care of while planning are:

- ▶ Which data sources are to be used?
- ▶ What are the field specifications of the source data (field name, type, data length)?
- ▶ Is data required to be synchronized and in what direction?
- ▶ If required, where are the additional data files like Photos located?
- ▶ Which fields are to be mapped 1:1?
- ▶ Which data fields are displayed in a profile entry, and which of them are editable by users?

It is also critical to ensure that IBM Connections has the proper access to the data and that the two systems can work together regarding data updates and synchronization.

### 4.1 Photographs

It is also possible to upload individual user photographs while creating IBM Connections Profiles. To do this, first you must identify which photo repository is to be used and then where you want the photographs dump to be taken for uploading.

The upload file size limit is 15 KB so this aspect needs to be taken care of while planning.

### 4.2 Setting up Manager attributes

The setting up of Manager attributes in user profiles is an optional but desired feature of Profiles population.

Each user profile contains a `manager_uid` field which stores the UID value of that person's manager. This information is used to build the *Reports To* display widget in the Profiles user interface.

Additionally, the `isManager` field (which equates to the Mark manager mapping task in the Profiles population wizard) is used to mark the user profile as being a manager. This information is used to build the *People Managed* display widget in the Profiles user interface. A Y or N attribute is assigned to an employee to indicate whether the employee is listed as a manager of other employees.

While planning, you have to decide whether you want to populate these fields or not and accordingly decide on running the required scripts.

## 4.3 Cleaning up data sources

Before you import data into the IBM Connections databases, we suggest that you clean up your data sources and remove any redundant data. This not only leads to an error free import but also gives you an updated environment that you can use for other environments also. Also, it will save time during the import process.

This step should always be included in the deployment plan as apart from the advantages as mentioned above, cleaning up will also help you avoid any potential future issues in case you go for a clean up post installation of IBM Connections. In worst cases, you might need to do the import of Profiles data again.

## 4.4 Designing profiles

IBM Connections uses the data populated in various columns of PEOPLEDB and other related databases for displaying different attributes of a user profile. All these values are the ones that are imported from various LDAP fields. If not specifically mentioned, these values are populated using the default mapping by the population wizard.

We recommend to have a detailed field level information of your LDAP ready before the data population. This helps you to accurately populate the data in the mapped fields and avoid any potential future issues.

## 4.5 Using profile types for custom profiles by user name

A profile-type defines a set of properties, also referred to as a schema, that are inherent to all profiles of that type. This set of properties is used internally to group objects and enforce overall system constraints. Examples of common profile-types are customer, employee, and contractor.

All profile records are classified by their profile-type property. If a property is not specified in the profile-type property definition of a profile record, it is not exposed to the Profiles user, either in the user interface or API. The deployer uniquely identifies each profile type using a *64-byte profile-type identifier* string.

Profile-type definitions are declared and managed in the `profiles-types.xml` file.

Profile-types are managed in an object hierarchy with the following rules:

- ▶ Profiles defines a single base type of *snx:person* that enumerates the set of fields required on all profile records.
- ▶ You can define subtypes of *snx:person* (such as customer, employee, or contractor) to add your own unique properties.
- ▶ A profile-type inherits all the property references from its parent type.
- ▶ A profile-type hierarchy cannot contain circular loops. The application will fail to start if any loops are detected in the configured hierarchy.
- ▶ A profile-type declaration that omits a *parentId* implicitly inherits from *snx:person*.

The following is a sample code:

---

```
<config>
  <type>
    <parentId>snx:person</parentId>
    <id>customer</id>
    ...
  </type>
</config>
```

---

### 4.5.1 Default profile-type

We recommend to explicitly map a defined profile-type to each profile record in the Profiles database as a part of the Profiles population process. If no profile-type is associated with the profile record, the Profiles application interprets the empty profile-type value as equivalent to the *default* value.

If the declaration of the *default* profile-type has been removed from the *profiles-types.xml* file, the application assigns the profile record the *snx:person* profile type. As a result, the application only presents the minimal set of attributes defined in the *snx:person* profile-type in the user interface.



## Preinstallation tasks

In this chapter, we explain the tasks that must be performed before installing IBM Connections. After you have decided the architecture environment, you must prepare your environment for IBM Connections installation.

- ▶ 5.1, “Verify software requirements” on page 40
- ▶ 5.2, “Setting up DNS and testing host names” on page 41
- ▶ 5.3, “Setting up LDAP and testing LDAP for data quality” on page 42
- ▶ 5.4, “Populating photo repository” on page 44
- ▶ 5.5, “Verifying operating system installation and disk space available” on page 47



## 5.1 Verify software requirements

An IBM Connections environment consists of many software such as WebSphere Application Server, relational database server, and Cognos. Some of the software come with IBM Connections. IBM Connections 4 is available at IBM Passport Advantage website at: <http://www.ibm.com/software/howtobuy/passportadvantage/>.

For the download procedures, see (Appendix C, “Downloading the software from Passport Advantage and PartnerWorld” on page 286)

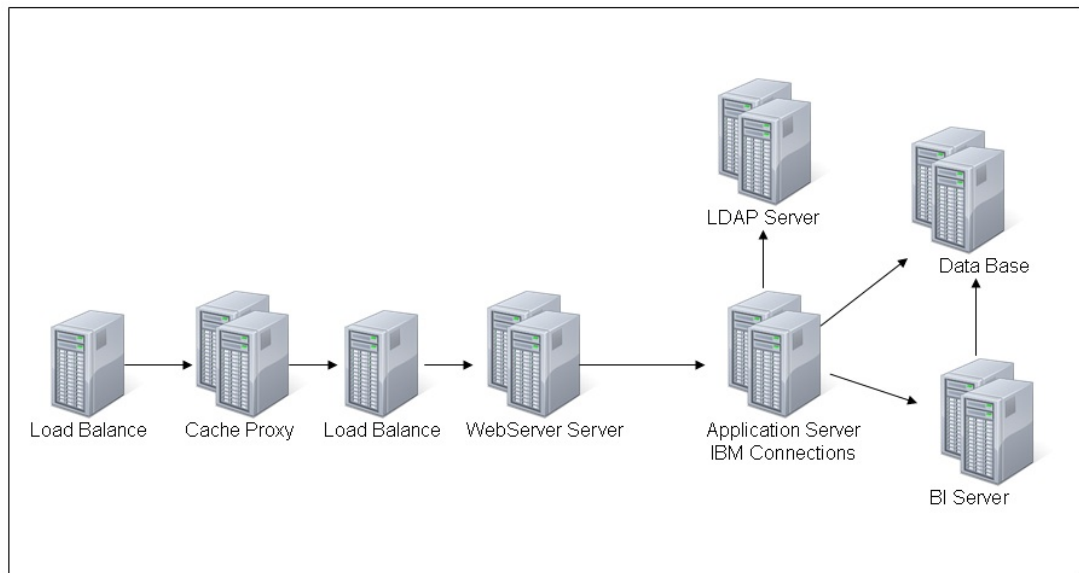
You also can find the part numbers related to the IBM Connections at: <http://www.ibm.com/support/docview.wss?uid=swg24033179>

The Sales Manual is at:

[http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep\\_sm/8/649/ENUS5724-S68/index.html&lang=en&request\\_locale=en](http://www-01.ibm.com/common/ssi/ShowDoc.wss?docURL=/common/ssi/rep_sm/8/649/ENUS5724-S68/index.html&lang=en&request_locale=en)

Prior to install IBM Connections and required software product, you must verify the software version of your IBM Connections environment to be deployed as described in 2.3, “Software requirements” on page 16.

The following figure shows our IBM Connections lab architecture based on software.



We use the following products:

- For the load balance and caching-proxy the software used is Edge components provided on WebSphere Application Server Supplementals packages, check the system requirements at <http://www-01.ibm.com/support/docview.wss?uid=swg27012442>
- For the web servers, the software installed is IBM HTTP Server that also provided on WebSphere Application Server Supplementals packages. For more information, see <http://www-01.ibm.com/software/webservers/httpservers/sysreq/>
- We also have the WebSphere Application Server installed on 3 servers. For the system requirements, visit <http://www-01.ibm.com/support/docview.wss?uid=swg27006921>  
IBM Cognos is installed on one server. For system requirements, visit <http://www-01.ibm.com/support/docview.wss?uid=swg27019126>

- For LDAP servers, we installed IBM Domino. For system requirements, visit <http://www-01.ibm.com/support/docview.wss?uid=swg27007909>
- For database, we have installed DB2. For system requirements, visit <http://www-01.ibm.com/support/docview.wss?uid=swg27010711>

All software installed on our lab environment are provided on IBM Connections packages.

You can find more information about the supported software at:

<http://publib.boulder.ibm.com/infocenter/prodguid/v1r0/clarity-reports/report/html/prereqsForProduct?deliverableId=1284667107599>

## 5.2 Setting up DNS and testing host names

An IBM Connections environment consists in many servers that run various software product integrated with IBM Connections. The communications between those servers is based on TCP connections and name resolution through dynamic name server (DNS), so you must have a DNS server configured on your environment, because during the installation and configuration process, you must provide host names of the following server:

- Database servers
- LDAP Servers
- WebSphere Application Servers
- Web Servers
- Other components such as Cognos server, Domino mail server, Identity Manager server, WebSphere Portal server, and Security Management server

Check if the servers can communicate with each other with the **ping** command. Run the following command to check the host name resolution on all the servers of your environment: **ping**

For example, from a WebSphere Application Server server, you can try to ping a web server, LDAP server, database server and all other servers that will be part of the IBM Connections deployment such as Cognos server and Tivoli Directory Integrator server.

The following figure shows that we can ping the IBM HTTP server (con-ihs01.itso.ibm.com) and LDAP server (ldap-dom.itso.ibm.com) from WebSphere Application Server (con-dmgr.itso.ibm.com) in our lab environment.

```
con-dmgr:~ # ping con-ihs01.itso.ibm.com
PING con-ihs01 (10.52.78.15) 56(84) bytes of data.
64 bytes from con-ihs01 (10.52.78.15): icmp_seq=1 ttl=128 time=4.84 ms
^C
--- con-ihs01 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 4.843/4.843/4.843/0.000 ms
con-dmgr:~ # ping ldap-dom.itso.ibm.com
PING ldap-dom.itso.ibm.com (10.52.78.14) 56(84) bytes of data.
64 bytes from ldap-dom.itso.ibm.com (10.52.78.14): icmp_seq=1 ttl=128 time=0.497
ms
^C
--- ldap-dom.itso.ibm.com ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.497/0.497/0.497/0.000 ms
con-dmgr:~ #
```

## 5.3 Setting up LDAP and testing LDAP for data quality

In our lab, we use Domino Directory Server as the LDAP users repository. If you want to use an existing LDAP Server other than Domino, make sure that it is V3 LDAP compliant.

Determine which Lightweight Directory Access Protocol (LDAP) attributes you want to use as the identifiers for IBM Connections users. Ensure that you have installed a supported LDAP directory.

### 5.3.1 LDAP pre-requirements

To ensure that the Profiles population wizard can return the maximum number of records from your LDAP directory, set the Size Limit parameter in your LDAP configuration to match the number of users in the directory. For example, if your directory has 100,000 users, set this parameter to 100000. If you cannot set the Size Limit parameter, you can run the wizard multiple times. Alternatively, you can write a JavaScript function to split the original LDAP search filter, run the **collect\_dns\_iterate.bat** file, and then run the **populate\_from\_dns\_files.bat** file.

**Note:** For information about a limitation in environments with a Turkish locale, see the Base entry comparison for Turkish locale technote (<http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.wim.doc/baseentrycomparisonforturkishlocale.html>).

To prepare to configure your LDAP directory with IBM WebSphere Application Server, complete the following steps:

1. Identify LDAP attributes to use for the following roles. If no corresponding attribute exists, create one. You can use an attribute for multiple purposes. For example, you can use the mail attribute to perform the login and messaging tasks.
  - Display name  
The cn LDAP attribute is used to display a person's name in the product user interface. Ensure that the value you use in the cn attribute is suitable for use as a display name.
  - Log in  
Determine the attributes that you want the users to use to log in to IBM Connections. For example, uid.

**Note:** The login name must be unique in the LDAP directory.

  - Messaging  
(Optional) Determine which attribute to use to define the email address of a user. The email address must be unique in the LDAP directory. If a user does not have an email address and does not have an LDAP attribute that represents the email address, that user cannot receive notifications.
  - Global unique identifier (GUID)  
Determine which attribute to use as the unique identifier of each user and group in the organization. This value must be unique across the organization.
2. Collect the following information about your LDAP directory before configuring it for WebSphere Application Server:

- Directory Type: Identifies and selects a directory service from the available vendors and versions.
- Primary host name
- Port
- Bind distinguished name
- Bind password
- Certificate mapping
- Certificate filter, if applicable.
- LDAP entity types or classes: Identifies and selects LDAP object classes. For example, select the LDAP inetOrgPerson object class for the Person Account entity, or the LDAP groupOfUniqueNames object class for the Group entity.
- Search base: Identifies and selects the distinguished name (DN) of the LDAP subtree as the search scope, for example, **select o=ibm.com** to allow all directory objects underneath this subtree node to be searched. Examples for the Group Search, use the following LDAP attributes: Group, OrgContainer, PersonAccount, or inetOrgPerson.

### 5.3.2 Installing Domino

First you have to install an IBM Domino Server on designated machine, following the steps below:

1. Choose a name for the server. Refer to the name that you created based on your structure.
2. Identify the function of the server - for example, will it be a mail server or application server? On our lab we are using as mail server, the function of the server determines which tasks to enable during configuration.
3. Decide whether the server is part of an existing Domino domain or is the first server in a new Domino domain.
4. Our lab Domino is the first in a Domino domain, do the following:
  - a. Install the server program files.
  - b. Use the Domino server setup program to set up the server
  - c. Complete network-related setup.
  - d. Create organization certifier IDs and organizational unit certifier IDs as required by the hierarchical name scheme.
  - e. Distribute certifier IDs to administrators.
  - f. Implement Domino security.
5. Perform additional configuration procedures, based on the type of services, tasks, and programs that you want to run on this server.

After the Domino installation, you have to setting up the LDAP service on Domino

Follow these steps to set up a server to run LDAP service:

1. The LDAP task runs automatically on the administration server for the primary Domino Directory. On other servers in the domain, if configured, run the LDAP task manually
2. If your organization uses more than one Global Domain document, specify the one that the LDAP services uses to return Internet address to LDAP clients. Open the Global Domain document. In the "Use as default Global Domain" field, choose Yes.

3. To check whether you set up the LDAP service correctly, use an LDAP search utility such as `ldapsearch` provided with Domino, to issue a query to the LDAP service. Example from a group search:

```
ldapsearch -D -w -b "o=itso" -s sub  
"(|(objectclass=groupOfNames)(objectclass=groupOfUniqueNames))" dn
```

You have installed and enabled Domino to run LDAP services.

## 5.4 Populating photo repository

IBM Connections allows you to enhance your profile by adding a picture from yourselves enabling the profile photo feature. Depending on your organization's needs, you can choose specific profiles to enable or disable this feature. You can also configure access control settings for the profile photo feature according to profile type. You can populate your database photo repository using Tivoli Directory Integrator assembly-line commands

### 5.4.1 Populating photo repository

You can use the **dump\_photos\_to\_files** and **load\_photos\_from\_file** assembly-line commands to populate the profiles database with photo files. These commands are useful when you are moving the profiles database, allowing you to save the photos from the existing database on disk, repopulate the new database from the LDAP, and then load the photo files back into the new database.

To populate a new profiles database with photos, complete the following steps.

1. Use the **dump\_photos\_to\_files.bat** or **dump\_photos\_to\_files.sh** command to read the existing photos from the profiles database and store them on disk:

The following table shows the properties that are used by this command, and their default values. These properties can be found in the `profiles_tdi.properties` file.

| Property                             | Description   |
|--------------------------------------|---|
| <code>dump_photos_directory</code>   | The directory where the extracted files are stored. The default value is <code>/dump_photos</code> .  |
| <code>dump_photos_file</code>        | The list of people whose photos were collected. The default value is <code>collect_photos.in</code> .   |
| <code>load_photos_simple_file</code> | The list of people whose photos were collected. The default value is <code>collect_photos.in</code> . If you want to load only a subset of files from a location, edit this file. |

**Note:** When dumping multiple photo files, there must be a period separator between each entry. If the separator is omitted, an error is generated when you use the **load** command to import the files into the profiles database.

2. To populate the new database with the photo files that you saved in the previous step, use the **load\_photos\_from\_files.bat** or **load\_photos\_from\_files.sh** command to read the files from disk and populate the Profiles database with them.

**Note:**

- ▶ The table in step 1 shows the properties that relate to this command.
- ▶ Although in IBM Connections 2.0, the Profiles application can crop the photo uploaded by a user, the photo size limit in the underlying database is 15 KB. When Profiles is used with IBM Tivoli Access Manager enabled, the Tivoli Access Manager can only load files conforming to this size limit.

**Example**

Here is an example of an entry from the collect\_photos.in file:

---

```
photo:file:/C:/install_directory/TDISOL/TDI/./dump_photos/img1197046202619_9.dat
uid:FAdams
```

---

The characters following uid corresponds to the PROF\_UID in the profiles database.

Note the required period separator between each entry, for example,

---

```
photo:file:/C:/install_directory/TDISOL/TDI/./dump_photos/img1197046202619_9.dat
uid:FAdams
.
photo:file:/C:/install_directory/TDISOL/TDI/./dump_photos/img1197146402316_7.dat
uid:TAmado
.
```

---

You have finished to import your photos to IBM Connections.

## 5.4.2 Enabling profile photo

Edit settings in the *profiles-policy.xml* file to configure the profile photo feature according to profile type. To edit configuration files, you must use the IBM WebSphere Application Server wsadmin client. See Starting the wsadmin client ([http://infolib.lotus.com/resources/connections/4.0/doc/en\\_us/ic4\\_p5.html#t\\_admin\\_wsadmin\\_starting](http://infolib.lotus.com/resources/connections/4.0/doc/en_us/ic4_p5.html#t_admin_wsadmin_starting)) for information about how to start the wsadmin command-line tool.

The following steps provide information about the properties that you can set for the profile photo feature, and the access levels and scopes that you can configure.

1. Start the wsadmin client from the following directory of the system on which you installed the Deployment Manager: app\_server\_root ([http://infolib.lotus.com/resources/connections/4.0/doc/en\\_us/ic4\\_p5.html#i\\_ovr\\_r\\_directory\\_conventions](http://infolib.lotus.com/resources/connections/4.0/doc/en_us/ic4_p5.html#i_ovr_r_directory_conventions))\profiles\dm\_profile\_root\bin

where *app\_server\_root* is the WebSphere Application Server installation directory and *dm\_profile\_root* is the Deployment Manager profile directory, typically dmgr01.

You must start the client from this directory or subsequent commands that you enter do not execute correctly.

2. Start the Profiles Jython script interpreter.

Enter the following command to access the Profiles configuration files:

```
execfile("profilesAdmin.py")
```

If prompted to specify a service to connect to, type **1** to pick the first node in the list. Most commands can run on any node. If the command writes or reads information to or from a file using a local file path, you must pick the node where the file is stored.

3. Use the following command to check out the profiles-policy.xml file:

```
ProfilesConfigService.checkOutPolicyConfig("", "cell_name")
```

where:

- *working\_directory* is the temporary working directory to which the configuration XML and XSD files will be copied. The files are kept in this working directory while you make changes to them.
- *cell\_name* is the name of the IBM WebSphere Application Server cell hosting the Profiles application. This argument is required.

For example:

```
ProfilesConfigService.checkOutPolicyConfig("/wsadminoutput",  
"jdoe30Node02Cell")
```

4. Open the profiles-policy.xml file using a text editor, from the temporary directory to which you checked it out.

5. Edit the following properties for the profile photo feature as needed.

- profile.photo

Enables or disables the profile photo feature.

This property takes a string value. Possible values include:

- **true**. Enables the photo feature for users with the specified profile type. The user interface displays the user's photo and provides options for editing the photo.
- **false**. Disables the photo feature for users with the specified profile type. The user interface does not display the user's photo or options for editing the photo. A generic photo image is displayed in place of the user's photo.

- profile.photo.update

Control access to view the photo.

In addition to the scope attribute for this access control, *dissallowNonAdminIfInactive* can be used to indicate whether photos for inactive users can be viewed. Administrative users can view photos regardless of the configuration.

Access levels for this property can be defined using one of the following scopes:

- **none**. No one can update the profile photo of users with the specified profile type.
- **self**. Users with the specified profile type can update their own profile photo. Administrators can also update the profile photo of users with the specified profile type.

- profile.photo.view

Controls access to view the photo.

In addition to the *scope* attribute for this access control, *dissallowNonAdminIfInactive* can be used to indicate whether photos for inactive users can be viewed. Administrative users can view photos regardless of the configuration.

In the following photo policy sample, users who have been assigned the *reader* role can view active user's photos with the *default* profile type, but photos for inactive users

are only viewable by users who have been assigned the *admin* role. When a user's photo is not viewable, the default gray photo image is displayed.

---

```
<profileType type="default" enabled="true">
<acl name="profile.photo.view" scope="reader"
dissallowNonAdminIfInactive="true"/>
<acl name="profile.photo.update" scope="self" />
</profileType>
```

---

The following sample enables the profile photo feature for the default profile type, but restricts access to update profile photos to profile owners and administrators. For users with the contractor profile type, the profile photo is enabled, but no access is provided to update the profile photo for users of this profile type. The profile photo feature is disabled for users with the visitor profile type, and no one can update the profile photo for users of this profile type.

---

```
<feature name="profile.photo">
  <profileType type="default" enabled="true">
    <acl name="profile.photo.update" scope="self" />
  </profileType>
  <profileType type="contractor" enabled="true">
    <acl name="profile.photo.update" scope="none" />
  </profileType>
  <profileType type="visitor" enabled="false">
    <acl name="profile.photo.update" scope="none" />
  </profileType>
</feature>
```

---

6. Save your changes and check the `profiles-policy.xml` file back in using the following command:

```
ProfilesConfigService.checkInPolicyConfig()
```

7. To exit the `wsadmin` client, type `exit` at the prompt.
8. Stop and restart the Profiles server.

You have enable the photo profile.

## 5.5 Verifying operating system installation and disk space available

Before installing your IBM Connections environment, you must verify if your operation system are supported and provide sufficient disk space for a successful installation and operation of the product that you plan to install.

### 5.5.1 Operating system requirements

#### Linux

For IBM Connections on Linux ensure that you have the following packages and libraries installed:

- ▶ `scompat-libstdc++-33.x86_64`
- ▶ `libcanna-gtk2.i686`



- ▶ PackageKit-gtk-module
- ▶ gtk2.i686
- ▶ compat-libstdc++-33.i686
- ▶ compat-libstdc++-296
- ▶ compat-libstdc++
- ▶ libXtst.i686

**Note:** Ensure that the GTK library is available on your system. Even when your IBM Connection is to be installed on a 64-bit system, you still need the 32-bit version of the GTK library. If you use silent mode or console mode to install IBM Connections, you do not need the GTK libraries.

## AIX

For IBM Connections on AIX, ensure that you have X11 package installed on you server:

- ▶ X11.base.rte
- ▶ X11.apps.config

## Windows

IBM Connections on Windows does not required any additional software to be installed.

### 5.5.2 Applying operating system patches

It is important to have the operating system patches required for the IBM Connections to avoid installation issues on your environment. You can check the operating system requisites as described in 2.3, “Software requirements” on page 16.

### 5.5.3 Cognos requirements

If you plan to install Cognos, you need the libraries listed in the Cognos BI 10.1.1 Software Environments - Required Patches technote (<http://www-01.ibm.com/support/docview.wss?uid=swg27022463>).

### 5.5.4 Disk space

It is important to define how many users will use the system and how much data the users might generate to plan your IBM Connections environment. The following is the minimum space required for IBM Connections features:

- ▶ Activities - 10 GB for content store for holding files reference, images reference, text content, and so on.
- ▶ Blogs - 10 GB for content store for holding files reference, images reference, text content, and so on.
- ▶ Bookmarks - 1 GB for FavIcons Directory, the icons that are displayed on Bookmarks.
- ▶ Communities - 3 GB for content store
- ▶ Files - 10 GB for uploaded files, directory stores files to be uploaded to user blogs.
- ▶ Homepage - 1 GB for content store for holding files reference, images reference, text content, and so on.

- ▶ News - 500 MB per message store for holding files reference, images reference, text content, and so on.
- ▶ Profiles - 30 MB for cache file directory
- ▶ Search - 15 GB for index files directory, the disk space required for the search index is depended on the amount of content in the individual IBM Connections features and the disk space required will grow when the IBM Connections content grows.
- ▶ Wiki - 10 GB for content store for holding files reference, images reference, text content, and so on.

**Note:** The sizes of these directories will grow when the number of users and activities increases. Monitor the space available to know when is necessary to increase the capacity.

**Note:** Content store, are all data generated from an application (Activities, Blogs and Homepage) and are stored on databases. All other contents (Files, cache, Index, Temporary and Search) are stored on the shared folder defined during the installation procedure. For IBM Connections environments in WebSphere Application Server Cluster, they are stored on a shared file system, for example, a NFS directory of /opt/IBM/Connections/data/shared on Deployment Manager server

Each product in the IBM Connections environment has its own system requirements. For more information, see the Information Center of the product:

- ▶ Cognos Information Center  
[http://publib.boulder.ibm.com/infocenter/cbi/v10r1m0/index.jsp?topic=%2Fcom.ibm.svg.im.cognos.qrc\\_inst.10.1.0.doc%2Fqrc\\_inst\\_id426VerifySystemRequirements.html](http://publib.boulder.ibm.com/infocenter/cbi/v10r1m0/index.jsp?topic=%2Fcom.ibm.svg.im.cognos.qrc_inst.10.1.0.doc%2Fqrc_inst_id426VerifySystemRequirements.html)
- ▶ DB2 Information Center  
[http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/nav/2\\_0\\_2\\_1\\_2](http://pic.dhe.ibm.com/infocenter/db2luw/v9r7/nav/2_0_2_1_2)
- ▶ WebSphere Application Server Information Center  
[http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.installation.nd.doc/info/ae/ae/tins\\_prepare.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.installation.nd.doc/info/ae/ae/tins_prepare.html)
- ▶ Tivoli Directory Server Information Center  
([http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/install1202.htm?path=8\\_3\\_20#dskspace](http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMDS.doc/install1202.htm?path=8_3_20#dskspace))
- ▶ Tivoli Directory Integrator Information Center  
[http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMIDI.doc\\_7.0/adminguide11.htm?path=7\\_9\\_0\\_9\\_0\\_4\\_4\\_0#wq20](http://pic.dhe.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.IBMIDI.doc_7.0/adminguide11.htm?path=7_9_0_9_0_4_4_0#wq20)
- ▶ IBM Domino <http://publib.boulder.ibm.com/infocenter/domhelp/v8r0/index.jsp>



# Product deployment

Installing IBM Connections can be broken down in to the following distinct phases:

9. Preparing the computer environment - physical or virtual
10. Pre-installing and configuring the components Connections requires to run:
  - a. Setting up the installation manager
  - b. Installing the database
  - c. Creating the databases;
  - d. Installing Tivoli Directory Integrator
  - e. Installing IBM WebSphere Application Server
  - f. Installing IBM HTTP Server
  - g. Installing Cognos Business Intelligence
11. Installing Connections
12. Performing post-installation configuration steps

In this chapter, we describe the product installation and post-installation configuration steps.

- ▶ 6.1, “Setting up the Installation Manager” on page 52
- ▶ 6.2, “Installing the database management system” on page 54
- ▶ 6.3, “Installing Tivoli Directory Integrator” on page 63
- ▶ 6.4, “Installing WebSphere Application Server” on page 70
- ▶ 6.5, “Creating databases” on page 97
- ▶ 6.6, “Populating Profiles using population wizard” on page 98
- ▶ 6.7, “Installing Cognos Business Intelligence” on page 102
- ▶ 6.8, “Installing IBM Connections applications” on page 108
- ▶ 6.9, “Installing IBM HTTP Server” on page 117
- ▶ 6.10, “Post installation environment configuration” on page 127
- ▶ 6.11, “Post installation IBM Connections configuration” on page 160

## 6.1 Setting up the Installation Manager

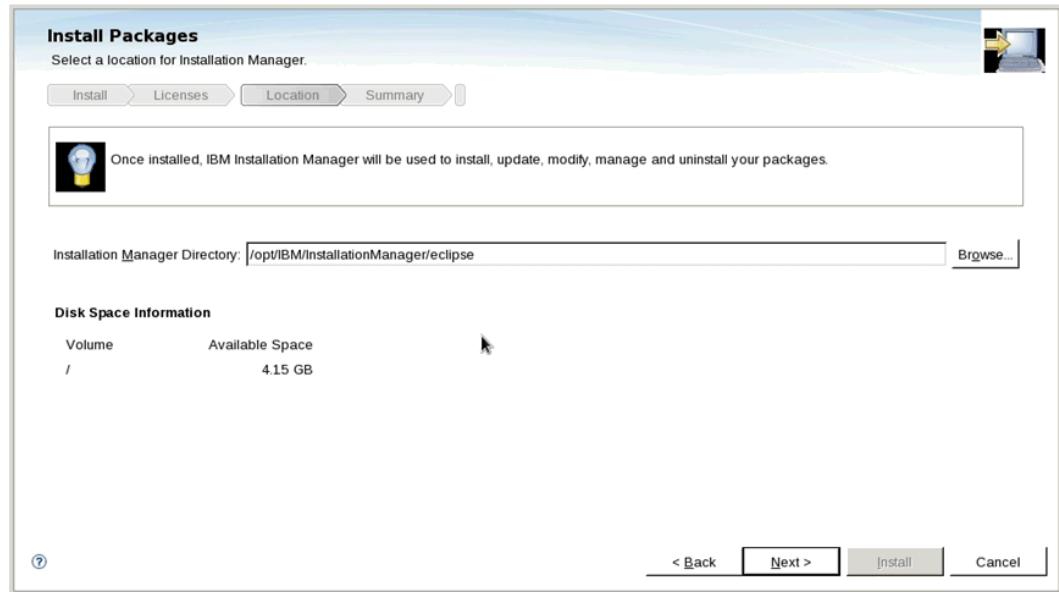
On this section we show you the steps to install the IBM Installation Manager. IBM Installation Manager is a tool responsible for installing, updating, and modifying packages. It allows you to manage IBM software applications and packages. Installation Manager also helps you to track what is installed, what is available for you to install, and organize the installation directories.

IBM Connections 4.0 provides the Installation Manager bundle on the installation package. Follow the steps below to have the IBM Installation Manager installed on you environment:

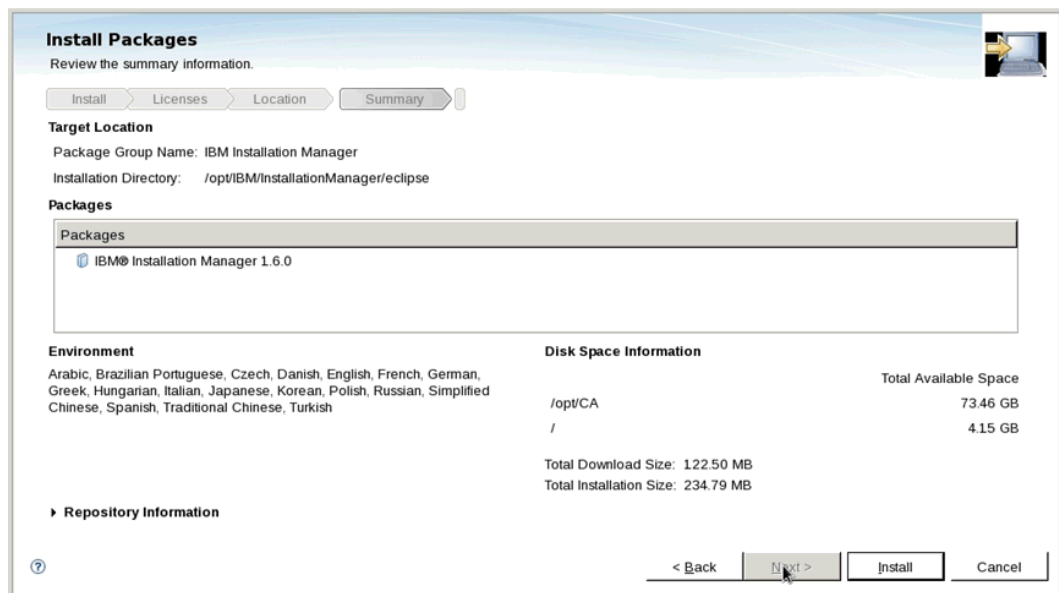
1. Expand the installation package CIA3EML.tar on a temporary directory, for exmaple, /tmp.
2. Run the **install.sh** on /tmp/IBM\_Connections\_Install/IMlinux to start the installation process.
3. Select IBM Installation Manager as the packages to be installed.



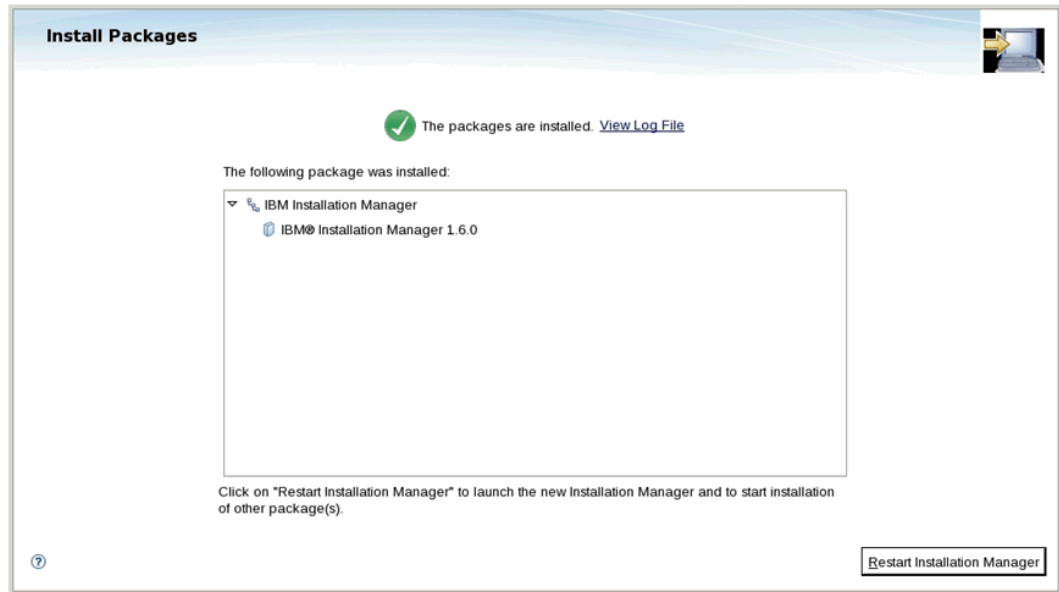
4. Read and accept the license agreement.
5. Select the path where the Installation Manager will be installed.



- Review the summary and click **Install** to start the installation.



- Check if the installation was successful and click **Restart Installation Manager** to start the Installation Manager console.



**Note:** For more information about the IBM Installation Manager, see IBM Information Center (<http://pic.dhe.ibm.com/infocenter/install/v1m0r0/index.jsp>).

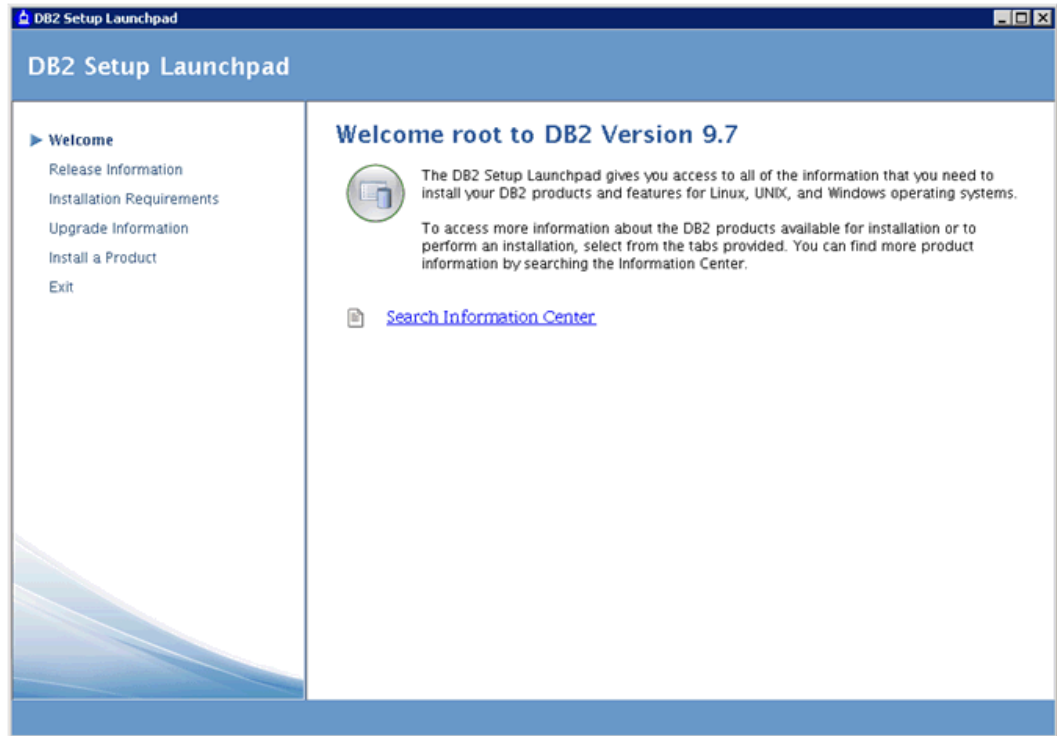
You can find the latest version of the IBM Installation Manager at IBM Support Portal ([http://www-947.ibm.com/support/entry/portal/download%3Ci%3Esoftware/rational/ibm\\_installation\\_manager](http://www-947.ibm.com/support/entry/portal/download%3Ci%3Esoftware/rational/ibm_installation_manager)).

## 6.2 Installing the database management system

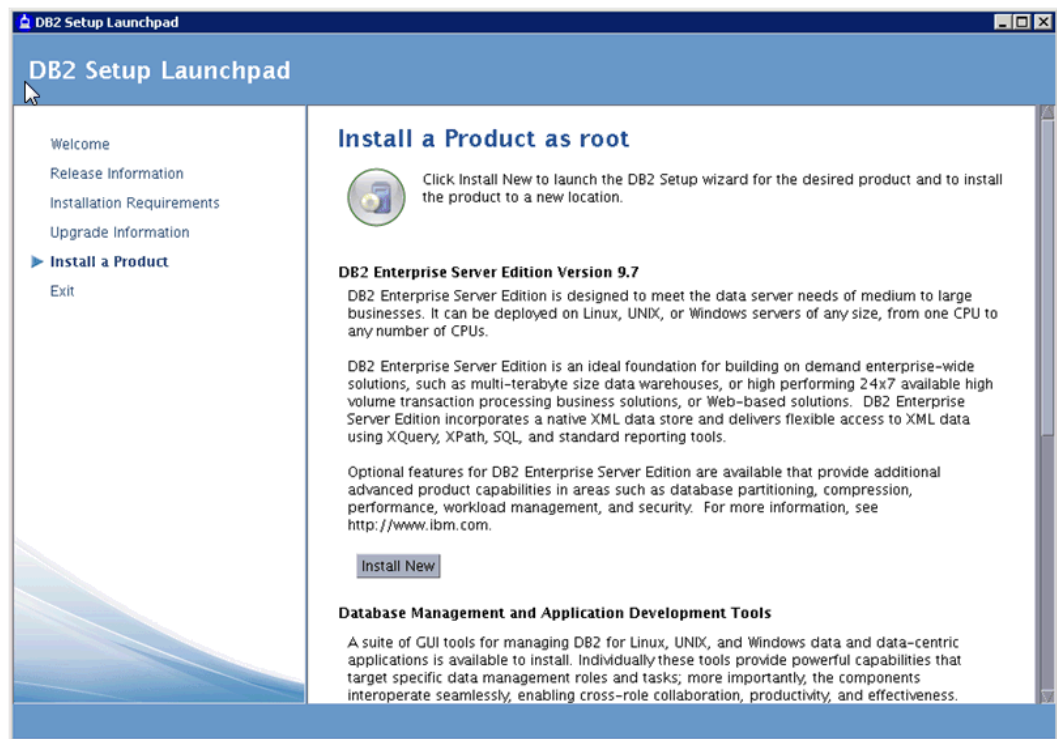
The relational database systems that IBM Connections supports including DB2, Oracle, and Microsoft SQL Server. DB2 is bundled with IBM Connections. In this section, we describe the DB2 installation steps.

In our lab environment, we use the following steps to install DB2 on Linux:

1. Start the installer by launching **db2setup** from the command line in Linux. The following figure shows the DB2 Setup launcher starts. Select on **Install a Product**

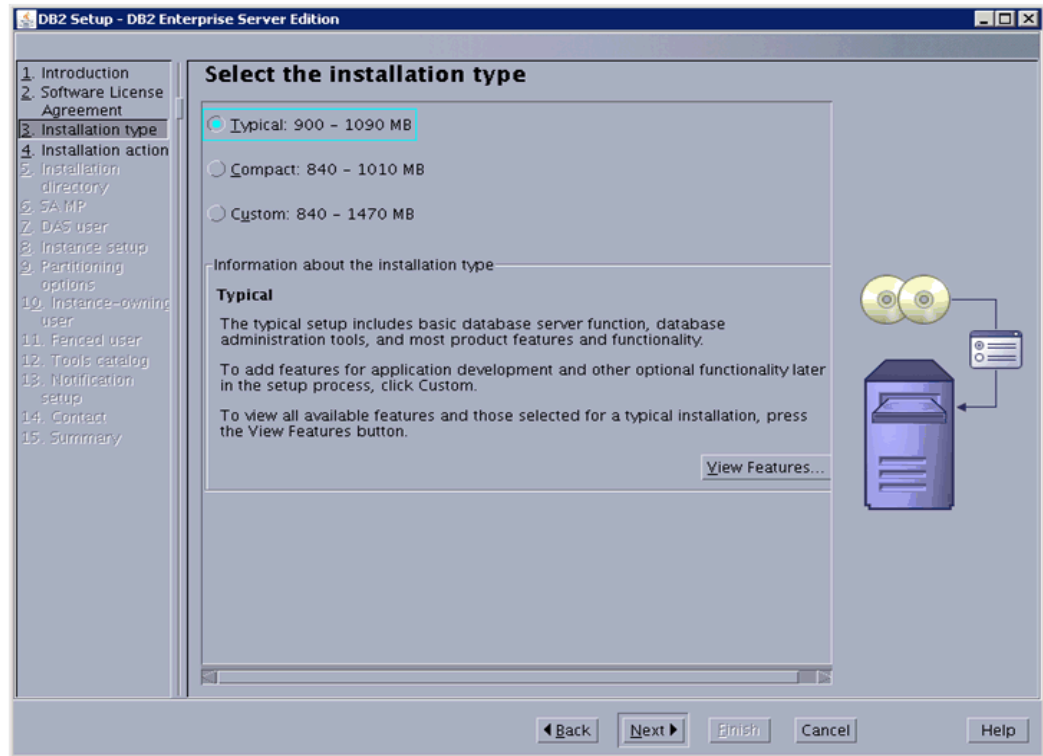


2. Click **Install New**.

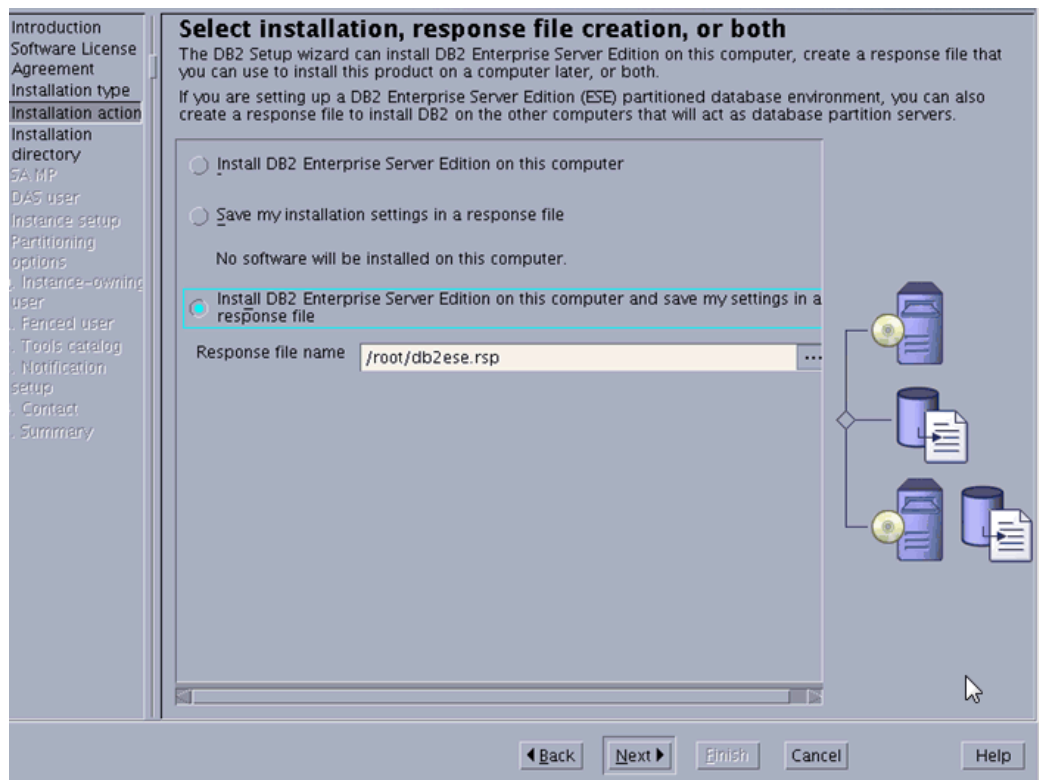


3. In the Welcome to the DB2 Setup Wizard screen, click **Next**.
4. Accept the software License.
5. Choose the **Typical** installation type.

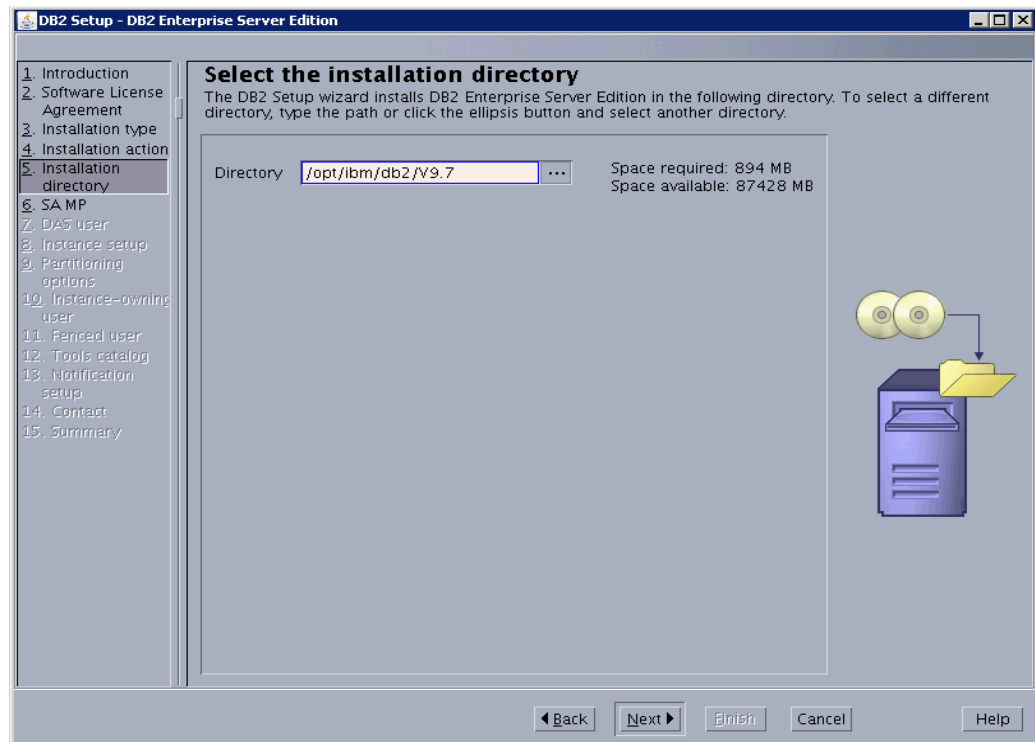




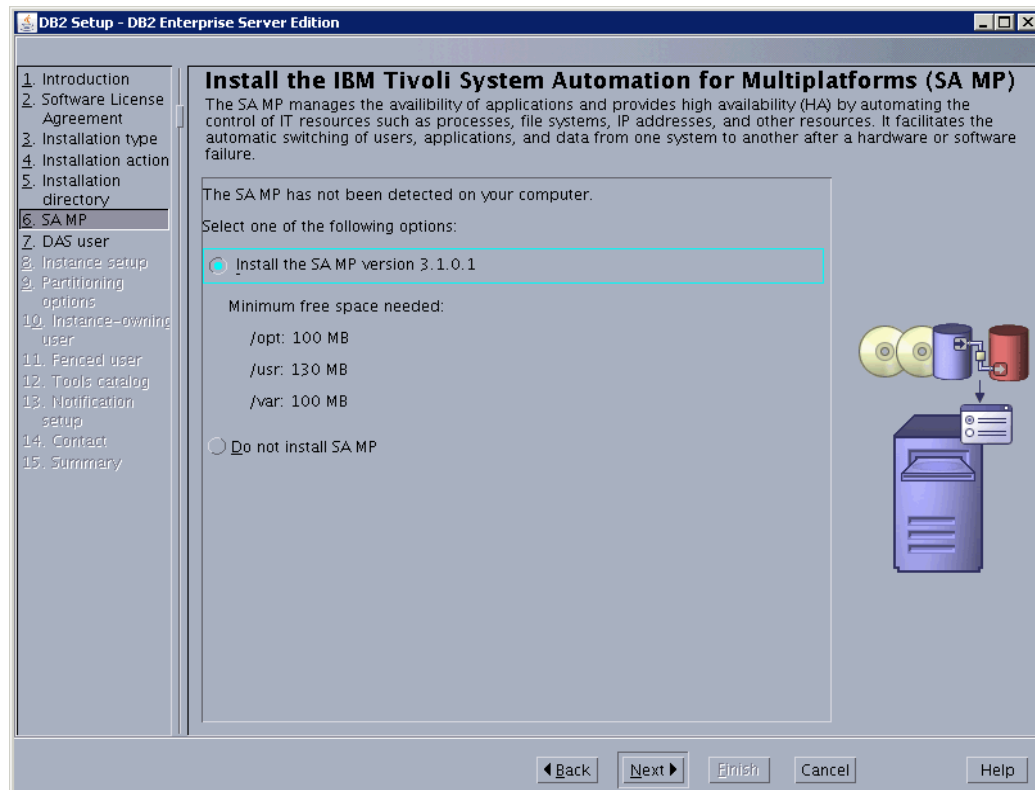
6. We chose to save the responses into a response file, `/root/db2ese.rs`, for future installation. We recommend using the `.rsp` file extension because it is used as a default when selecting a response file in the future.



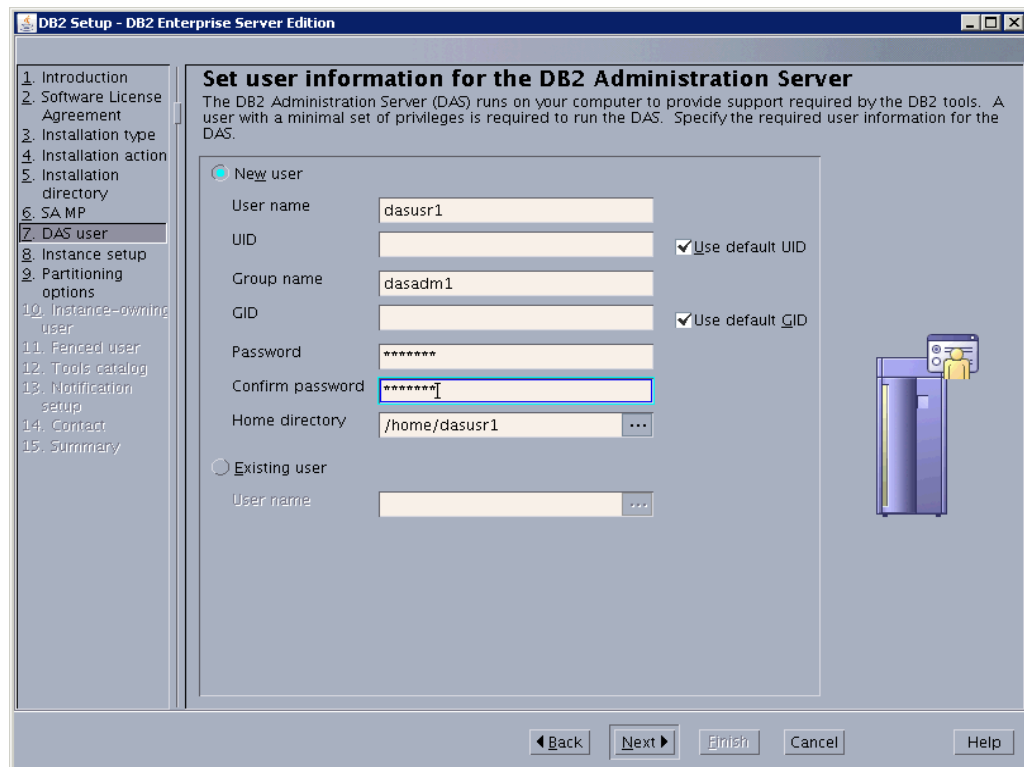
7. Choose the installation directory for DB2. On Linux, we chose to install it to the default directory **/opt/ibm/db2/V9.7**.



8. For our installation, we chose to include the IBM Tivoli System Automation to help us manage a high-availability solution for DB2.



9. Enter the user name and group that the DB2 application will run as. This user name and group should already exist on the operating system. For safety use a user name and group name which will not be present in your LDAP directory.



The screenshot shows the 'Set user information for the DB2 Administration Server' window. The left sidebar lists 15 steps, with '7. DAS user' selected. The main area has a title bar and a description: 'The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.' Below this, there are two radio buttons: 'New user' (selected) and 'Existing user'. The 'New user' section contains fields for 'User name' (dasusr1), 'UID' (empty), 'Group name' (dasadm1), 'GID' (empty), 'Password' (masked with asterisks), 'Confirm password' (masked with asterisks), and 'Home directory' (/home/dasusr1). There are checkboxes for 'Use default UID' and 'Use default GID'. The 'Existing user' section has a 'User name' field. At the bottom are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

**DB2 Setup - DB2 Enterprise Server Edition**

**Set user information for the DB2 Administration Server**

The DB2 Administration Server (DAS) runs on your computer to provide support required by the DB2 tools. A user with a minimal set of privileges is required to run the DAS. Specify the required user information for the DAS.

☒ New user

User name: dasusr1

UID:  ☒ Use default UID

Group name: dasadm1

GID:  ☒ Use default GID

Password:

Confirm password:

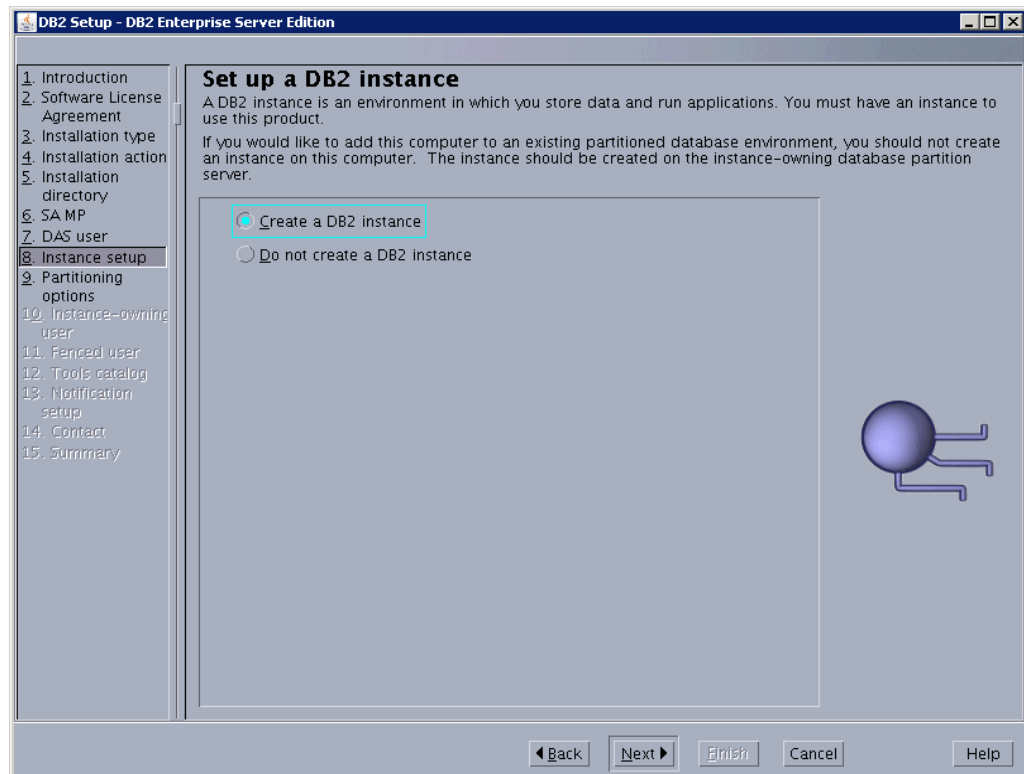
Home directory: /home/dasusr1

☐ Existing user

User name:

Back Next Finish Cancel Help

10. Choose to create a DB2 instance.



The screenshot shows the 'Set up a DB2 instance' window. The left sidebar lists 15 steps, with '8. Instance setup' selected. The main area has a title bar and a description: 'A DB2 instance is an environment in which you store data and run applications. You must have an instance to use this product. If you would like to add this computer to an existing partitioned database environment, you should not create an instance on this computer. The instance should be created on the instance-owning database partition server.' Below this, there are two radio buttons: 'Create a DB2 instance' (selected) and 'Do not create a DB2 instance'. At the bottom are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

**DB2 Setup - DB2 Enterprise Server Edition**

**Set up a DB2 instance**

A DB2 instance is an environment in which you store data and run applications. You must have an instance to use this product.

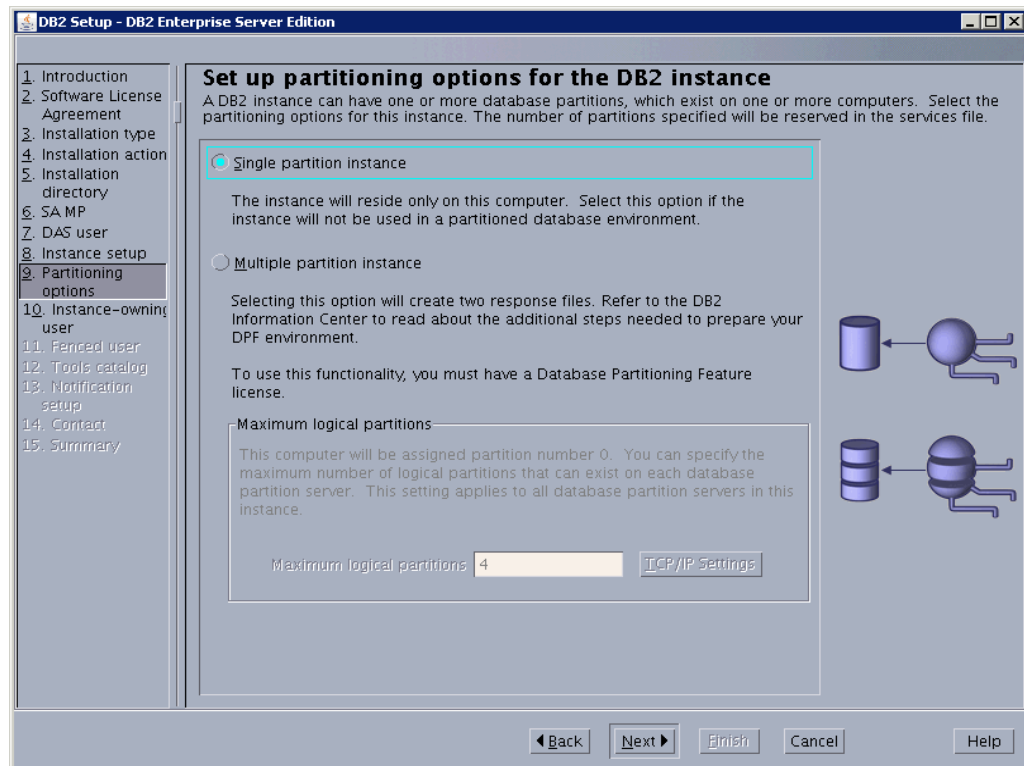
If you would like to add this computer to an existing partitioned database environment, you should not create an instance on this computer. The instance should be created on the instance-owning database partition server.

☒ Create a DB2 instance

☐ Do not create a DB2 instance

Back Next Finish Cancel Help

## 11. Choose **Single partition Instance**.



**DB2 Setup - DB2 Enterprise Server Edition**

**Set up partitioning options for the DB2 instance**

A DB2 instance can have one or more database partitions, which exist on one or more computers. Select the partitioning options for this instance. The number of partitions specified will be reserved in the services file.

☒ **Single partition instance**

The instance will reside only on this computer. Select this option if the instance will not be used in a partitioned database environment.

☐ **Multiple partition instance**

Selecting this option will create two response files. Refer to the DB2 Information Center to read about the additional steps needed to prepare your DPF environment.

To use this functionality, you must have a Database Partitioning Feature license.

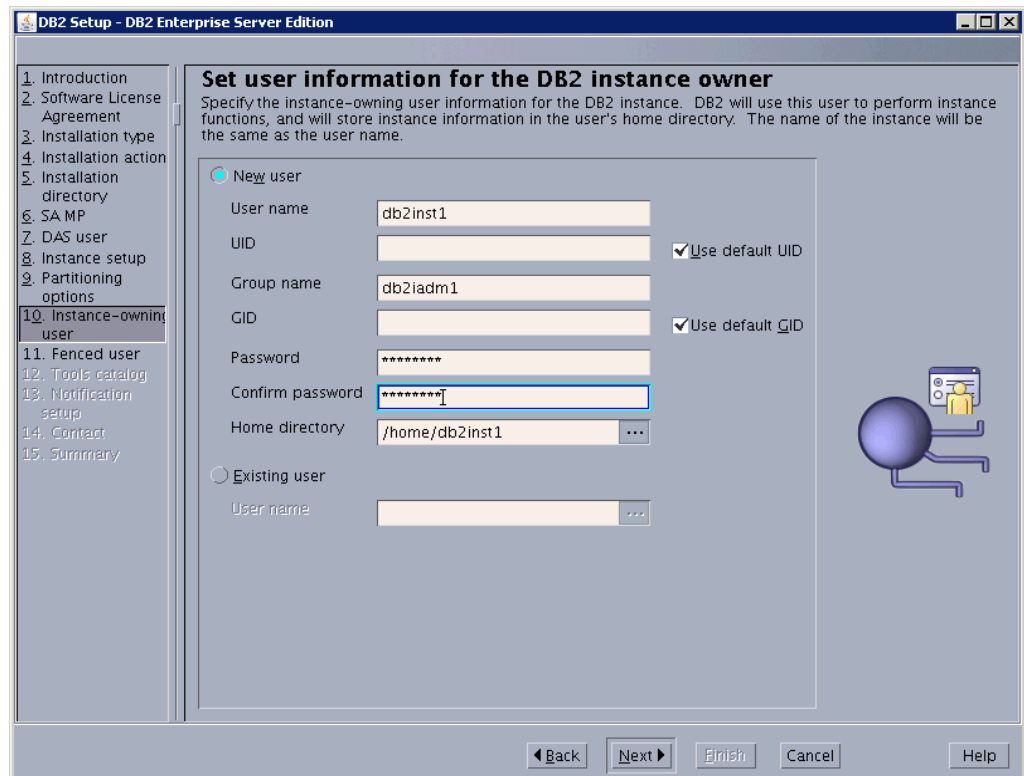
**Maximum logical partitions**

This computer will be assigned partition number 0. You can specify the maximum number of logical partitions that can exist on each database partition server. This setting applies to all database partition servers in this instance.

Maximum logical partitions:  [TCP/IP Settings](#)

Navigation buttons: [Back](#) [Next](#) [Finish](#) [Cancel](#) [Help](#)

12. The installer then asks for you to supply the user name and details for a user to run the DB2 instance. Use the form to create a new user (you must have rights to do this as the user who is running the installer), or choose an existing user.



**DB2 Setup - DB2 Enterprise Server Edition**

**Set user information for the DB2 instance owner**

Specify the instance-owning user information for the DB2 instance. DB2 will use this user to perform instance functions, and will store instance information in the user's home directory. The name of the instance will be the same as the user name.

☒ **New user**

User name:

UID:  ☒ Use default UID

Group name:

GID:  ☒ Use default GID

Password:

Confirm password:

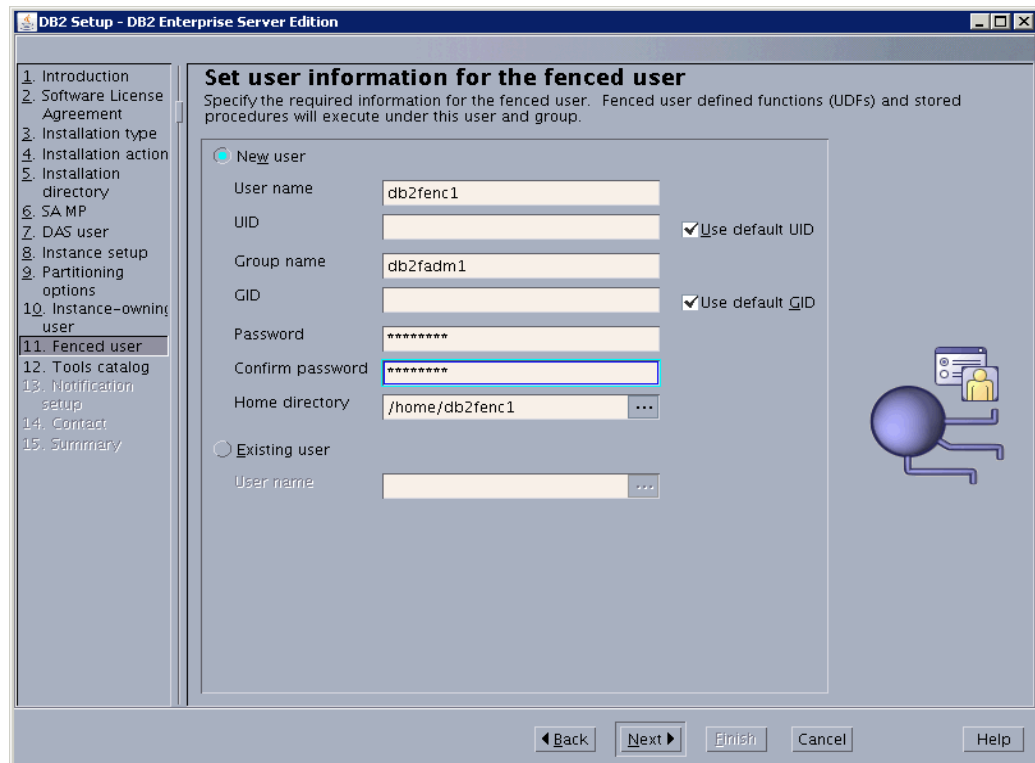
Home directory:  [...](#)

☐ **Existing user**

User name:  [...](#)

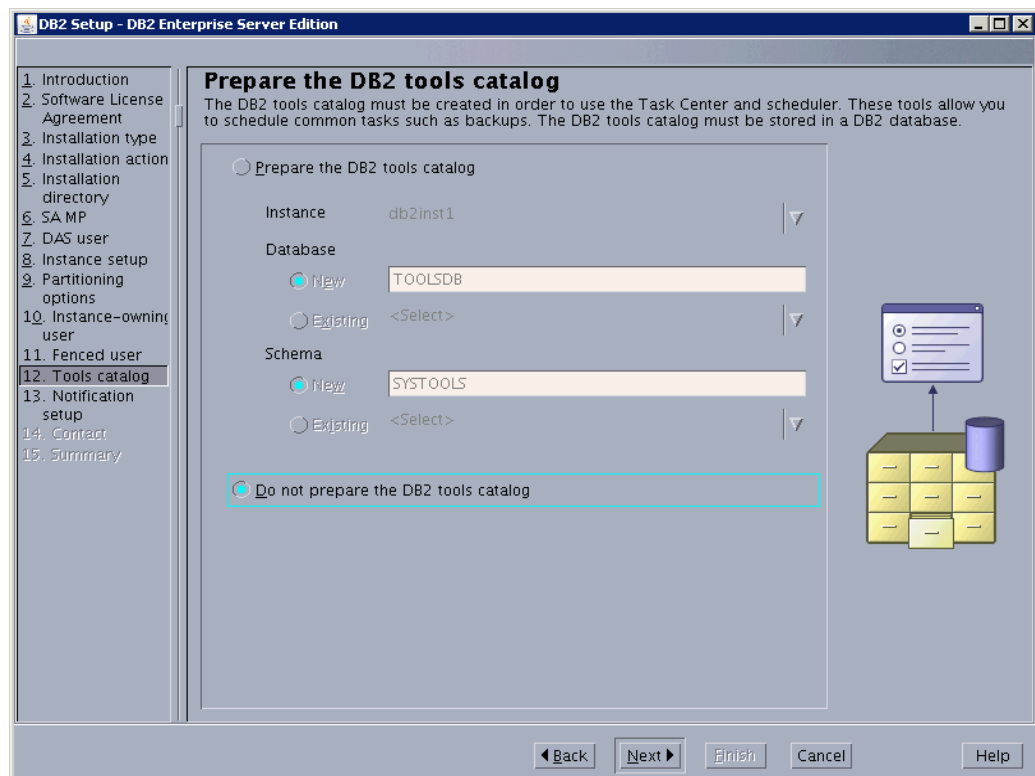
Navigation buttons: [Back](#) [Next](#) [Finish](#) [Cancel](#) [Help](#)

13. Supply the name of the Fenced User, which is a special account used to run stored procedures and other functions.



The screenshot shows the 'Set user information for the fenced user' window in the DB2 Setup - DB2 Enterprise Server Edition. The left sidebar lists steps 1 through 15, with '11. Fenced user' selected. The main area has a title bar and a description: 'Specify the required information for the fenced user. Fenced user defined functions (UDFs) and stored procedures will execute under this user and group.' There are two radio buttons: 'New user' (selected) and 'Existing user'. Under 'New user', there are fields for 'User name' (db2fenc1), 'UID' (empty), 'Group name' (db2fadm1), 'GID' (empty), 'Password' (masked with asterisks), 'Confirm password' (masked with asterisks), and 'Home directory' (/home/db2fenc1). There are checkboxes for 'Use default UID' and 'Use default GID', both of which are checked. Under 'Existing user', there is a 'User name' field. At the bottom, there are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

14. For the Tools Catalog. We chose not to prepare the Tools catalog at install time, but this can be done later.



The screenshot shows the 'Prepare the DB2 tools catalog' window in the DB2 Setup - DB2 Enterprise Server Edition. The left sidebar lists steps 1 through 15, with '12. Tools catalog' selected. The main area has a title bar and a description: 'The DB2 tools catalog must be created in order to use the Task Center and scheduler. These tools allow you to schedule common tasks such as backups. The DB2 tools catalog must be stored in a DB2 database.' There are two radio buttons: 'Prepare the DB2 tools catalog' and 'Do not prepare the DB2 tools catalog' (selected). Under 'Prepare the DB2 tools catalog', there are fields for 'Instance' (db2inst1), 'Database' (TOOLSDB), and 'Schema' (SYSTOOLS). There are also 'New' and 'Existing' radio buttons for each of these fields. At the bottom, there are buttons for 'Back', 'Next', 'Finish', 'Cancel', and 'Help'.

15. If you want to receive email notifications from the server, such as maintenance requirements or errors, setup the SMTP server details here.

The screenshot shows the 'Set up notifications' window in the DB2 Setup - DB2 Enterprise Server Edition. The left sidebar lists the installation steps, with '13. Notification setup' selected. The main area has the title 'Set up notifications' and a description: 'You can set up your DB2 server to automatically send e-mail or pager notifications to alert administrators when a database needs attention. The contact information is stored in the administration contact list. You need an unauthenticated SMTP server to send these notifications.'

There are three radio buttons for the first section:

- ☒ Set up your DB2 server to send notifications
- ☐ Do not set up your DB2 server to send notifications at this time

Below the first radio button, there is a text field for 'Notification SMTP server' containing 'smtp.itso.ibm.com'. Below that, there is a section for 'Administration contact list location' with two radio buttons:

- ☒ Local - Create a contact list on this computer
- ☐ Remote - Use an existing contact list that resides on another DB2 server

Below the 'Remote' radio button is a text field for 'Remote DB2 server'. Below the second radio button is a paragraph: 'If you do not set up your DB2 server to send notifications, the health alerts are still recorded in the administration notification log.'

On the right side, there is an illustration of a database server and a contact list.

16. Specify the user who will receive the notifications.

The screenshot shows the 'Specify a contact for health monitor notification' window in the DB2 Setup - DB2 Enterprise Server Edition. The left sidebar lists the installation steps, with '14. Contact' selected. The main area has the title 'Specify a contact for health monitor notification' and a description: 'By default, a health monitor runs on the DB2 instance you are setting up. When a health alert is generated, e-mail or pager notifications will be sent to an administration contact who is in the administration contact list.'

There are two radio buttons for the first section:

- ☒ New contact
- ☐ Defer this task until after installation is complete

Below the 'New contact' radio button, there is a section for 'Administration contact for this instance' with two text fields:

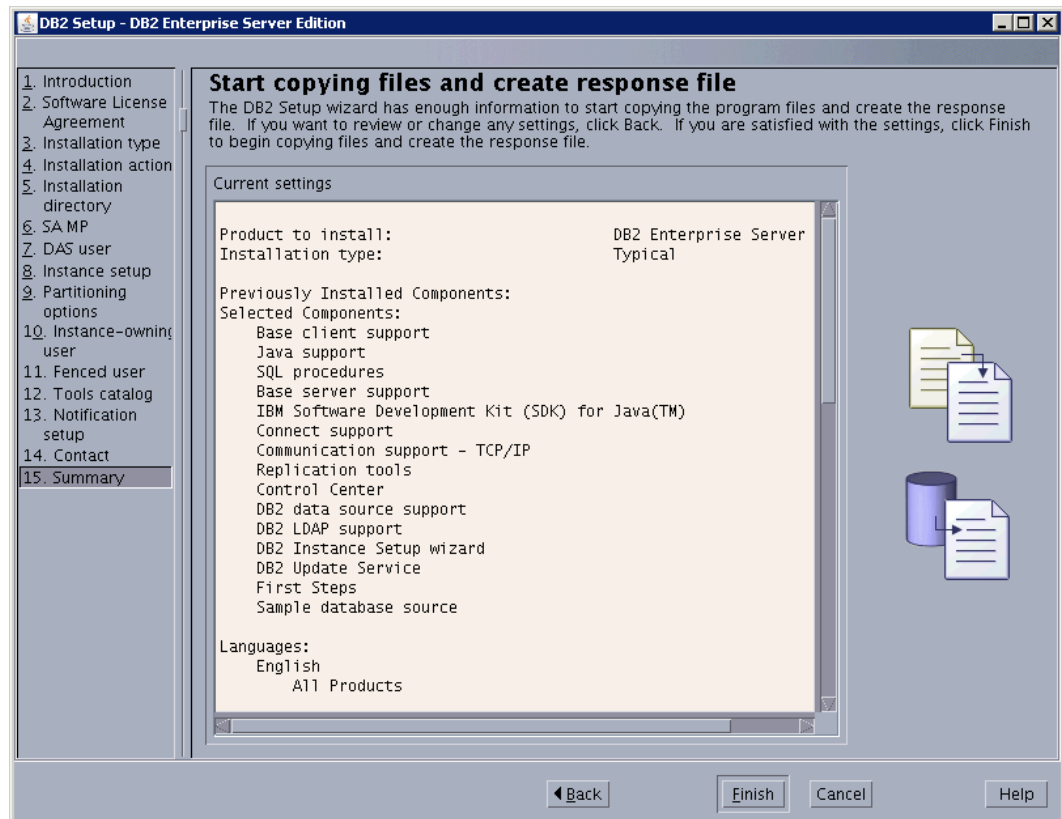
- Name: db2inst1
- E-mail address: db2inst1@itso.ibm.com

Below the 'E-mail address' field is a checkbox labeled 'E-mail address is for a pager device' which is unchecked.

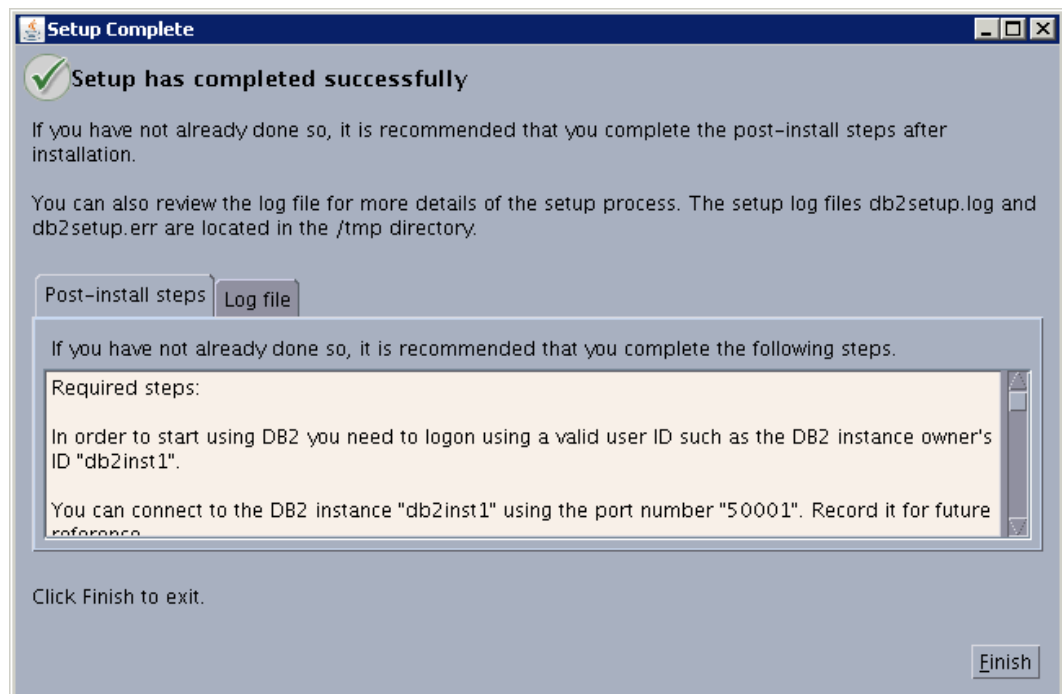
On the right side, there is an illustration of a database server and a contact list.

At the bottom of the window, there are buttons: Back, Next, Finish, Cancel, and Help.

17. Review the settings you select in the Summary screen and click **Finish** to start installation.



18. When the installation finishes, you should see a successful window as shown below. Take special note of the Post-Install Steps and click **Finish**.



## 6.3 Installing Tivoli Directory Integrator

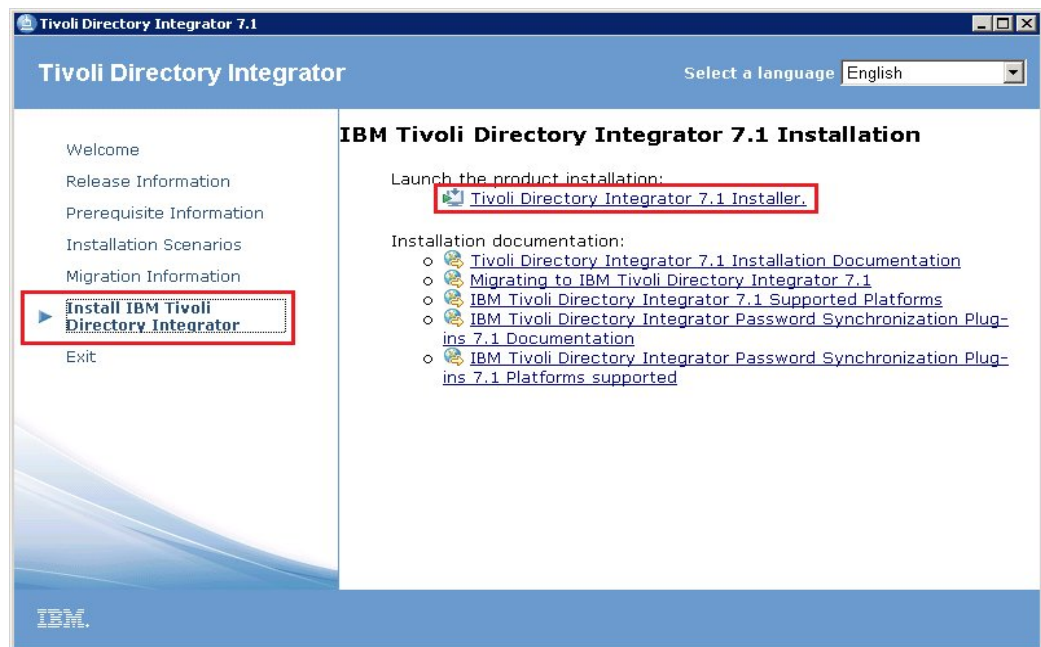
In this section, we explain how to install Tivoli Directory Integrator 7.1 and apply Fix Pack.

### 6.3.1 Installing Tivoli Directory Integrator

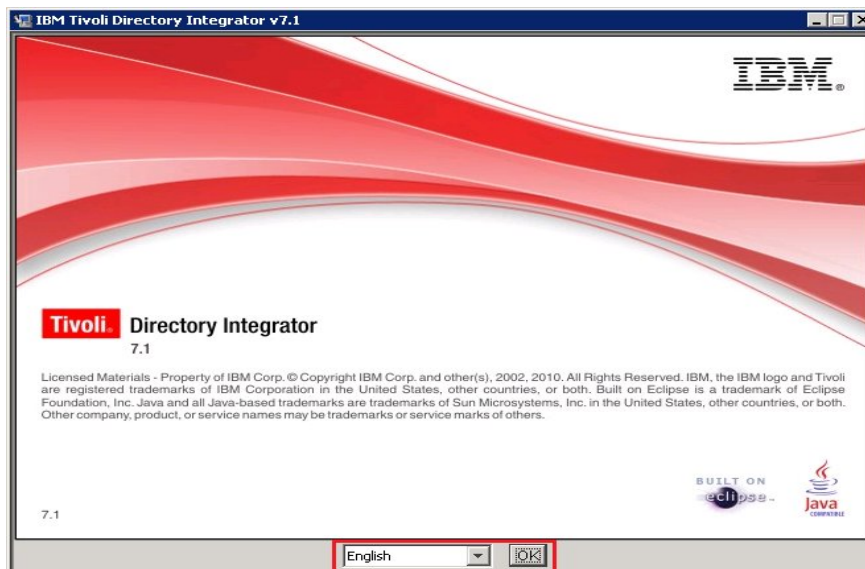
Follow these steps to install Tivoli Directory Integrator 7.1:

1. Unzip the Tivoli Directory Integrator 7.1 for Windows (CZ9MKML) in a temporary directory (c:\temp), and start the **launchpad.bat** to launch the welcome screen.

Click **Install IBM Tivoli Directory Integrator** and click **Tivoli Directory integrator 7.1 Installer**.

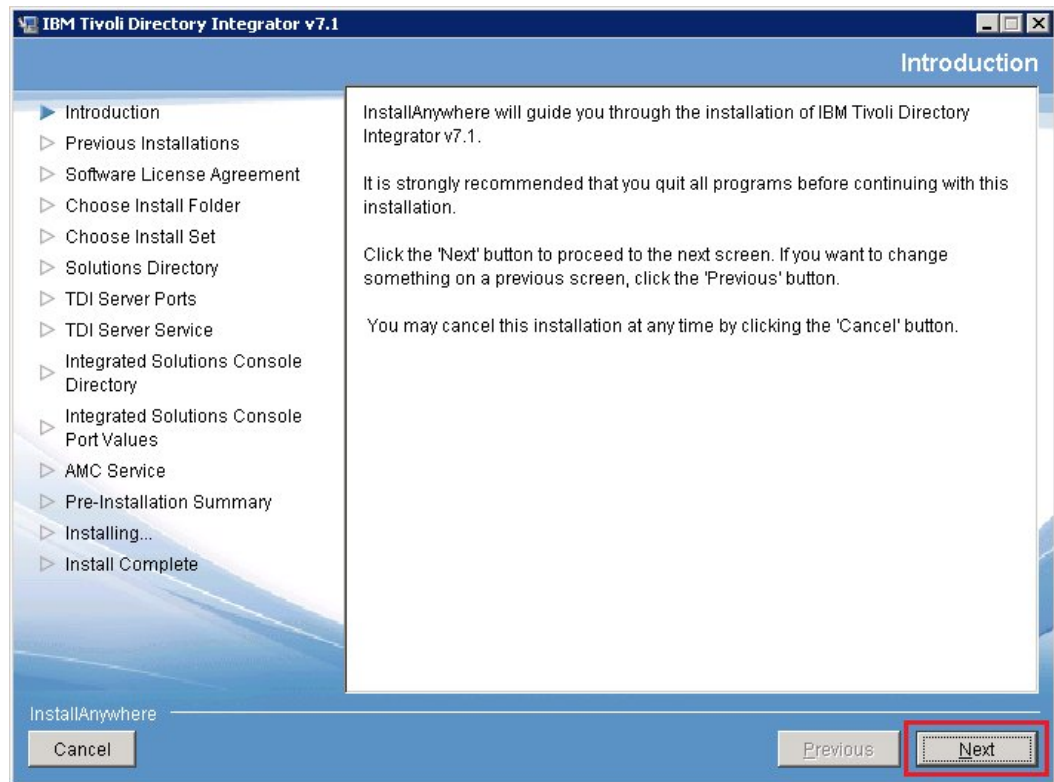


2. Select your Language.

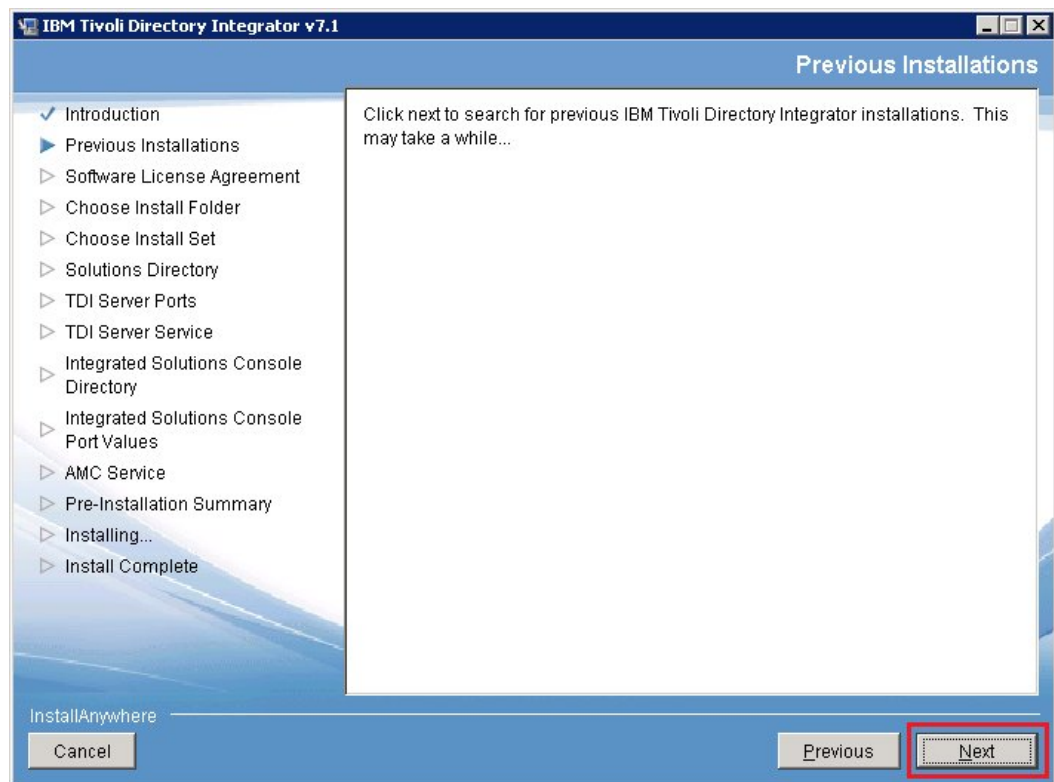




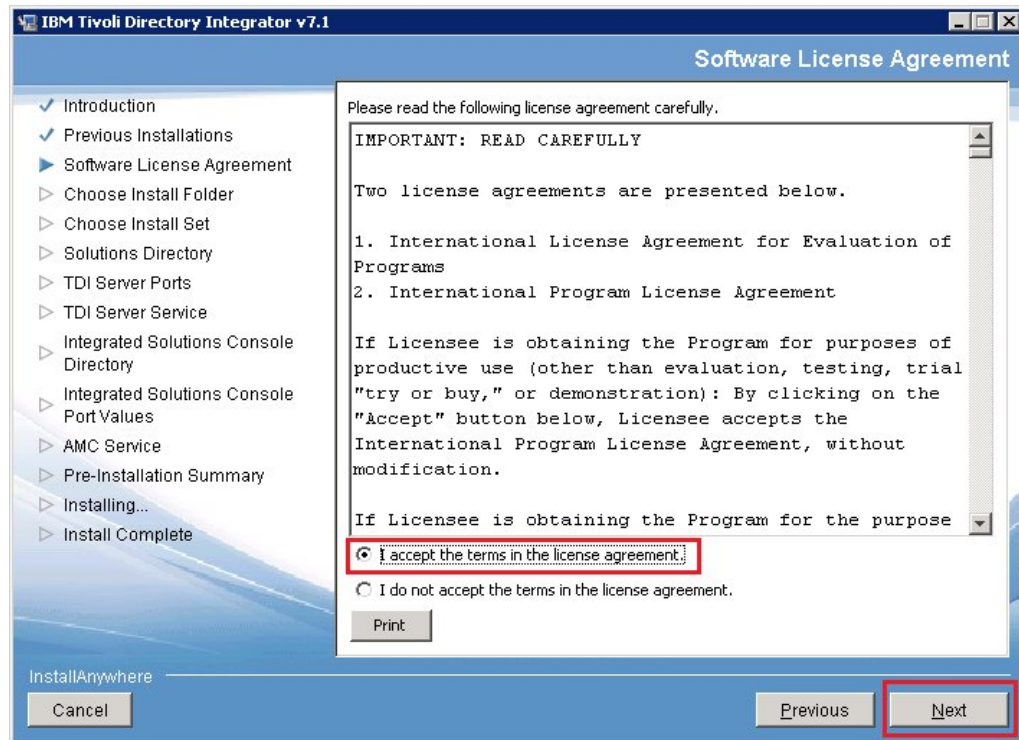
3. In the Introduction page, click **Next**.



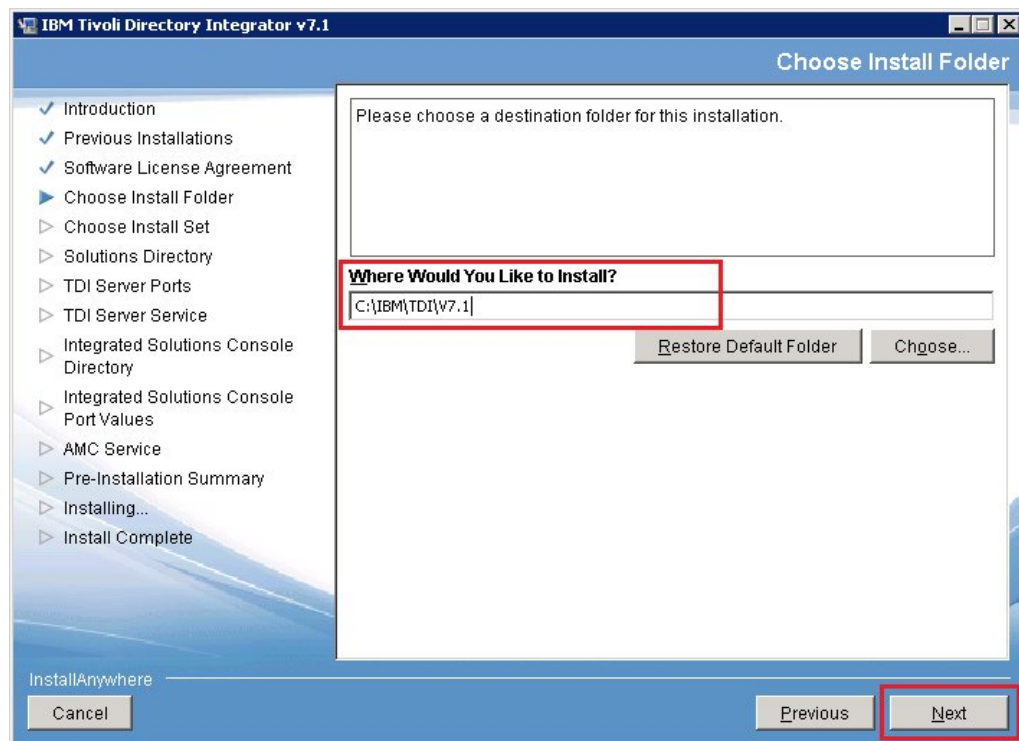
4. In the Previous Installations page, click on **Next**.



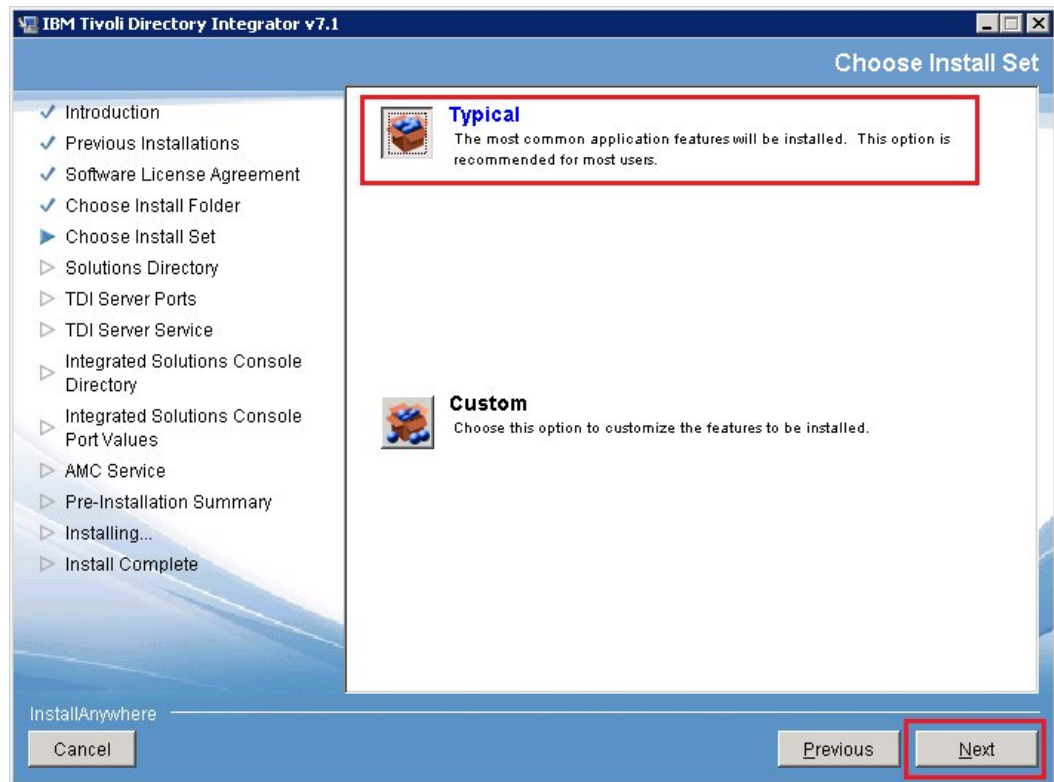
5. In the Software License Agreement page, click "**I accept the terms in the license agreement**" and click **Next**.



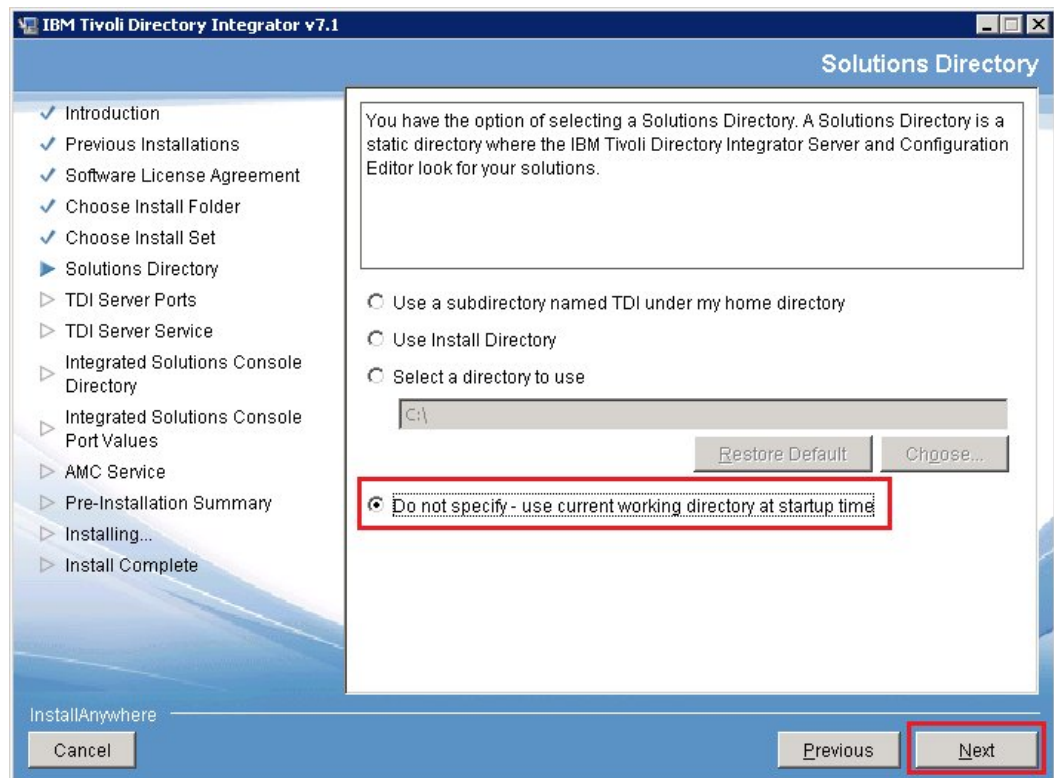
6. In the **Choose Install Folder** page. Specify an Installation directory and click on **Next**. We recommend keeping the path name short and using 8 character folder names. Common practice on Windows is to place the installation in a folder such as IBM, not Program Files (x86) to avoid the spaces and longer folder names.



7. In the **Choose Install Set** page, Select **Typical** and click **Next**.



8. In the Solutions Directory page, Select **Do not specify – use current working directory at startup time** and click **Next**.



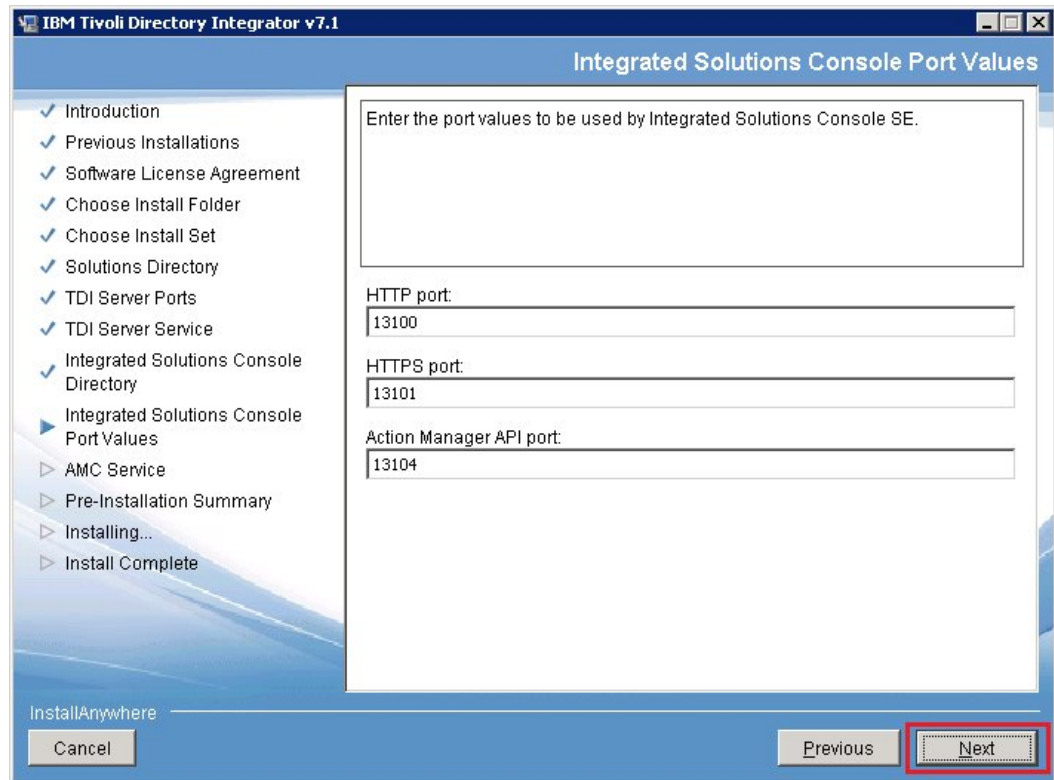
9. In the TDI Server Ports page. Accept the default values and click on **Next**.

The screenshot shows the 'Server Port Values' dialog box in the IBM Tivoli Directory Integrator v7.1 installer. The left sidebar contains a list of installation steps, with 'TDI Server Ports' highlighted. The main area contains four text input fields with the following labels and values: 'Server Port' (1099), 'System Store Port' (1527), 'REST API Port' (1098), and 'System Queue Port' (41001). At the bottom right, the 'Next' button is highlighted with a red rectangle.

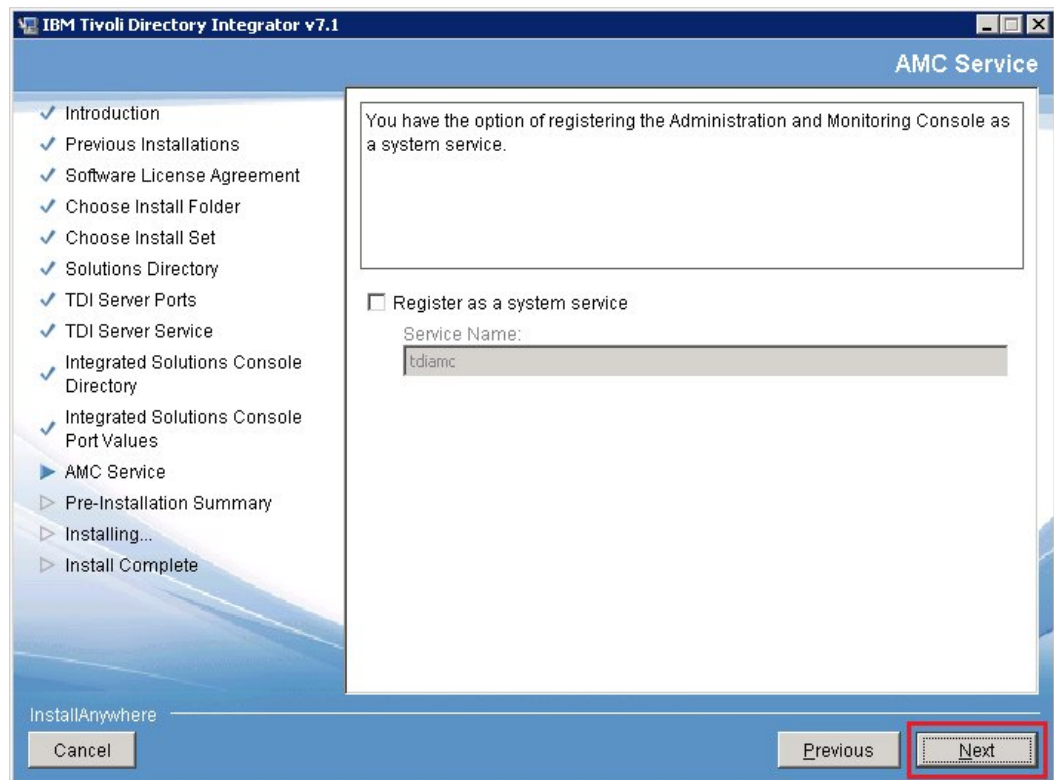
10. In the TDI Server Service page. Accept the default values and click **Next**.

The screenshot shows the 'Register Server as Service' dialog box in the IBM Tivoli Directory Integrator v7.1 installer. The left sidebar contains a list of installation steps, with 'TDI Server Service' highlighted. The main area contains a checkbox labeled 'Register as a system service' which is checked. Below it, the 'Service Name' field contains the text 'tdisrv'. At the bottom right, the 'Next' button is highlighted with a red rectangle.

11. In the Integrated Solutions Port Values page. Accept the default values and click on **Next**.

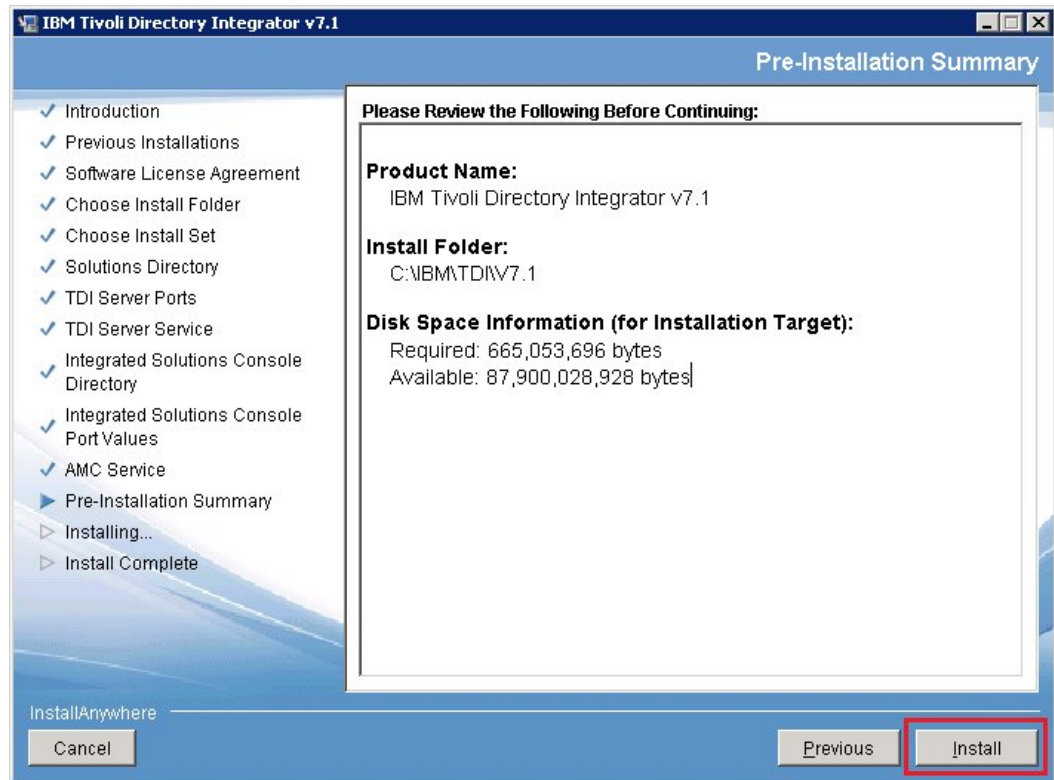


12. In the AMC Service page. Accept the default values and click **Next**.

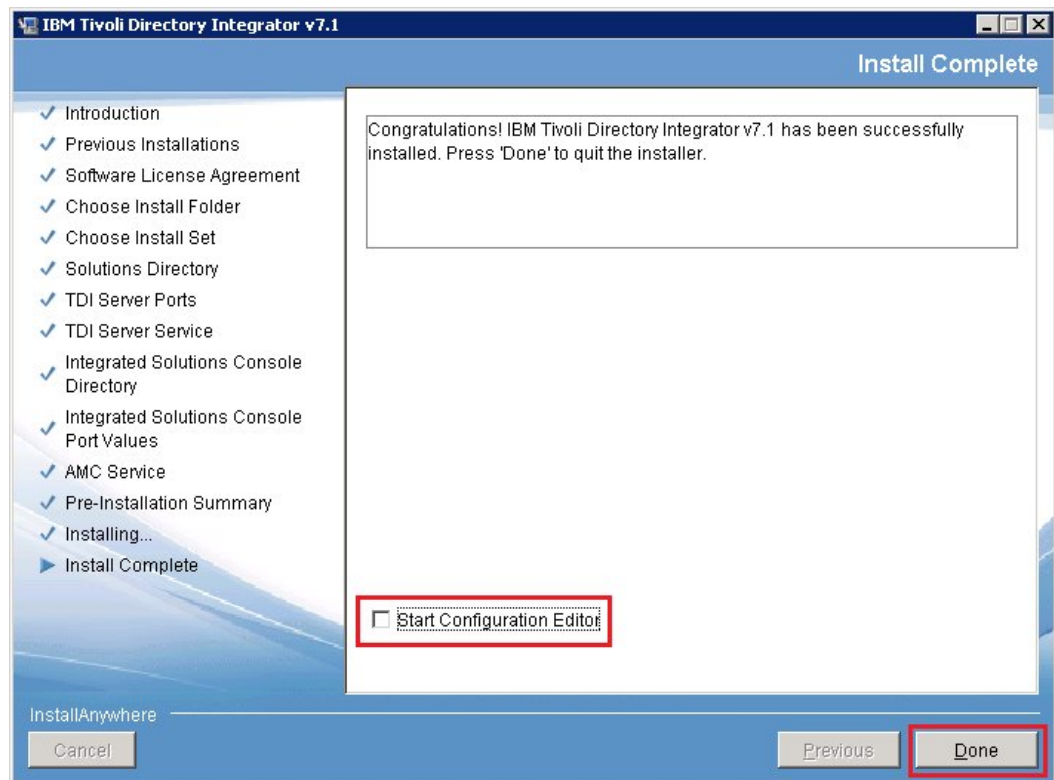


13. In the **Pre-Installation Summary** page. Review the information in the Pre-Installation Summary window and click **Install**.





14. In the Installing Complete page. Uncheck **Start the Configuration Editor** and click **Done**.



You have finished the IBM Tivoli Directory Integrator V7.1 installation.

## 6.3.2 Applying Fix Pack

After install Tivoli Directory Integrator 7.1 apply Fix Pack 6 using the following steps:

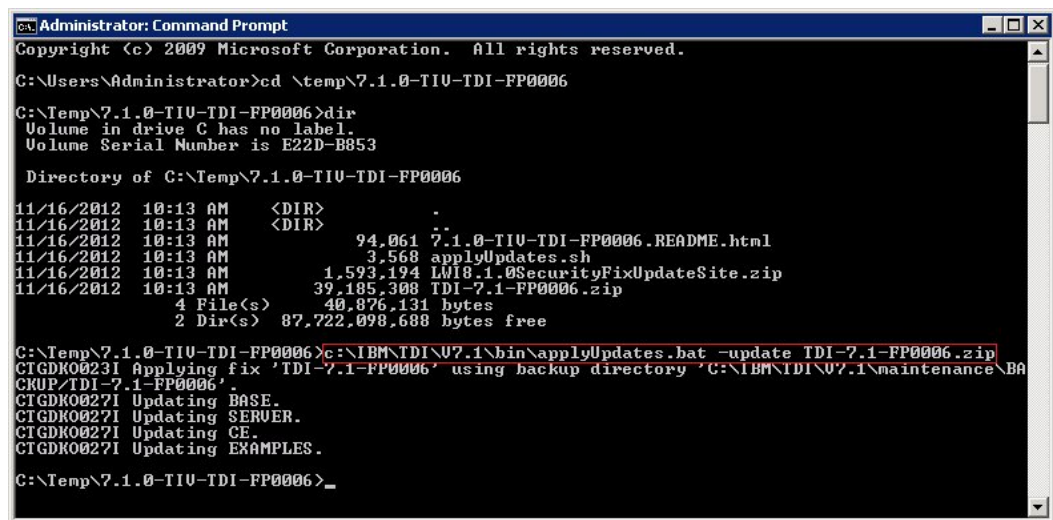
1. Download Fix Pack (**7.1.0-TIV-TDI-FP0006.zip**) from IBM Support Portal - Fix Central (<http://www-933.ibm.com/support/fixcentral/>).
2. Unzip the Tivoli Directory Integrator 7.1 Fix Pack 6 (7.1.0-TIV-TDI-FP0006) in a temporary directory (c:\temp) and go to this directory:

```
cd \temp\7.1.0-TIV-TDI-FP0006
```

3. Run the following command:

```
c:\IBM\TDI\7.1\bin\applyUpdates.bat -update TDI-7.1-FP0006.zip
```

The following figure shows an installation output:



```
Administrator: Command Prompt
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\Administrator>cd \temp\7.1.0-TIV-TDI-FP0006
C:\Temp\7.1.0-TIV-TDI-FP0006>dir
Volume in drive C has no label.
Volume Serial Number is E22D-B853

Directory of C:\Temp\7.1.0-TIV-TDI-FP0006

11/16/2012  10:13 AM    <DIR>          .
11/16/2012  10:13 AM    <DIR>          ..
11/16/2012  10:13 AM                94,061  7.1.0-TIV-TDI-FP0006.README.html
11/16/2012  10:13 AM                3,568  applyUpdates.sh
11/16/2012  10:13 AM            1,593,194  LM18.1.0SecurityFixUpdateSite.zip
11/16/2012  10:13 AM       39,185,308  TDI-7.1-FP0006.zip
               4 File(s)              40,876,131 bytes
               2 Dir(s)              87,722,098,688 bytes free

C:\Temp\7.1.0-TIV-TDI-FP0006>c:\IBM\TDI\7.1\bin\applyUpdates.bat -update TDI-7.1-FP0006.zip
CTGDK0023I Applying fix 'TDI-7.1-FP0006' using backup directory 'C:\IBM\TDI\7.1\maintenance\BA
CKUP\TDI-7.1-FP0006'.
CTGDK0027I Updating BASE.
CTGDK0027I Updating SERVER.
CTGDK0027I Updating CE.
CTGDK0027I Updating EXAMPLES.
C:\Temp\7.1.0-TIV-TDI-FP0006>
```

## 6.4 Installing WebSphere Application Server

IBM Connection 4 runs as an application (it is actually a number of independent applications that are installed as one) on WebSphere Application Server. WebSphere is infrastructure software, or middleware, designed for dynamic On Demand Business and for enabling SOA for your enterprise. It delivers a proven, secure, robust, and reliable software portfolio that provides an excellent return on investment. WebSphere Application Server is the IBM runtime environment for Java-based applications. Because different e-business application scenarios require different levels of application server capabilities, WebSphere Application Server is available in multiple packaging options as follow:

- ▶ WebSphere Application Server - Express V7.0
- ▶ WebSphere Application Server V7.0
- ▶ WebSphere Application Server for Developers V7.0
- ▶ WebSphere Application Server Network Deployment V7.0
- ▶ WebSphere Application Server for z/OS V7.0

To install IBM Connections 4, you must install WebSphere Application Server Network Deployment. WebSphere Application Server Network Deployment provides full capabilities to support the complex applications including clustering, load balancing, and high availability.

In this section, we show the steps to install the servers that hosts WebSphere Application Server, configure the Deployment Manager, configure the additional nodes, install the update maintenance tool, install fix packs, and enable the console security. For more information about WebSphere Application Server Network Deployment, see WebSphere Information Center([http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.webSphere.nd.multiplatform.doc/info/ae/ae/welcome\\_ndmp.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp?topic=/com.ibm.webSphere.nd.multiplatform.doc/info/ae/ae/welcome_ndmp.html)).

The procedure to set up WebSphere Application Server systems for the IBM Connections is as follows:

1. Installing and configuring Deployment Manager

This step is to create a server for managing the WebSphere environment. In our example, we define the Deployment Manager cell and create Integrated Solutions Console (ISC) to deploy IBM Connections.

2. Installing additional nodes

These nodes are added into Deployment Manager cell to host the IBM Connections files deployed on WebSphere Application server.

3. Configuring LDAP in the Integrated Solutions Console.

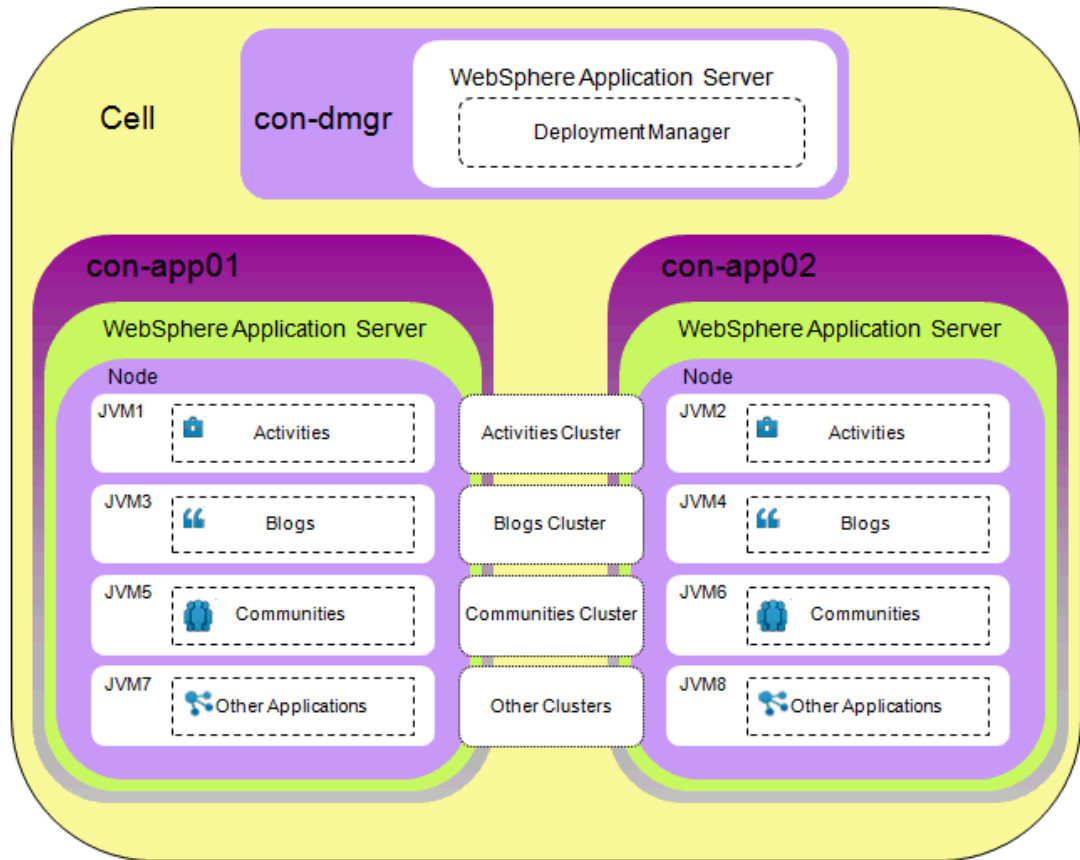
IBM Connections requires an user registry repository to authenticate users. You have to configure WebSphere to access the LDAP.

4. Configuring security on Integrated Solutions Console.

To secure the WebSphere infrastructure, you must enable the global security using ISC. After enabled the global security at ISC, all servers under the WebSphere requires authentication to access them.

The following figure shows the logical topology of the IBM Connections servers of our lab scenario. In this scenario, we have configured 3 Linux servers con-dmgr, con-app01 and con-app02. The con-dmgr is our cell (cell is responsible for manage multiple nodes), con-app01 and con-app02 are defined as a node (node is an administrative grouping of application servers for configuration and operational management). On our environment all servers are installed on Linux and WebSphere Application Server Network Deployment.





## 6.4.1 WebSphere Application Server deployment

### Installing and configuring Deployment Manager

WebSphere Application Server Network Deployment is responsible for managing the WebSphere infrastructure. Complete these steps to install and configure Network Deployment :

1. Unzip the WebSphere Application Server Network Deployment package file (C1G35ML.tar.gz) in a temporary directory (for example, /tmp).
2. To start the installer, run **launchpad.sh** (launchpad.bat for Windows) to start the installer. You can also start the installation from /tmp/WAS directory and run the **install** file.

**Note:** You might need to make the **launchpad.sh** file executable on Linux before it will run. Use **chmod** command to do this.








In the Welcome WebSphere Application Server Network Deployment window, choose the first option, **WebSphere Application Server Network Deployment**.

## Welcome to WebSphere Application Server Network Deployment

IBM WebSphere Application Server Network Deployment, Version 7.0 is an integrated platform that contains an Application Server, Web development tools, a Web server, and additional supporting software and documentation. This launchpad may serve as a single point of reference for installing your Application Server environment.

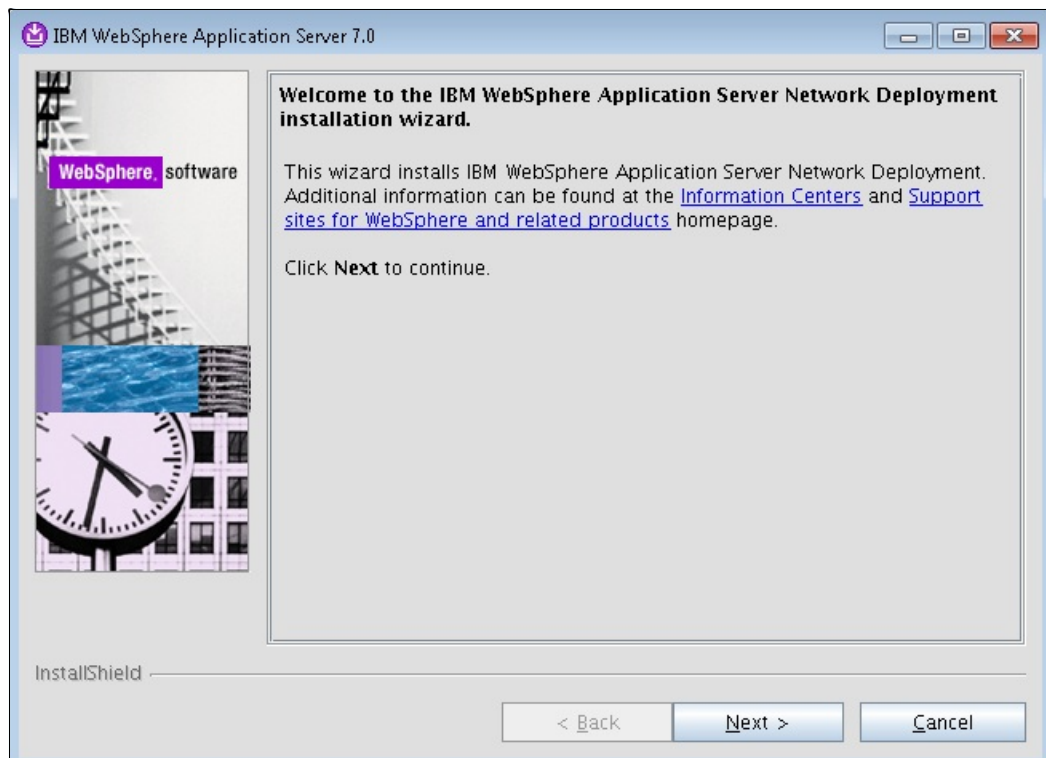
We recommend viewing the [installation diagrams](#) for illustrations of common application server environments. For full documentation visit the on-line [WebSphere Information Center](#).

**To begin**, select an entry from the list below to initialize a product installation wizard. Alternatively, select a product on the navigation list to left to read descriptions of the products, and browse help documentation and support links before starting an installation wizard.

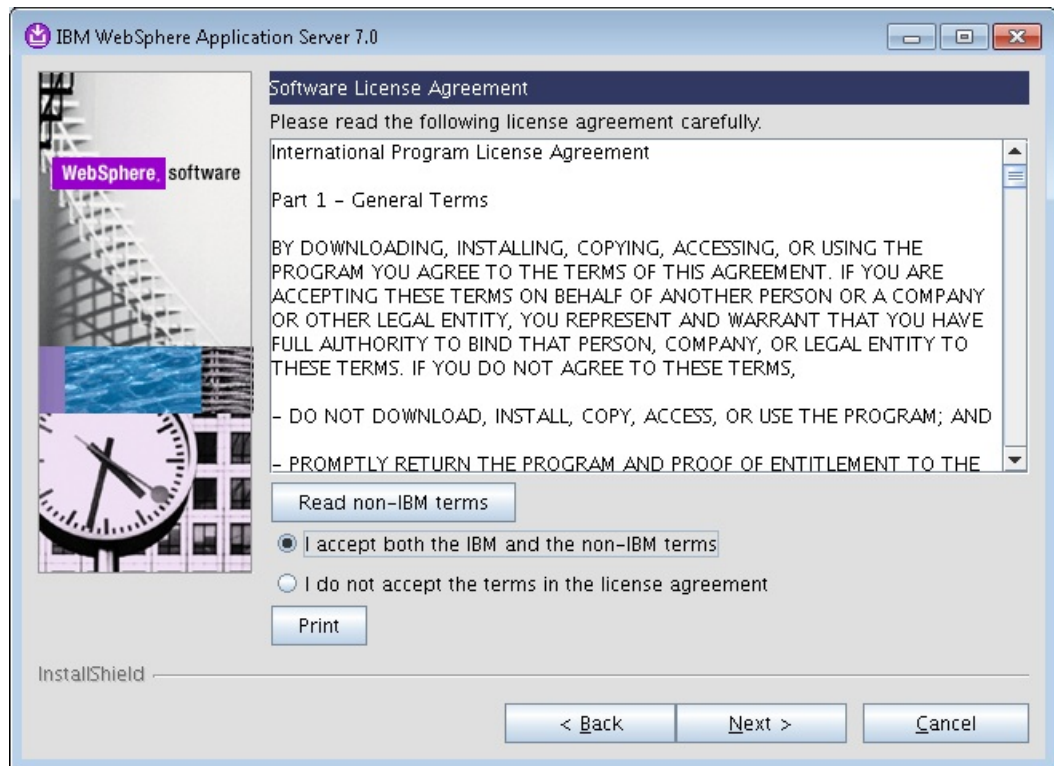
- **WebSphere Application Server Network Deployment**  
 [Launch the installation wizard for WebSphere Application Server Network Deployment.](#)
- **IBM HTTP Server**  
 [Launch the installation wizard for IBM HTTP Server.](#)
- **Web Server plug-ins**  
 [Launch the installation wizard for Web Server plug-ins.](#)
- **WebSphere DMZ Secure Proxy Server**  
 [Launch the installation wizard for DMZ Secure Proxy Server.](#)
- **IBM Update Installer for WebSphere Software**  
 [Launch the installation wizard for IBM Update Installer for WebSphere Software.](#)
- **IBM Edge Components**  
 [Launch the installation wizard for Edge Components Load Balancer for IPv6.](#)  
 [Launch the installation wizard for Edge Components Load Balancer.](#)
- **IBM Tivoli Composite Application Manager for WebSphere Application Server**  
 [Launch the installation wizard for IBM Tivoli Composite Application Manager.](#)

(C) Licensed Materials - Property of IBM Corp.  
 © Copyrights by IBM Corp. and by others 2006, 2008.  
 All Rights Reserved.  
 IBM, Rational, Tivoli, and WebSphere are trademarks of IBM Corp. in the United States, other countries, or both.  
 Other company, product, or service names may be trademarks or service marks of others.

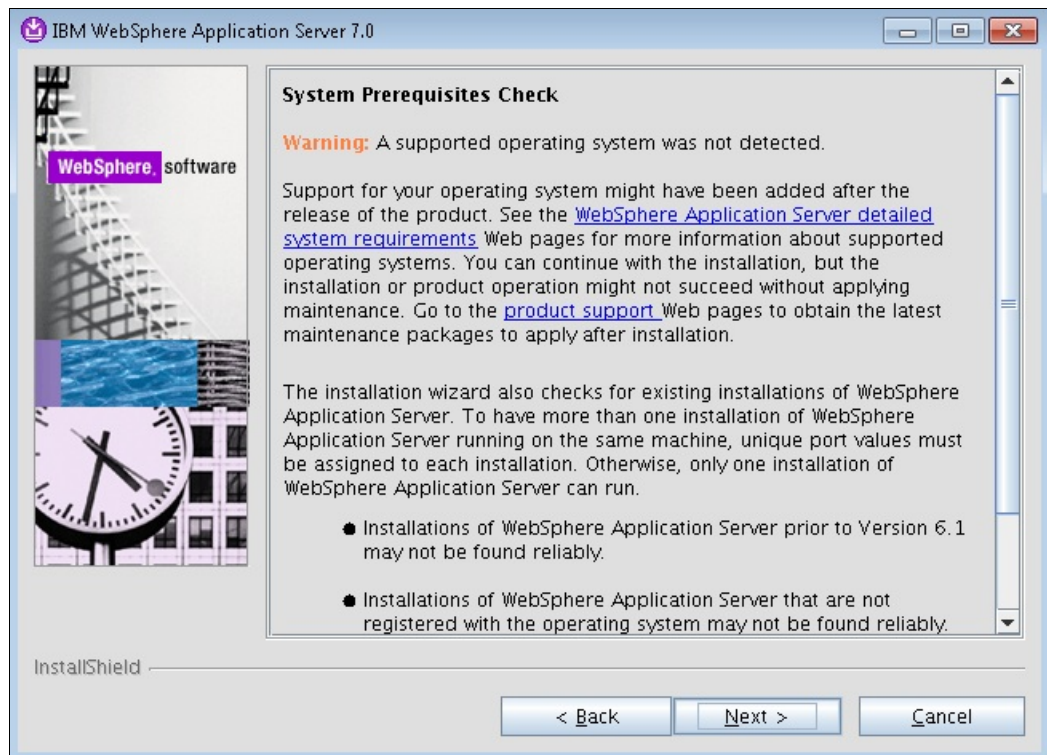
Click **Launch the installation wizard for WebSphere Application Server Network Deployment**,



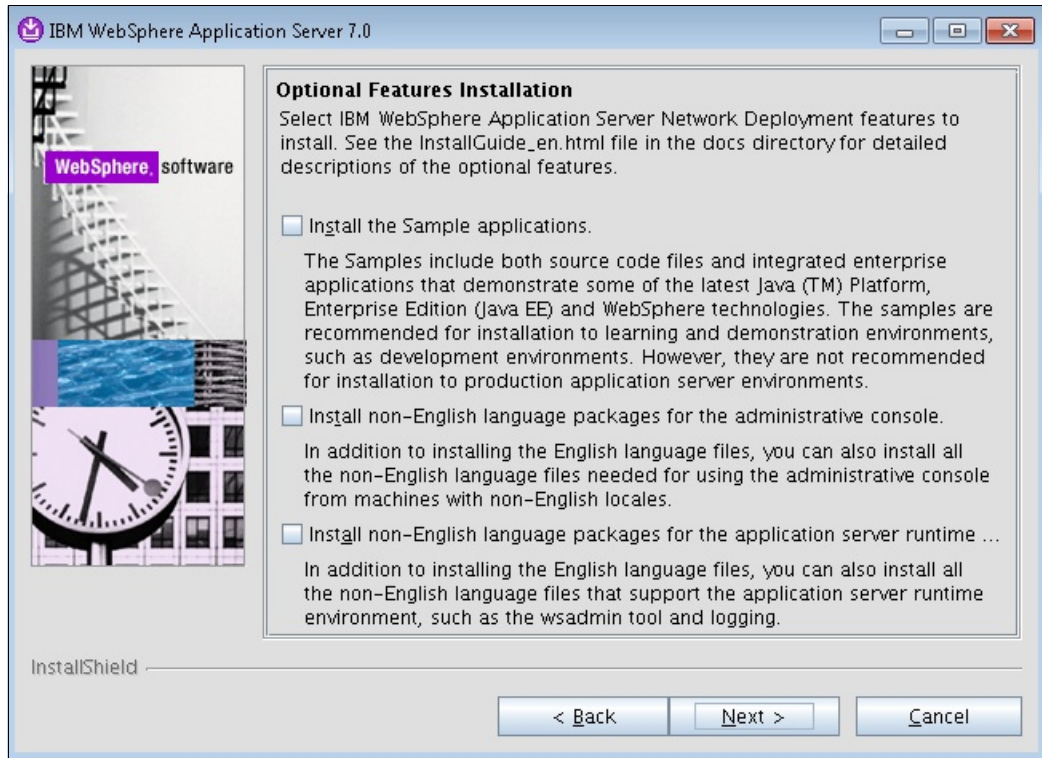
3. After you have read the Software license agreement, accept the agreement to continue.



- The installation wizard checks the prerequisites of your operating system. You might receive an warning informing that your operating system is not detected. This is because your environment might have been added after the product release, probably your environment is newer than the minimum required to install WAS ND so you can click on **Next**. To check the compatibility, see 5.1, "Verify software requirements" on page 40.



5. In the optional features to be installed on WebSphere Application Serve window, you can install the Samples to test your environment when the installation finished, add support language to administrative console and also the support language runtime environment, can be added. For our installation, we do not need any optional features.

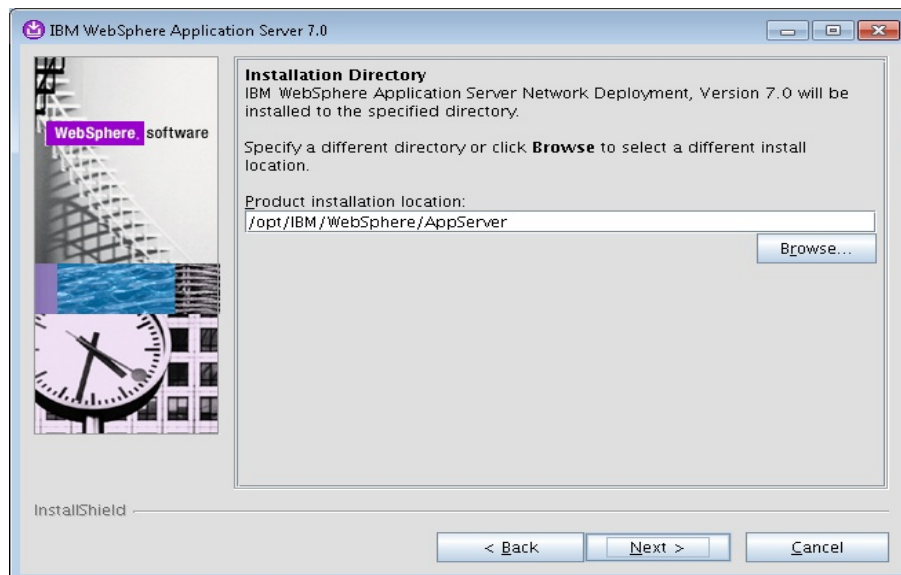


6. The installation wizard allows you to choose the directory to install your WebSphere Application Server. By default, the installation directory is as follows:

Linux: **/opt/IBM/WebSphere/AppServer**

AIX: **/usr/IBM/WebSphere/AppServer**

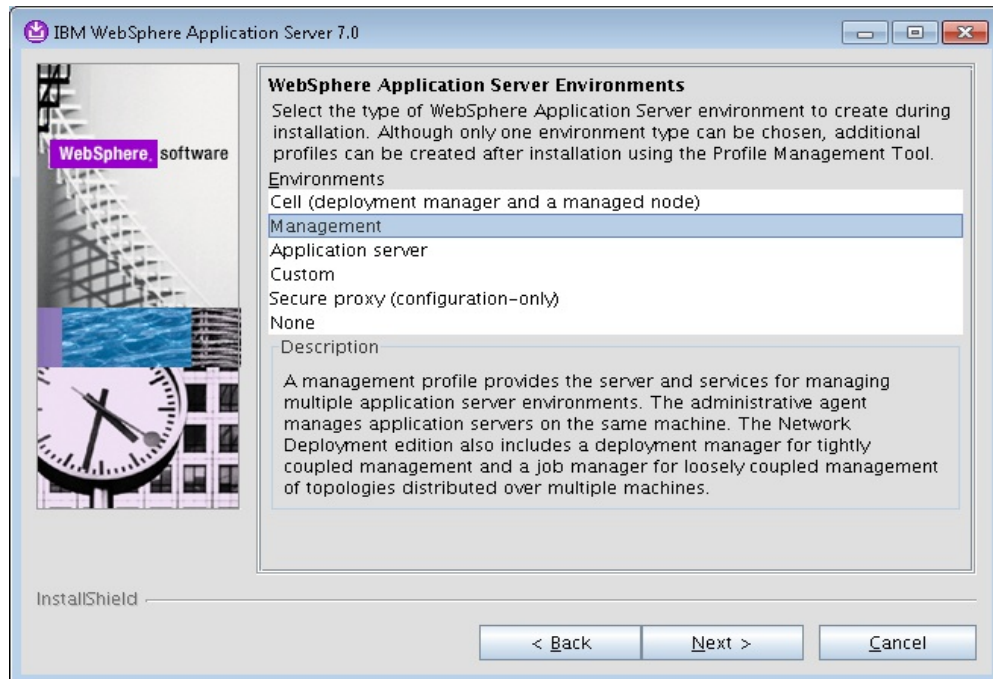
Windows: **:\IBM\WebSphere\AppServer**



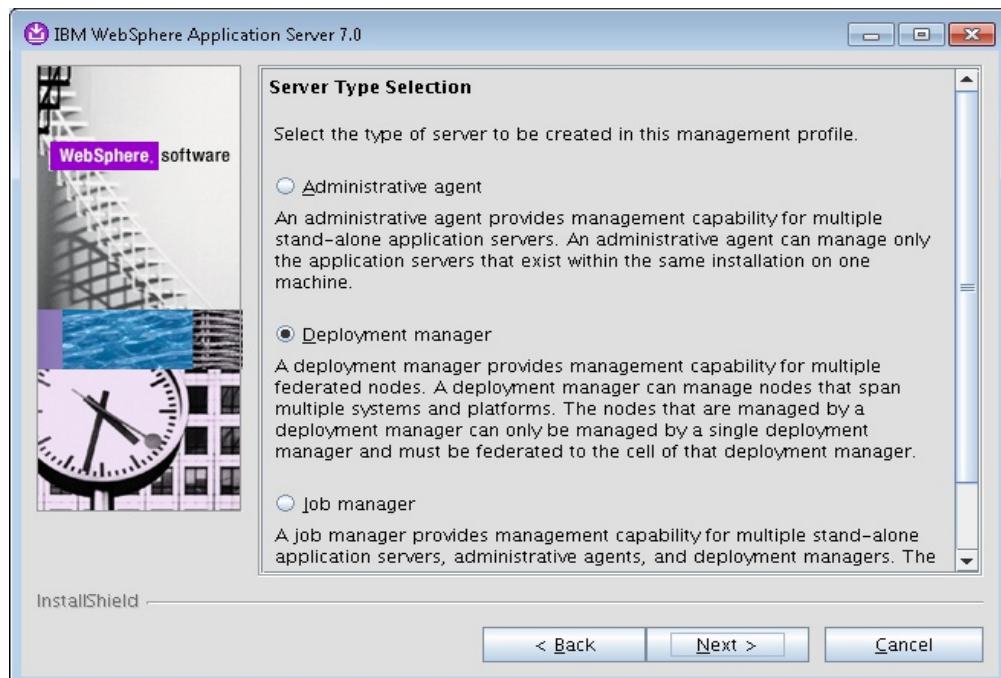


7. Choose the profile to be installed. For the Deployment Manager, select **Management** as the profile.

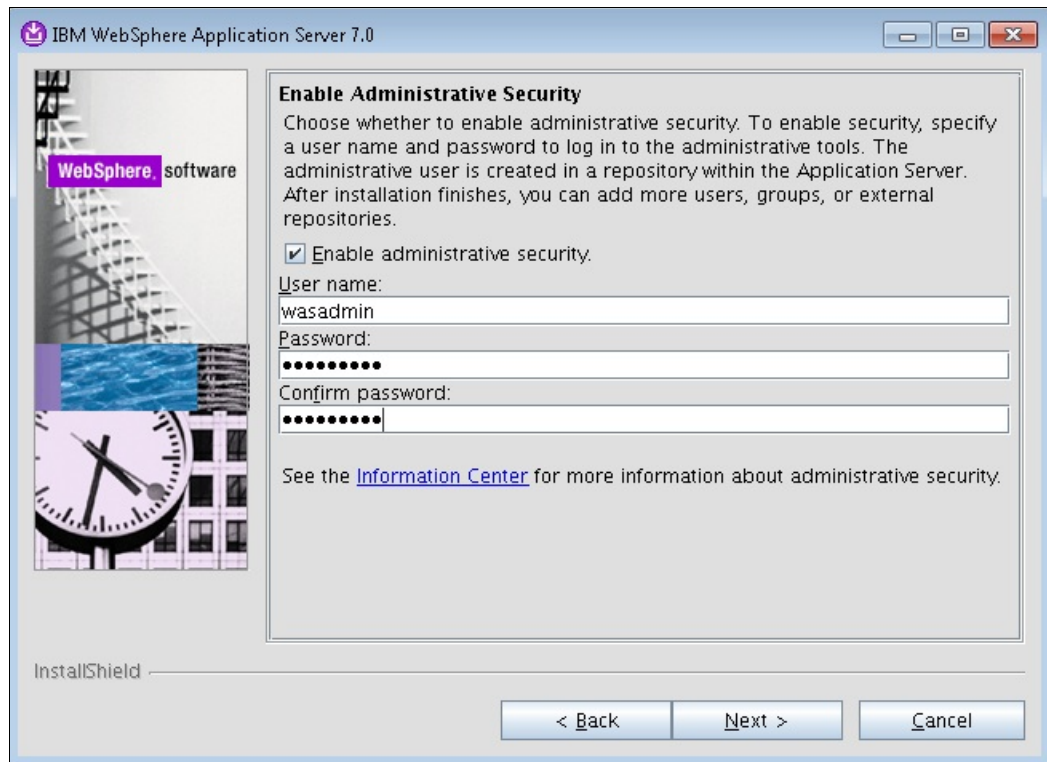
**Note:** For more information about profile, see WebSphere Application Server V7.0: Concepts, Planning and Design Redbook  
<http://www.redbooks.ibm.com/redbooks/pdfs/sg247708.pdf>



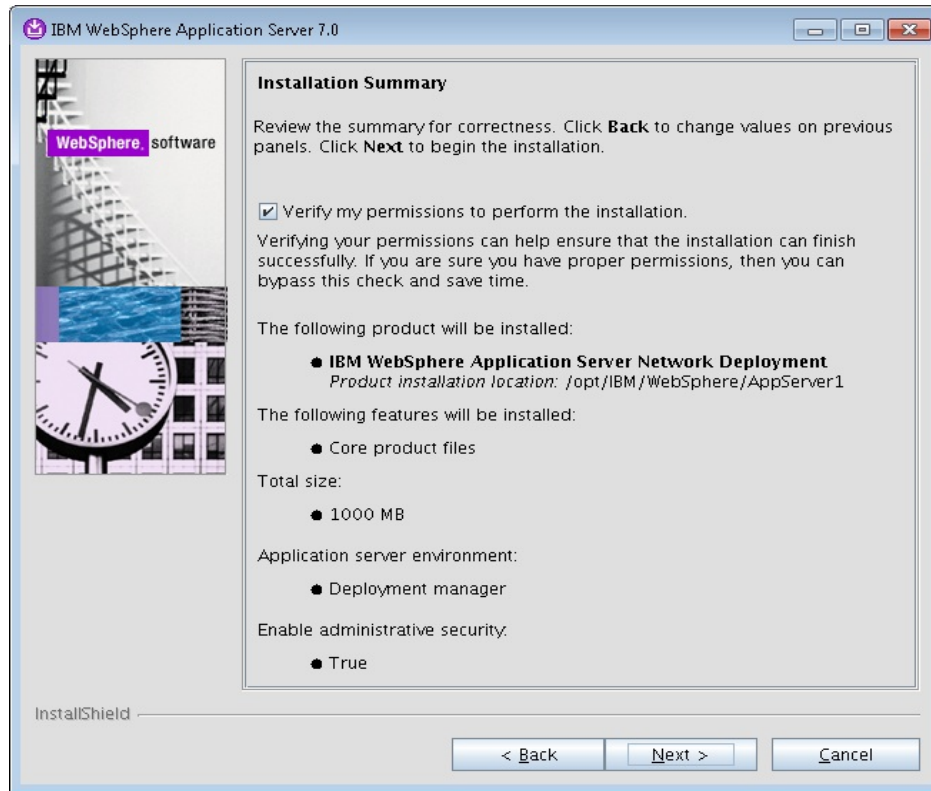
8. Select **Deployment manager** as the server type for allowing managing multiple federated nodes.



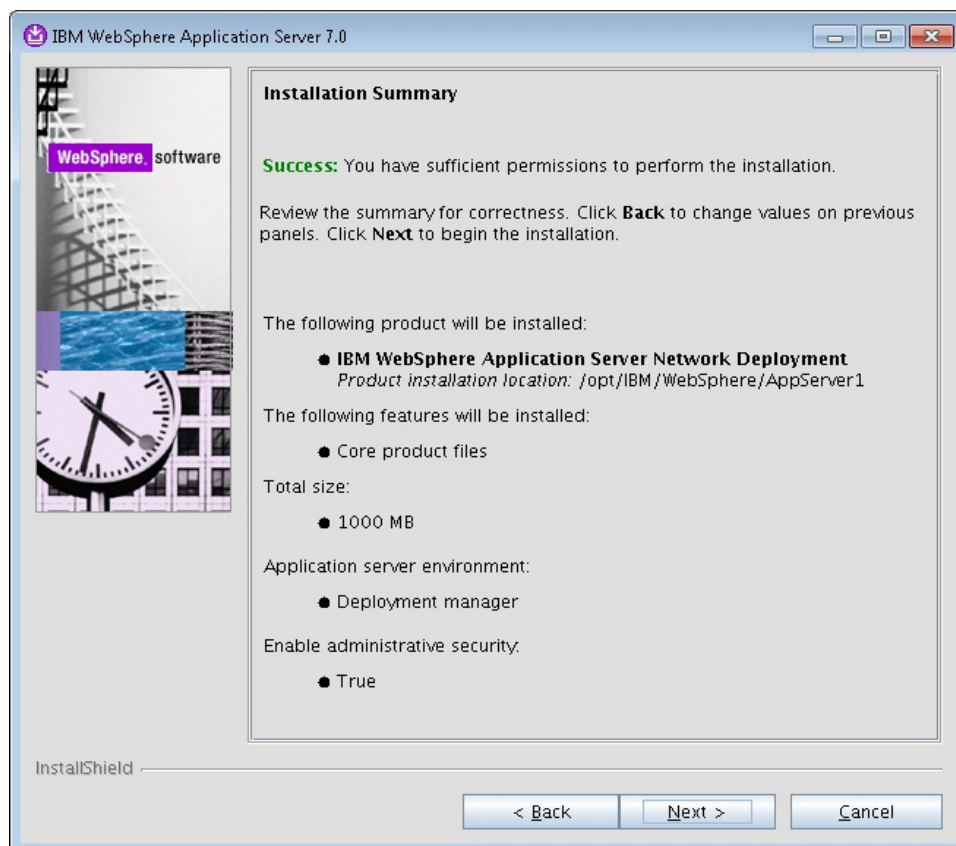
9. To have the installation wizard configure the secure administrative console during the installation, mark **Enable administrative security** and provide an **user name** and **password**., This user name must not exist on LDAP repository., for example **wasadmin**.



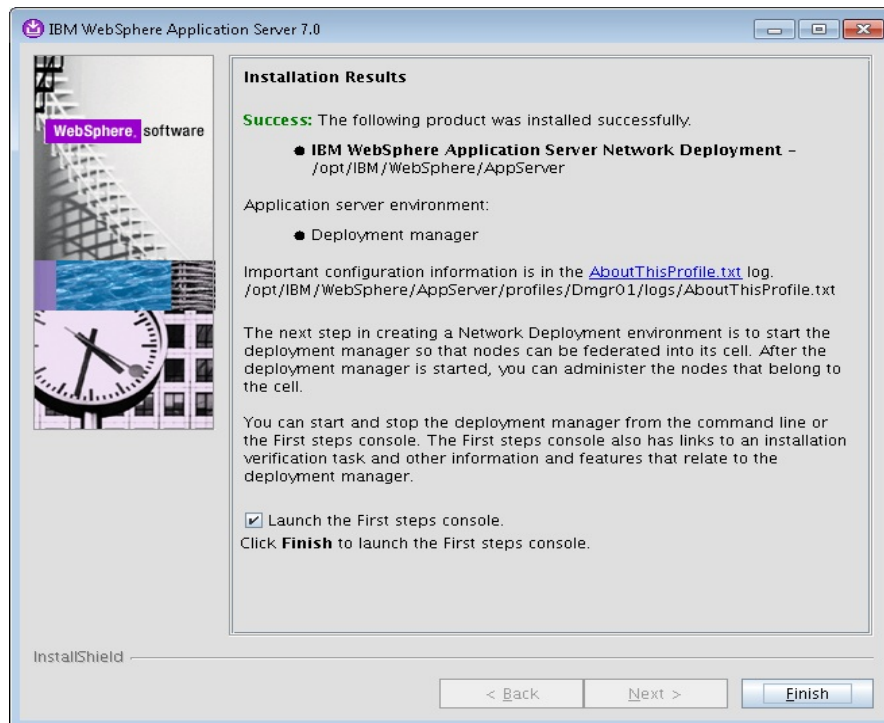
10. The Centralized Installation Manager (CIM) creates a repository with the installation contents that allows you to install and uninstall WebSphere Application Server binaries and maintenance patches from a centralized location. Do not check centralized repository installation.
11. After we have defined all the installation parameters, the installation wizard provides a summary. Click **Verify my permissions to perform the installation** to have the installation wizard check permission before performs the installation.



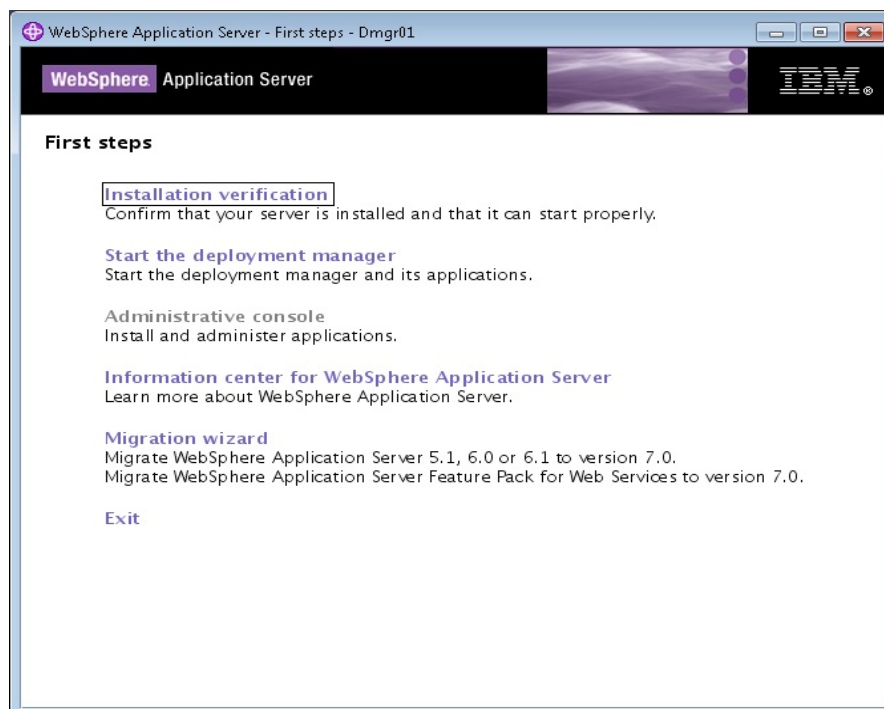
12. If there are no permission issues, the wizard returns success as the validation result. Click **Next** to start the installation process.



13. The installation wizard provides the success result at the end of the installation. For the installation log, see *AboutThisProfile.txt* on `/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/AboutThisProfile.txt`.

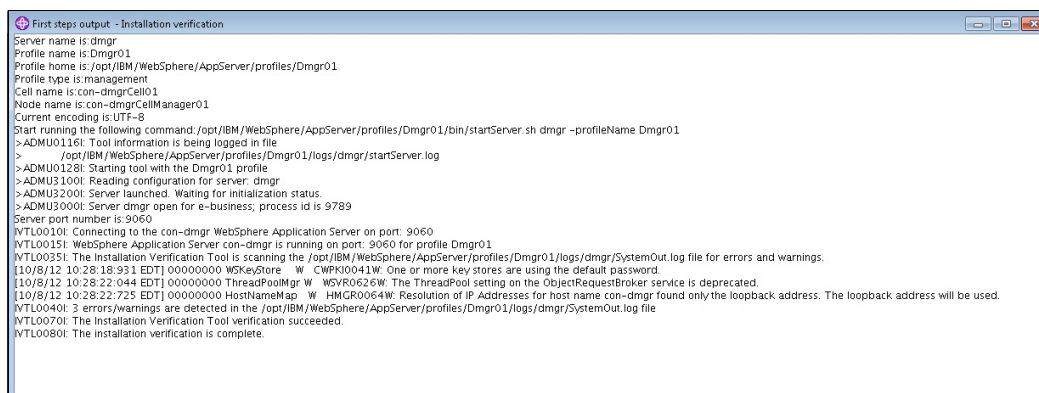


14. When the installation completes the installer shows the First Steps wizard. This allows you to perform a number of post-install operations, including **Installation Verification**. We recommend running the installation verification process to ensure that the WAS installation is healthy.





15. The installation verification: Checks if your Deployment Manager is able to start and run a validation.



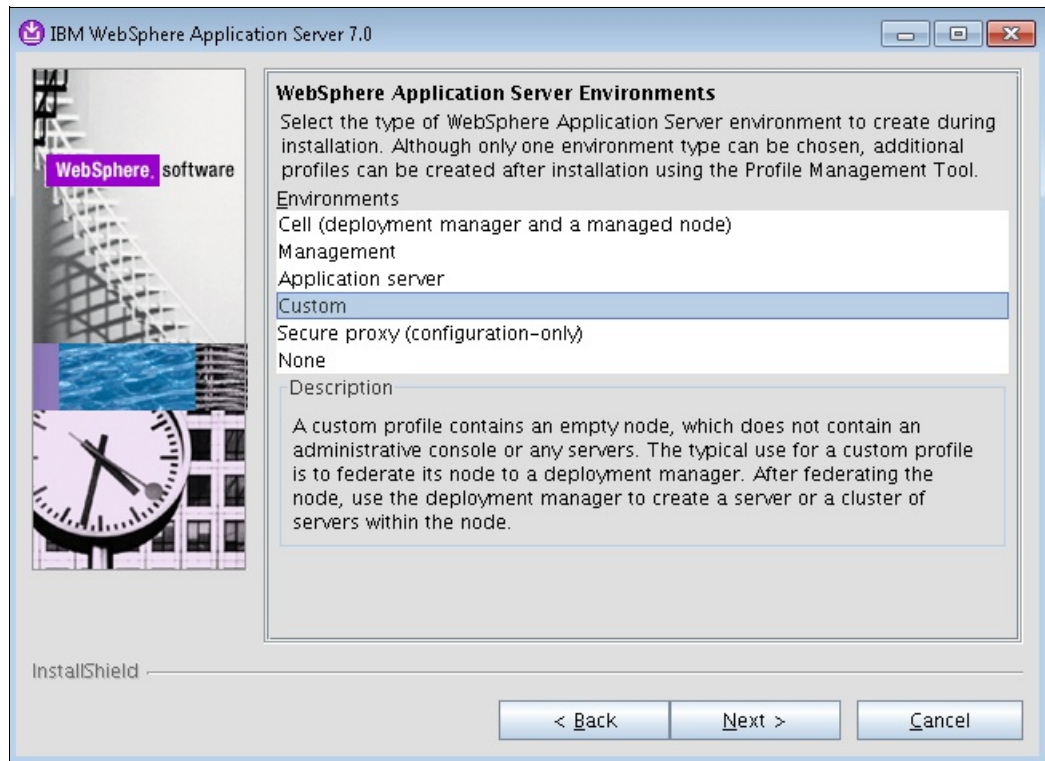
```
First steps output - Installation verification
Server name is: dmgr
Profile name is: Dmgr01
Profile home is: /opt/IBM/WebSphere/AppServer/profiles/Dmgr01
Profile type is: management
Cell name is: con-dmgrCell01
Node name is: con-dmgrCellManager01
Current encoding is UTF-8
Start running the following command: /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin/startServer.sh dmgr -profileName Dmgr01
> ADMU0116I: Tool information is being logged in file
> /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/dmgr/startServer.log
> ADMU0128I: Starting tool with the Dmgr01 profile
> ADMU3100I: Reading configuration for server: dmgr
> ADMU3200I: Server launched. Waiting for initialization status.
> ADMU3000I: Server dmgr open for e-business; process id is 9789
Server port number is: 9060
VTLO010I: Connecting to the con-dmgr WebSphere Application Server on port: 9060
VTLO015I: WebSphere Application Server con-dmgr is running on port: 9060 for profile Dmgr01
VTLO035I: The Installation Verification Tool is scanning the /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/dmgr/SystemOut.log file for errors and warnings.
[10/8/12 10:28:18:931 EDT] 00000000 WSKyStore W CWPX0041W: One or more key stores are using the default password.
[10/8/12 10:28:22:044 EDT] 00000000 ThreadPooMgr W WSVR0626W: The ThreadPoo setting on the ObjectRequestBroker service is deprecated.
[10/8/12 10:28:22:725 EDT] 00000000 HostNameMap W HMGRO064W: Resolution of IP Addresses for host name con-dmgr found only the loopback address. The loopback address will be used.
VTLO040I: 3 errors/warnings are detected in the /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/dmgr/SystemOut.log file
VTLO070I: The Installation Verification Tool verification succeeded.
VTLO080I: The installation verification is complete.
```

You have finished the WAS ND installation and configuration, we have a cell deployed named con-dmgrCell01.

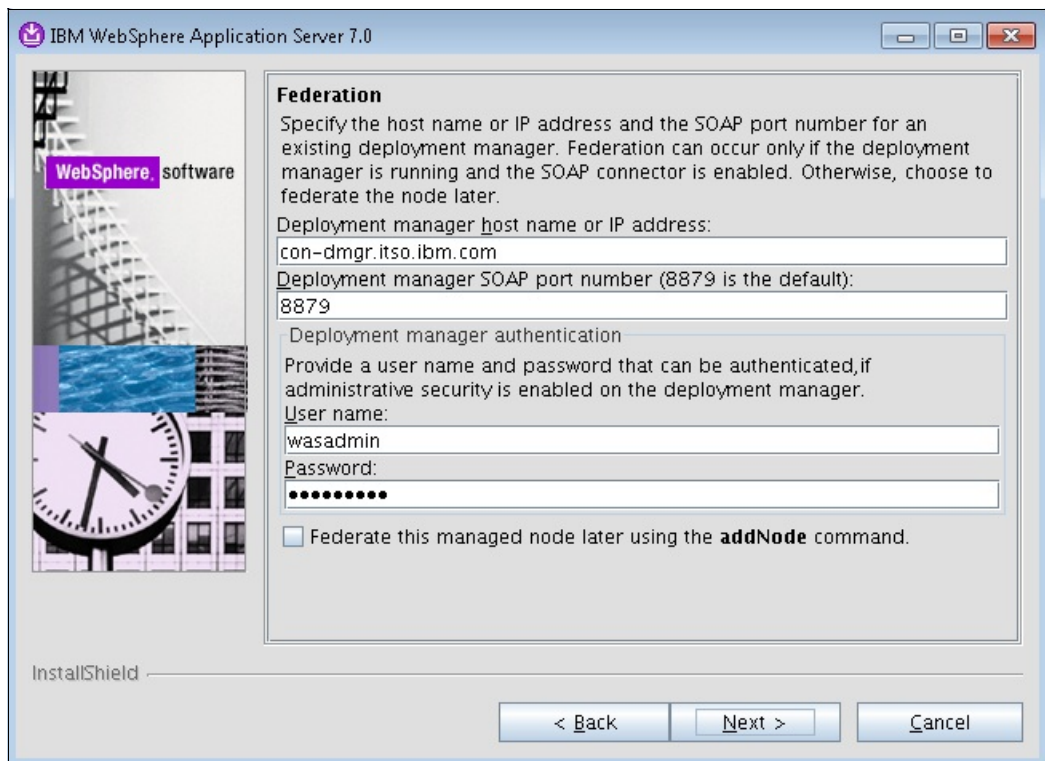
## Installing and configuring a Node

After installing the Deployment Manager, you must install WebSphere Application Server and configure it as a node. On each additional node that hosts IBM Connections you federate the node into the Deployment Manager installed in the previous step. The installation steps are similar to the installation steps of the WebSphere Application Server ND. For the node that hosts IBM Connections, the WebSphere Application Server profile is Custom.

1. Unzip the WebSphere Application Server Network Deployment package file (C1G35ML.tar.gz) in a temporary directory (for example, /tmp). Go to the WAS directory (/tmp/WAS) and run **install** to start the installation wizard.
2. Accept the the software license agreement to continue.
3. The installation wizard checks the prerequisites of your operational system. You might receive an warning informing that your operating system is not detect. This is because your environment might been added after the product release, probably your environment is newer than the minimum required to install WAS ND so you can click on **Next**. To check the compatibility, see 5.1, “Verify software requirements” on page 40.
4. Choose the installation directory. By default, the installation wizard sets the following directories:  
Linux: **/opt/IBM/WebSphere/AppServer**  
AIX: **/usr/IBM/WebSphere/AppServer**  
Windows: **:\IBM\WebSphere\AppServer**
5. Choose the profile to be installed. For the IBM Connections node, select **Custom**.

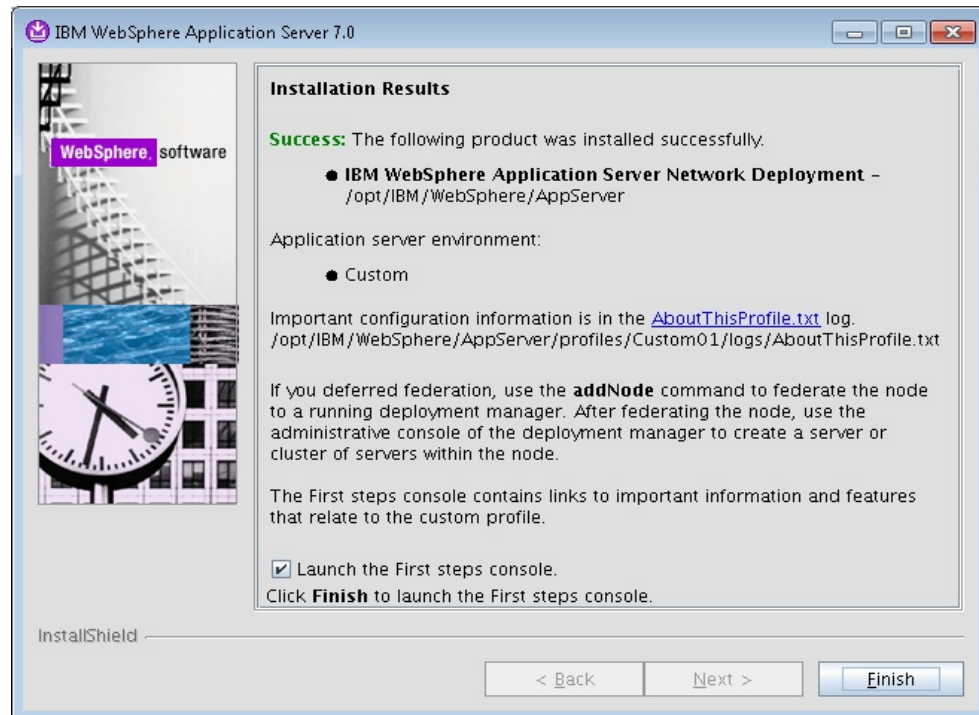


- On the Federation window, provide the **Deployment manager host name**, **SOAP port**, **user name** and **password**, defined during the WAS ND installation.



- After you have defined all the installation parameters, the installation wizard provides a summary and checks the permission before perform the installation.

8. If there are no permission issues, the wizard returns success as validation result. Click **Next** to start the installation process.
9. The installation wizard provides the success result when finishes the installation. For the installation log, see AboutThisProfile.txt on /opt/IBM/WebSphere/AppServer/profiles/Custom01/logs/AboutThisProfile.txt.



10. The installation finishes successfully.



## Verifying WebSphere Version

To verify the WebSphere Application Server version, run the following command:

- Linux: `/opt/IBM/WebSphere/AppServer/bin/versionInfo.sh`
- AIX: `/usr/IBM/WebSphere/AppServer/bin/versionInfo.sh`
- Windows: `\Program Files\IBM\WebSphere\AppServer\bin\versionInfo.bat`

The following figure shows the result of the `versionInfo` command.

```
con-dmgr:/opt/IBM/WebSphere/AppServer/bin # ./versionInfo.sh
WVER0010I: Copyright (c) IBM Corporation 2002, 2005, 2008; All rights reserved.
WVER0012I: VersionInfo reporter version 1.15.5.1, dated 6/15/11

-----
IBM WebSphere Application Server Product Installation Status Report
-----

Report at date and time October 22, 2012 3:21:11 PM EDT

Installation
-----
Product Directory      /opt/IBM/WebSphere/AppServer
Version Directory      /opt/IBM/WebSphere/AppServer/properties/version
DTD Directory          /opt/IBM/WebSphere/AppServer/properties/version/dtd
Log Directory          /opt/IBM/WebSphere/AppServer/logs
Backup Directory       /opt/IBM/WebSphere/AppServer/properties/version/nif/backup
TMP Directory          /tmp

Product List
-----
ND                      installed

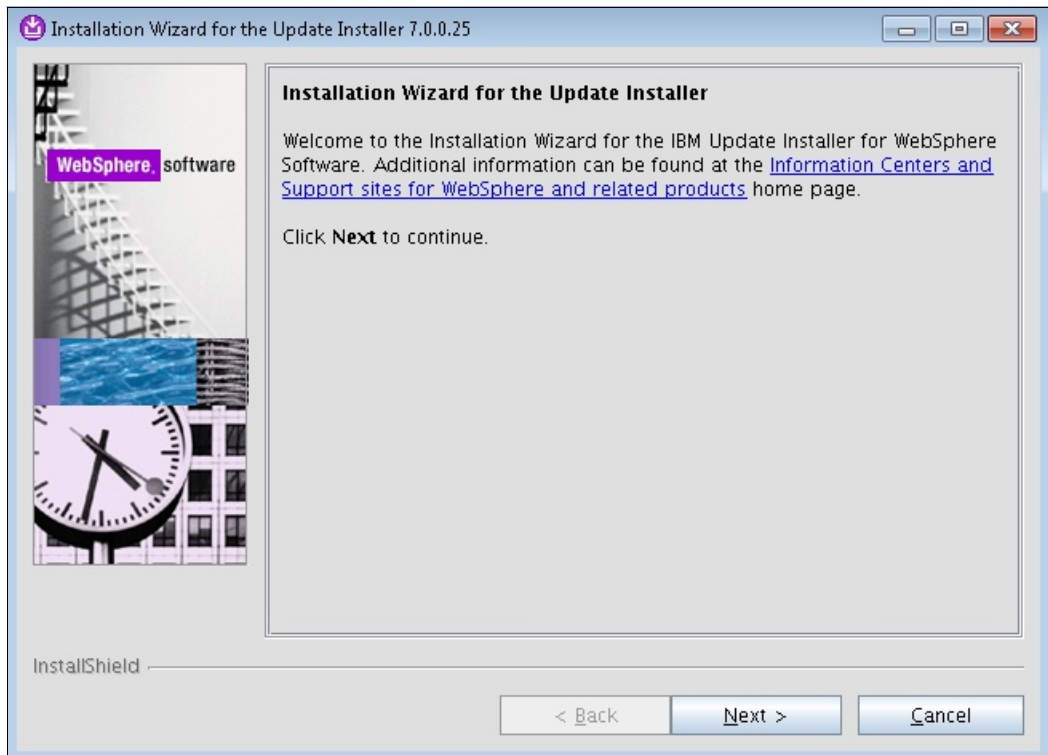
Installed Product
-----
Name                    IBM WebSphere Application Server - ND
Version                 7.0.0.21
ID                      ND
Build Level             cf211150.04
Build Date              12/14/11
Architecture            AMD (64 bit)

-----
End Installation Status Report
-----
```

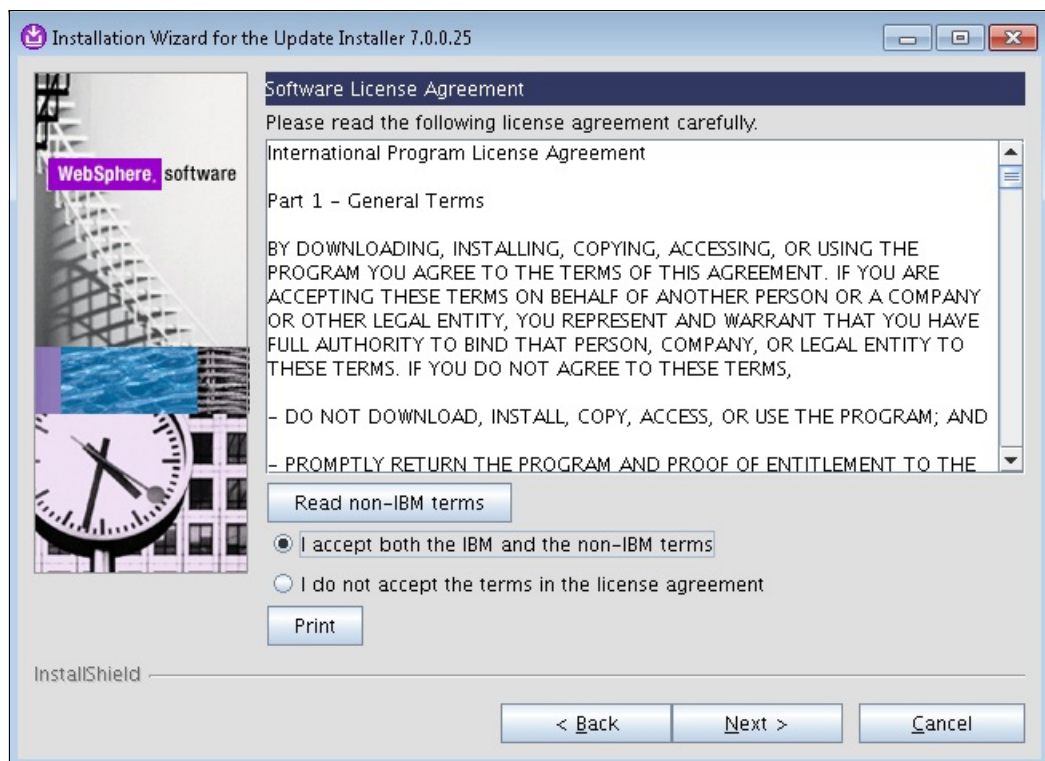
For the recommended fixes for WebSphere Application Server, see WebSphere Application Server fix pack website (<http://www-01.ibm.com/support/docview.wss?uid=swg27004980>).

IBM Connections requires fix pack 21 to be installed on WAS. You must install the update installer to apply the fix pack on WAS. Follow these steps to complete update installer installation and fix pack 21:

1. Stop WebSphere Application Server before start the Update Installer installation.
2. Unzip the downloaded Update Installer source to a temporary folder (for example, `/tmp`) and start the installation by running `/tmp/UpdateInstaller/ install`.

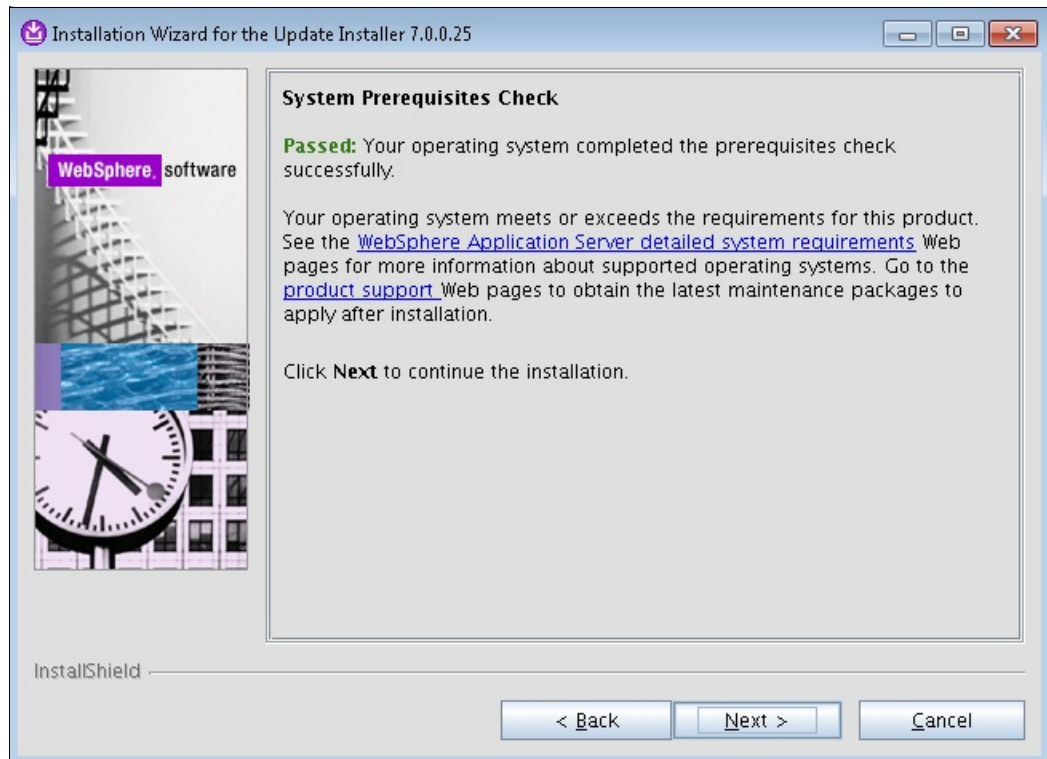


3. Read and accept the license agreement to continue. Click on **I accept both the IBM and the non-IBM terms**.

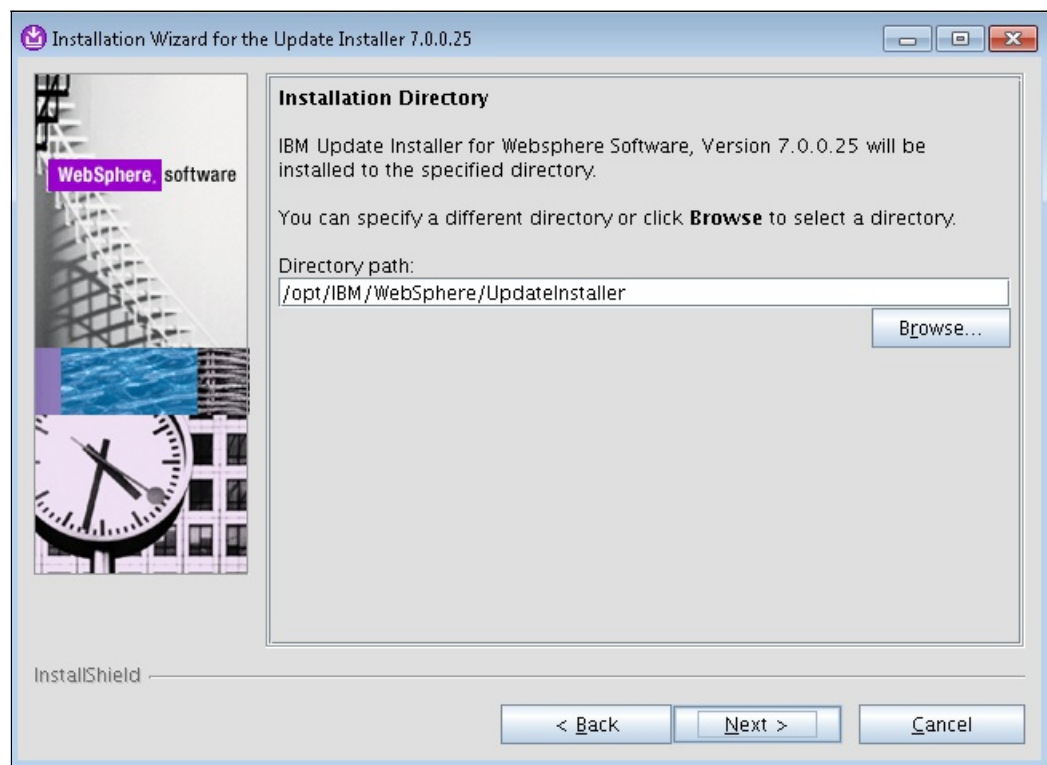


4. The wizard checks the system requirements of your operating system.

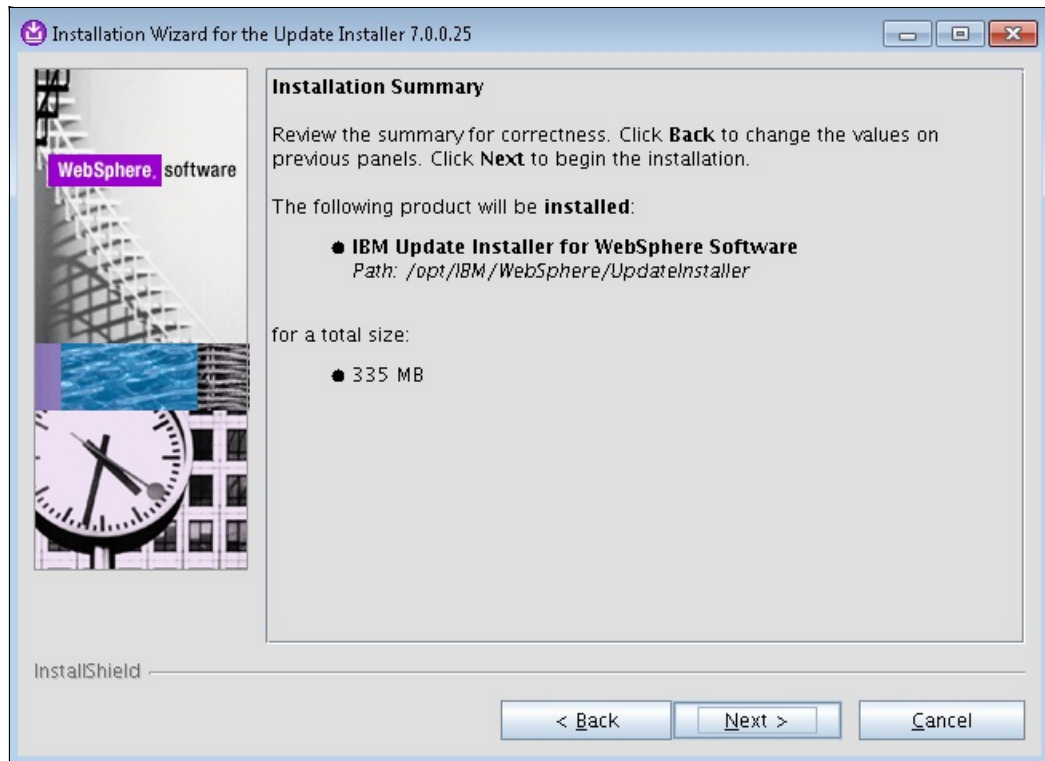




5. Choose the installation directory to install the Update Installer. The default on a Linux system is **/opt/IBM/WebSphere/UpdateInstaller**.

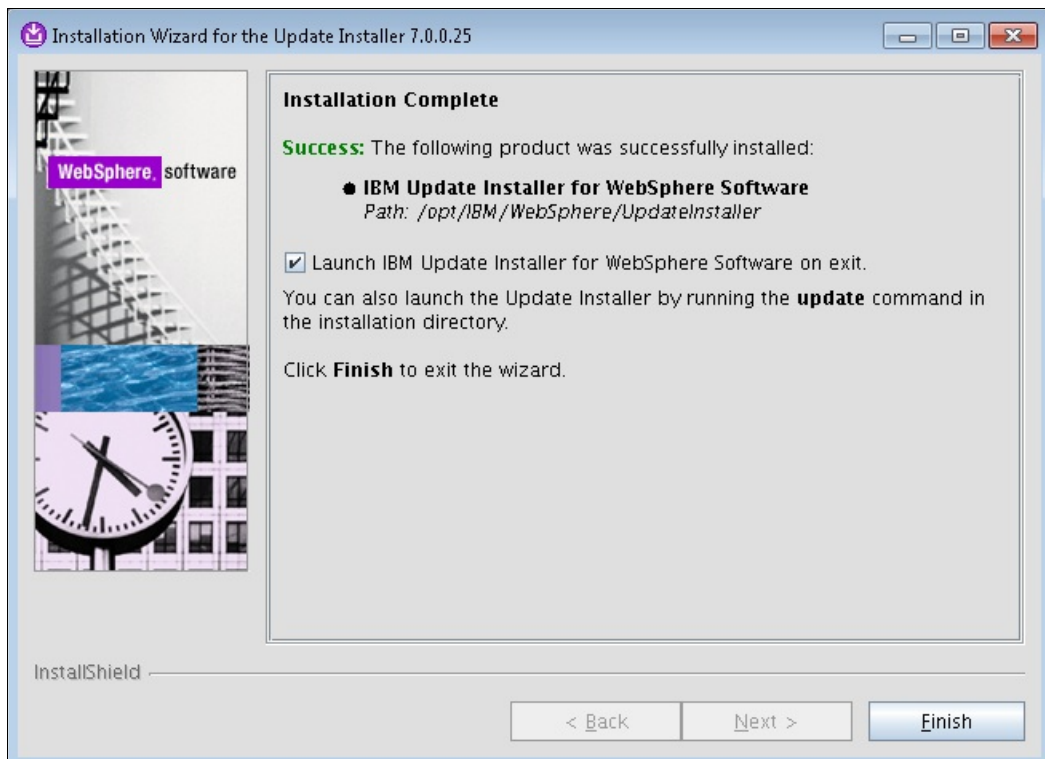


6. The installation wizard reports the summary for you to validate if the parameters are correctly defined before continuing.



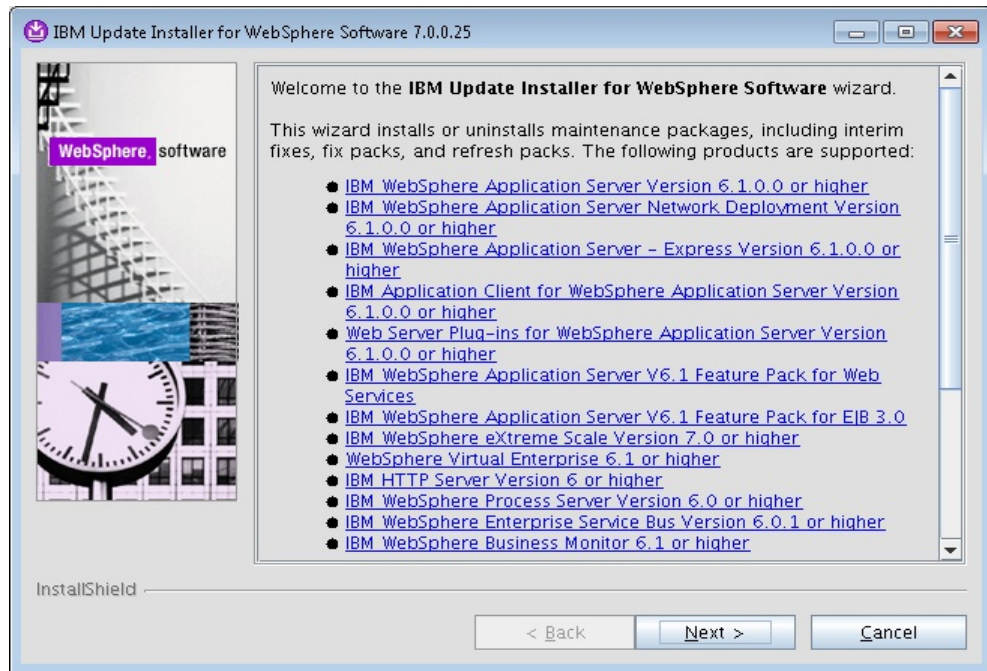
7. If you want to start the Update Installer automatically when the installation is finished, check **Launch IBM Update Installer for WebSphere Software on exit**.

If you do not start the Update Installer automatically after the installation, You can start the Update Installer manually by running `/opt/IBM/WebSphere/UpdateInstaller/update.sh`.

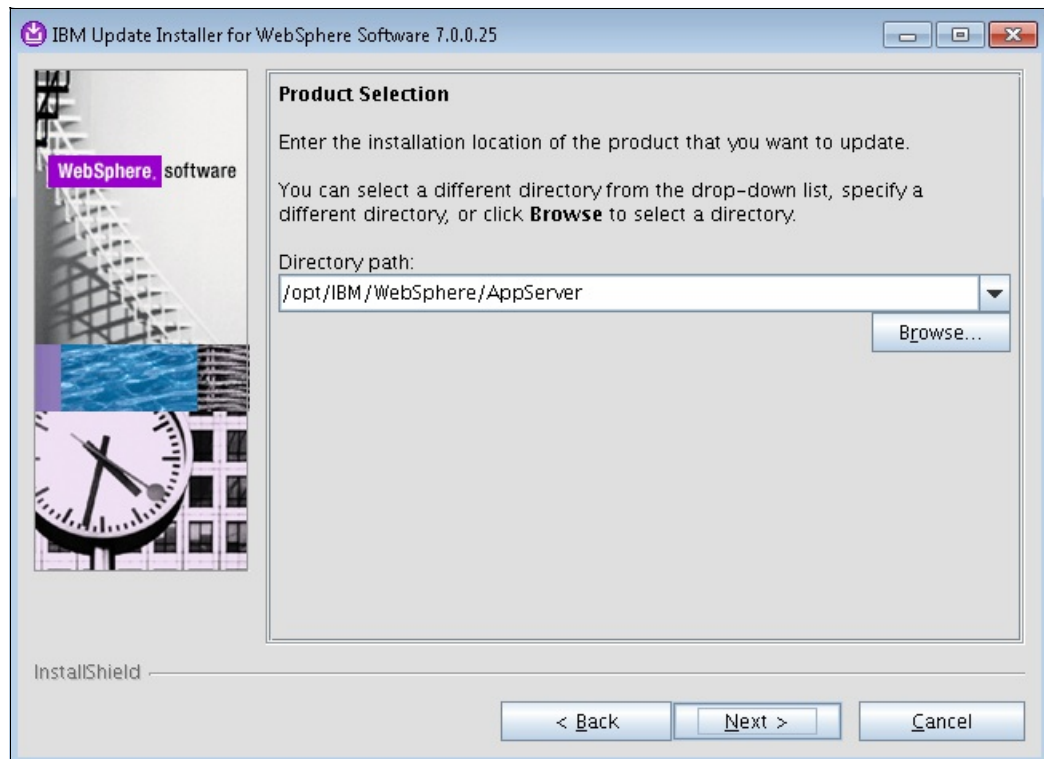


8. Since we selected to start the Update Installation automatically, the update process starts and the Welcome window shows you the supported products.

To install a WebSphere Application Server fix pack, download the fix pack and store the files in a temporary directory (for example, `/opt/IBM/WebSphere/UpdateInstaller/maintenance`).

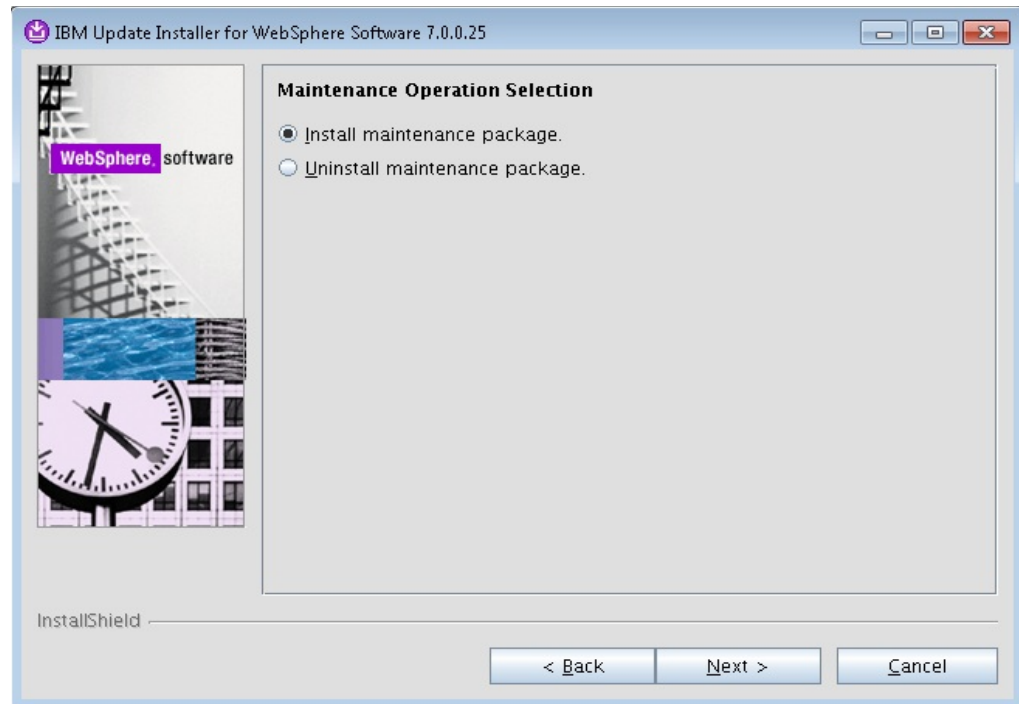


9. Select the product that you want to update by clicking the dropdown list and select the installed product to be updated.

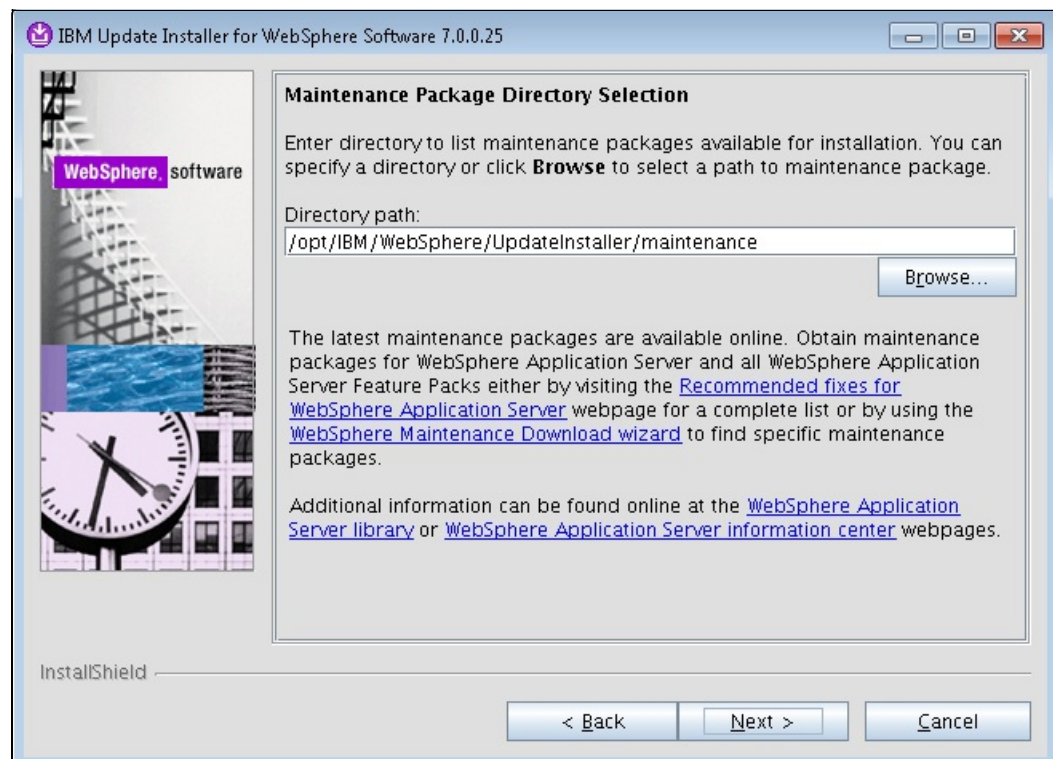




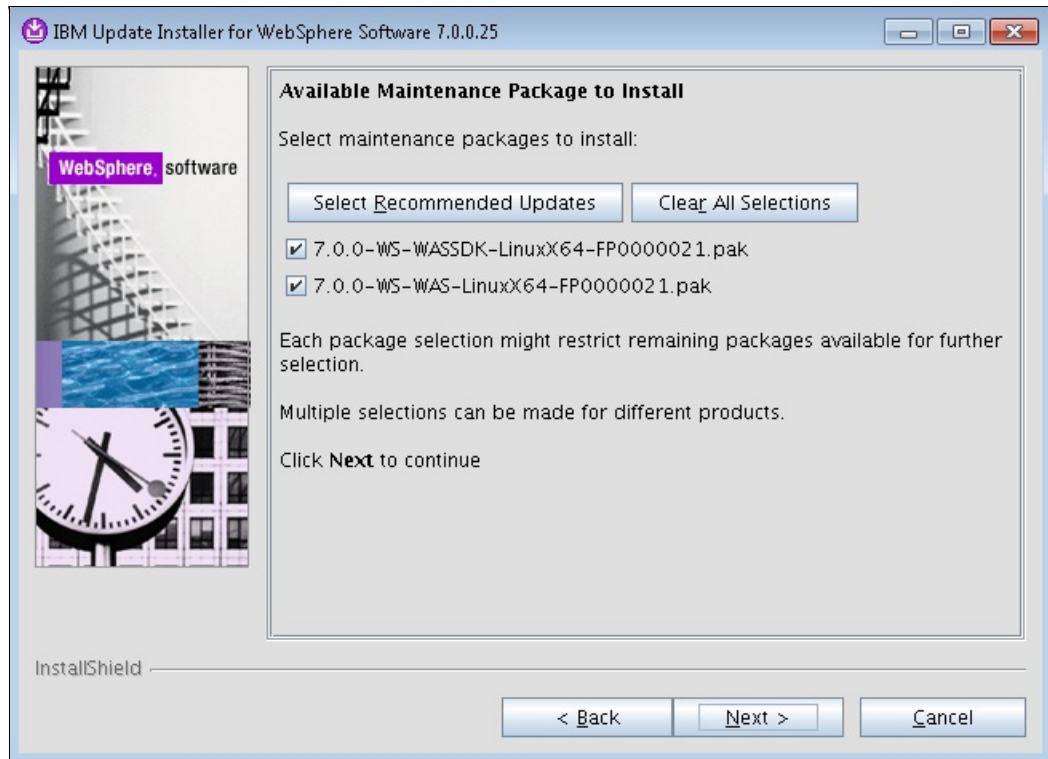
10. The following options are available to manage your maintenance update. Select **Install maintenance package**.



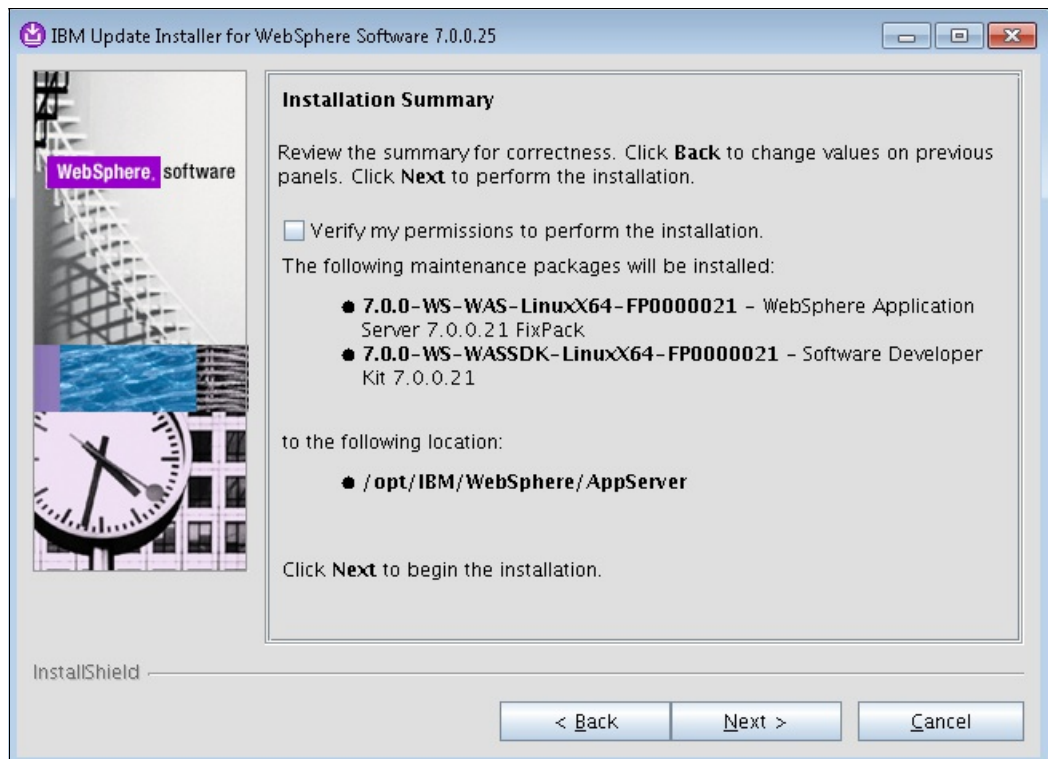
11. Enter the directory where you have stored your fix pack. The wizard lets you choose the directory where the fix pack is stored ( for example, **/opt/IBM/WebSphere/UpdateInstaller/maintenance**)



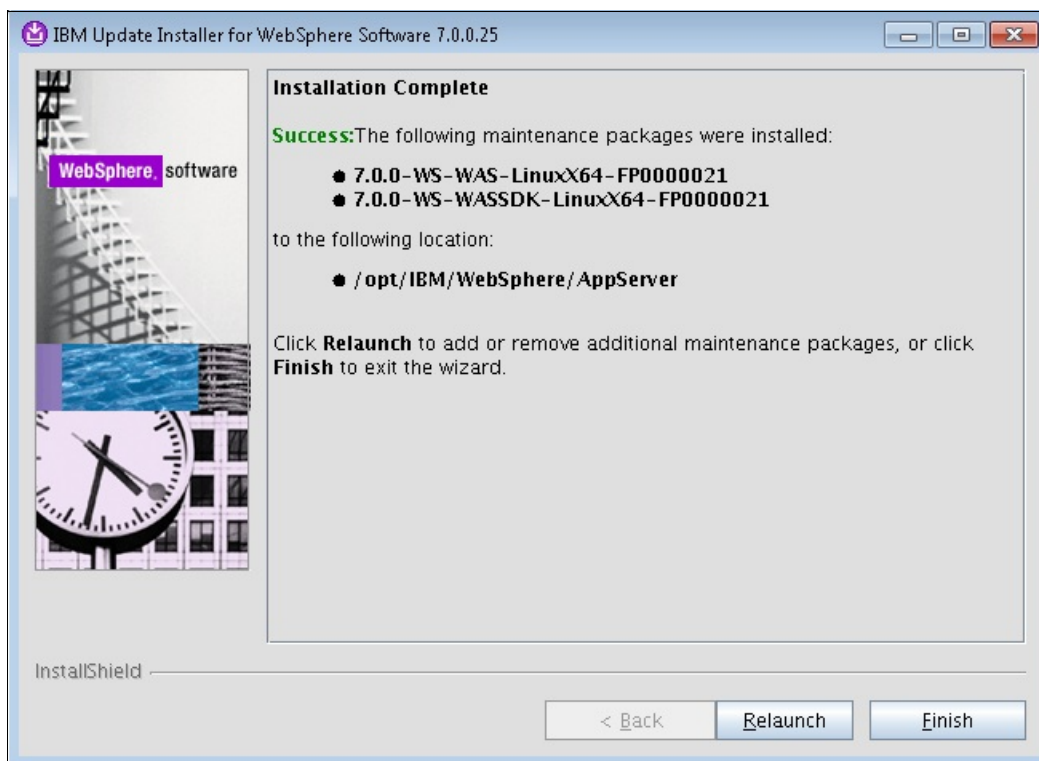
12. The Update wizard automatically recognizes the files in the maintenance directory and selects the files to be installed.



13. You can verify the permission before starting the maintenance installation by checking **Verify my permissions to perform the installation**.



14. The wizard provides the result of the maintenance installation:



You have installed and applied the fix pack on WebSphere Application Server using Update Installer.

## 6.4.2 Configuring WebSphere to use LDAP repository

To support the IBM Connections installation, you have to configure WebSphere Application Server to access at least one LDAP directory to allow IBM Connections to authenticate the users on LDAP user repository.

Following these steps to add one or more LDAP servers as a **federated repository** using Integrated Solutions Console (ISC):

1. Access the WebSphere Console from a web browser, for example, <https://con-dmgr.itso.ibm.com:9043/ibm/console/>
2. Expand the **Security** on the left menu and click **Global security**. Select **Federated repositories** on *Available realm definitions* and click **Configure**.

**Global security**

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

Security Configuration Wizard      Security Configuration Report

**Administrative security**

☒ Enable administrative security

- [Administrative user roles](#)
- [Administrative group roles](#)
- [Administrative authentication](#)

**Application security**

☒ Enable application security

**Java 2 security**

☒ Use Java 2 security to restrict application access to local resources

☐ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

**User account repository**

Current realm definition

Federated repositories

Available realm definitions

Federated repositories

[Configure...](#) [Set as current](#)

**Authentication**

Authentication mechanisms and expiration

☒ LTPA

☐ Kerberos and LTPA

- [Kerberos configuration](#)
- [Authentication cache settings](#)
- ☐ Web and SIP security
- ☐ RMI/IIOP security
- ☐ Java Authentication and Authorization Service
- ☐ Use realm-qualified user names

- [Security domains](#)
- [External authorization providers](#)
- [Custom properties](#)

[Apply](#) [Reset](#)

### 3. Select **Add Base entry to Realm**.

**Global security**

**Global security > Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

**General Properties**

\* Realm name  
defaultWIMFileBasedRealm

\* Primary administrative user name  
wasadmin

**Server user identity**

☒ Automatically generated server identity

☐ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

☒ Ignore case for authorization

Repositories in the realm:

[Add Base entry to Realm...](#) [Use built-in repository](#) [Remove](#)

| Select                   | Base Entry                 | Repository Identifier  | Repository Type |
|--------------------------|----------------------------|------------------------|-----------------|
| <input type="checkbox"/> | o=defaultWIMFileBasedRealm | InternalFileRepository | File            |

You can administer the following resources:

Total 1

**Additional Properties**

- [Property extension repository](#)
- [Entry mapping repository](#)
- [Supported entity types](#)

**Related Items**

- [Manage repositories](#)
- [Trusted authentication realms - inbound](#)

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

**Help**

**Field help**  
For field help information, select a field label or list marker when the help cursor is displayed.

**Page help**  
[More information about this page](#)

### 4. Click **Add Repository**.

**Global security** > **Federated repositories** > **Repository reference**

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.

**General Properties**

\* Repository  
 none defined Add Repository...

\* Distinguished name of a base entry that uniquely identifies this set of entries in the realm

Distinguished name of a base entry in this repository

Apply OK Reset Cancel

5. Enter the following parameters to configure the LDAP connection and credentials:
  - *Repository identifier*: Define a name to identify the repository to be added, for example, Renovations LDAP directory.
  - *Directory Type*: Select the LDAP type on the list.
  - *Primary host name*: Enter the full qualified host and domain name of the LDAP server (FQDN).
  - *Port*: Enter the TCP port that your LDAP is configured.
  - *Bind distinguished name*: If your LDAP does not allow anonymous search, you must provide a user name and password in canonical format, e.g. cn=Administrator, o=itso
  - *Bind password*: Enter the bind user password.
  - *Login properties*: Specify the login attribute or attributes that you want to use for authentication. Common examples are uid; cn; mail for unique ID, common name and mail. Separate multiple values with semi-colons.

Global security > Federated repositories > Repository reference > New

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

**General Properties**

\* Repository identifier  
ldap-dom

**LDAP server**

\* Directory type  
IBM Lotus Domino

\* Primary host name  
ldap-dom.itso.ibm.com

Port  
389

Failover server used when primary is not available:

Delete

| Select | Failover Host Name | Port |
|--------|--------------------|------|
|        | None               |      |

Add

Support referrals to other LDAP servers  
ignore

**Security**

Bind distinguished name  
domadmin

Bind password  
\*\*\*\*\*

Login properties  
uid

LDAP attribute for Kerberos principal name

Certificate mapping  
EXACT\_DN

Certificate filter

☐ Require SSL communications

☒ Centrally managed

[Manage endpoint security configurations](#)

☐ Use specific SSL alias

CellDefaultSSLSettings [SSL configurations](#)

The additional properties will not be available until the general properties for this item are applied or saved.

**Additional Properties**

- Performance
- LDAP entity types
- Group attribute definition

Apply OK Reset Cancel

6. On the Repository reference page, the following fields represent the LDAP attribute type and value pairs for the base element in the realm and the LDAP repository.

The type and value pair are separated by an equal sign (=), for example: o=itso. These can be the same value when a single LDAP repository is configured for the realm or can be different in a multiple LDAP repository configuration.

- *Distinguished name of a base entry that uniquely identifies this set of entries in the realm:* Identifies entries in the realm. This base entry must uniquely identify the external repository in the realm. If multiple repositories are included in the realm, use this field to define an additional distinguished name (DN) that uniquely identifies this set of entries within the realm.
- *Distinguished name of a base entry in this repository:* Identifies entries in the LDAP directory. The base entry indicates the starting point for searches in this LDAP directory server.

**Note:** If you have defined flat groups in the Domino directory, do not enter a value in this field. Flat groups are group names such as SalesGroup, as opposed to: cn=SalesGroup,ou=Groups,o=itso. If you configure a search base in this Step, you will not be able to access the groups



**Global security**

☐ Messages

⚠ Changes have been made to your local configuration. You can:

- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

⚠ The server may need to be restarted for these changes to take effect.

**Global security > Federated repositories > Repository reference**

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.

**General Properties**

\* Repository  
 ldap-dom

\* Distinguished name of a base entry that uniquely identifies this set of entries in the realm  
 o=itso

Distinguished name of a base entry in this repository

7. Click **Apply** and **Save**.
8. If you want to add more LDAP repositories, repeat the steps.

**Note:** If you are using a Domino LDAP, replace the default mapping with dominoPerson and dominoGroup object classes for person account and group entities.

9. On the WebSphere Console, access the **Federated repositories** and click the name of the repository at *Repository Identifier* (for example, ldap-dom) to return to the Repository page.

**Global security**

**Global security > Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

**General Properties**

\* Realm name  
 defaultWIMFileBasedRealm

\* Primary administrative user name  
 wasadmin

**Server user identity**

☒ Automatically generated server identity

☐ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

☒ Ignore case for authorization

**Repositories in the realm:**

| Select                                      | Base Entry                 | Repository Identifier  | Repository Type |
|---|----------------------------|------------------------|-----------------|
| You can administer the following resources: |                            |                        |                 |
| <input type="checkbox"/>                    | o=defaultWIMFileBasedRealm | InternalFileRepository | File            |
| <input type="checkbox"/>                    | o=itso                     | ldap-dom               | LDAP:DOMINO     |
| Total 2                                     |                            |                        |                 |

**Additional Properties**

- Property extension repository
- Entry mapping repository
- Supported entity types

**Related Items**

- Manage repositories
- Trusted authentication realms - inbound

10. On *Additional Properties*, click **LDAP entity types**.

The additional properties will not be available until the general properties for this item are applied or saved.

**Additional Properties**

- [Performance](#)
- [LDAP entity types](#)
- [Group attribute definition](#)

11. Edit the **Group** and **PersonAccount**.

Global security

[Global security](#) > [Federated repositories](#) > [ldap-dom](#) > **LDAP entity types**

Use this page to list entity types that are supported by the member repositories or to select an entity type to view or change its configuration properties.

⊞ Preferences

| Entity Type                                 | Object Classes                                   |
|---|--|
| You can administer the following resources: |  |
| <a href="#">Group</a>                       | dominoGroup                                      |
| <a href="#">OrgContainer</a>                | organization;organizationalUnit;domain;container |
| <a href="#">PersonAccount</a>               | dominoPerson                                     |
| Total 3                                     |  |

12. Click **Apply** and **Save**.

The WebSphere Application Server is configured to use a LDAP repository.

### 6.4.3 Configuring security on ISC

After you configure your LDAP repositories, you must define the WebSphere Application Server to use this repository to authenticate all users.

Complete these steps to configuring the WebSphere Application Server security, using Integrated Solutions Console (ISC):

1. On the Integrated Solution Console, click **Security** on the left menu and choose **Global Security**, on *Available realm definitions* at the *User account repository*, select **Federated repository** and click **Configure**. Set the following parameters:
  - *Realm name*: Select the principal repository in *Repository identifier*, for example, **o=itso**
  - *Primary administrative user name*: This is the administrative user name of your LDAP server, for example, **domadmin**.



**Global security > Federated repositories**

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

**General Properties**

\* Realm name  
o=itso

\* Primary administrative user name  
domadmin

**Server user identity**

☒ Automatically generated server identity

☐ Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node  
Password

☒ Ignore case for authorization

Repositories in the realm:

Add Base entry to Realm... Use built-in repository Remove

| Select                                      | Base Entry                 | Repository Identifier  | Repository Type |
|---|----------------------------|------------------------|-----------------|
| You can administer the following resources: |                            |                        |                 |
| <input type="checkbox"/>                    | o=defaultWIMFileBasedRealm | InternalFileRepository | File            |
| <input type="checkbox"/>                    | o=itso                     | ldap-dom               | LDAP:DOMINO     |
| Total 2                                     |                            |                        |                 |

**Additional Properties**

- Property extension repository
- Entry mapping repository
- Supported entity types

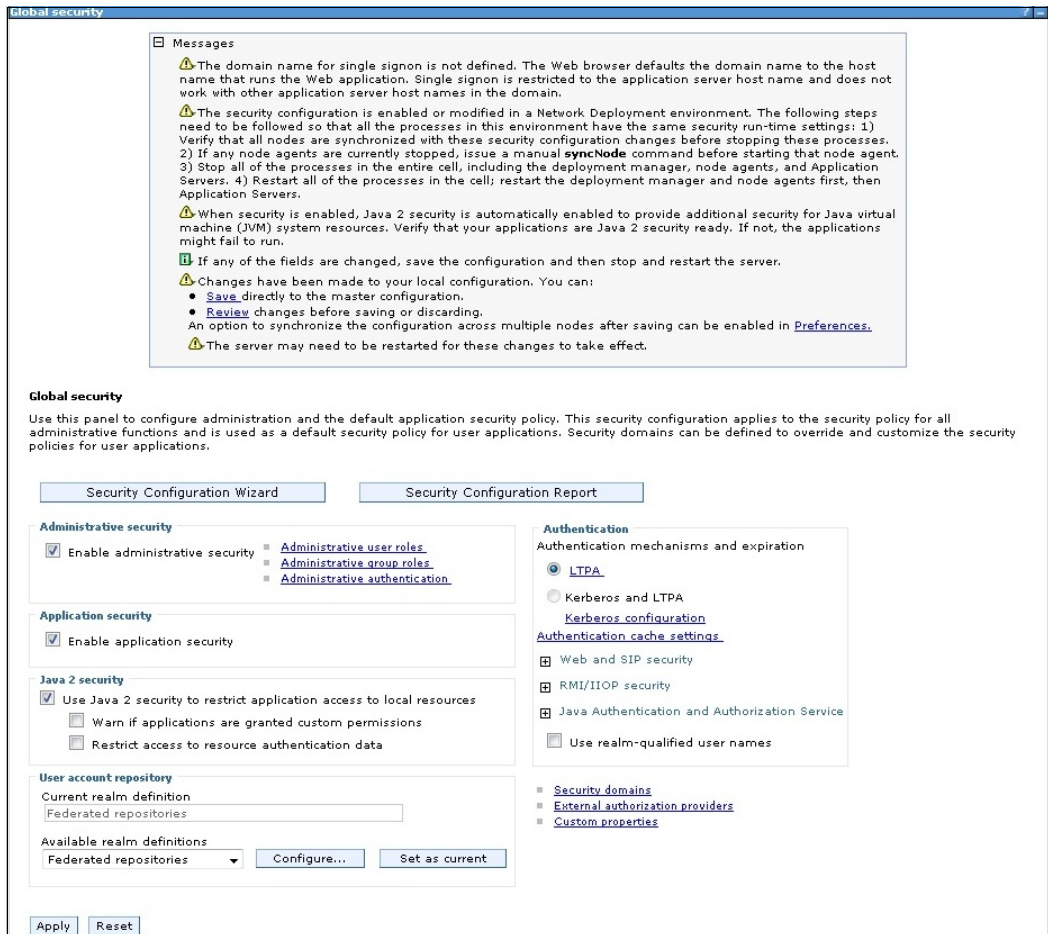
**Related Items**

- Manage repositories
- Trusted authentication realms - inbound

Apply OK Reset Cancel

Click **OK** and **save** configuration.

- On the **Global security** window, select **Federated repository** at *Available realm definitions* and click **Set as current**. Verify if the **Enable administrative security** is checked and click **OK** and **Save**.



3. Restart the WebSphere Application Server and try to access the ISC using the user name defined as the primary administrator.

You have finished the WebSphere Application Server installation and configuration, now you can install the IBM Connections.

## 6.5 Creating databases

When DB2 is successfully installed, you must apply the supplied license file in order to avoid the DB2 instance being a trial version and eventually stopping. To do this, follow this procedure:

1. As Administrator or root user, locate the *DB2\_ESE\_Restricted\_QS\_Activation\_97.zip* file which is supplied as part of the IBM Connections files (part number CZ381ML).
2. Extract the ZIP file and make a note of the location of the resulting lic file. You can move it somewhere more convenient.
3. Open a terminal or command prompt and navigate to the DB2 bin folder.
4. Enter the following command:

```
db2licm -a path_to_lic_file/db2ese_o.lic
```

where path\_to\_lic\_file is the directory to which you extracted the db2ese\_o.lic file.

5. Verify that the new license has been added by typing the command `db2licm -l`. Assuming it reports the correct licence, restart DB2.

You can create DB2 database for IBM Connections using DB2 Database Wizard. Locate the Database Wizards ZIP file obtained as part of the IBM Connections 4 installation files and unzip them to a convenient location. Follow these steps to create a DB2 database:

1. If your DB2 is on a Windows 2008 64-bit. system, you must perform DB2 administration tasks with full administrator privileges.
  - a. Logged in as the instance owner, open a command prompt and change to the DB2 bin directory. For example:  
`C:\Program Files\IBM\SQLLIB\BIN.`
  - b. Enter the following command:  
`db2cwadmin.bat.`  
This command opens the **DB2** command line processor while also setting your DB2 privileges.
2. From the IBM Connections Wizards directory, open the following file to launch the wizard:
  - Linux: `./dbWizard.sh`
  - Microsoft Windows: `dbWizard.bat`
3. Click **Next** to continue.
4. Select the option to create a database and click **Next**.
5. Enter the details of the database you want to create and then click **Next**:
  - Select a database type.
  - Select the location of the database.
  - Specify a database instance.
6. Select an application and click **Next**.
7. Review the Pre Configuration Task Summary to ensure that the values you entered on previous pages in the wizard are correct. If you want to make a change, click **Back** to edit the value. Click **Create** to begin creating databases.

**Note:** Click **Show detailed database commands** to preview each **SQL** command before it is run by the wizard. If you choose to save the commands, you must have write-access to the folder that you choose to save them in.

8. Review the Post Configuration Task Summary panel and, if necessary, click **View Log** to open the log file. Click **Finish** to exit the wizard.

## 6.6 Populating Profiles using population wizard

IBM Connections uses profiles database to store user related information. Tivoli Directory Integrator (TDI) tool uses one set of assembly lines to extract user related data from different LDAP repositories and another set of assembly lines to store user information to profiles database. The population wizard manually extracts data from LDAP server and moves the data to profiles database.

## 6.6.1 Preparing to run profile populating wizard

The population wizard is a GUI tool captures the details for LDAP server, database server and database driver. The tool runs on both Windows and UNIX platform. In our lab setup, we installed the tool on Windows platform using the follow steps:

1. Extract the IBM\_Connections40\_Wzd\_WIN\_CIA3GML.exe file to a temporary directory.  
For example, C:\IBM\Wizards.
2. Copy the following DB2 jdbc driver files from the database server to a temporary directory.  
For example, C:\IBM\DB2Drivers
  - db2jcc.jar
  - db2jcc\_license\_cu.jar
3. Disable JIT compiler and increase the runtime memory to store more users in memory.  
For example, go to C:\IBM\TDI\7.1 directory and update the ibmdisrv.bat file as follows:

– Before:

---

```
TDI_JAVA_PROGRAM%" -classpath "%TDI_HOME_DIR%\IDILoader.jar" %ENV_VARIABLES%  
com.ibm.di.loader.ServerLauncher %*
```

---

– After:

---

```
%TDI_JAVA_PROGRAM%" -Xms256M -Xmx1024M -Xnojit -classpath  
"%TDI_HOME_DIR%\IDILoader.jar" %ENV_VARIABLES%  
com.ibm.di.loader.ServerLauncher %*
```

---

## 6.6.2 Running the profile population wizard

Prior to running the population wizard tool, make sure that database server and LDAP server is accessible from the system where the script is running. In our lab environment we used DB2 as the data store for IBM Connections applications.

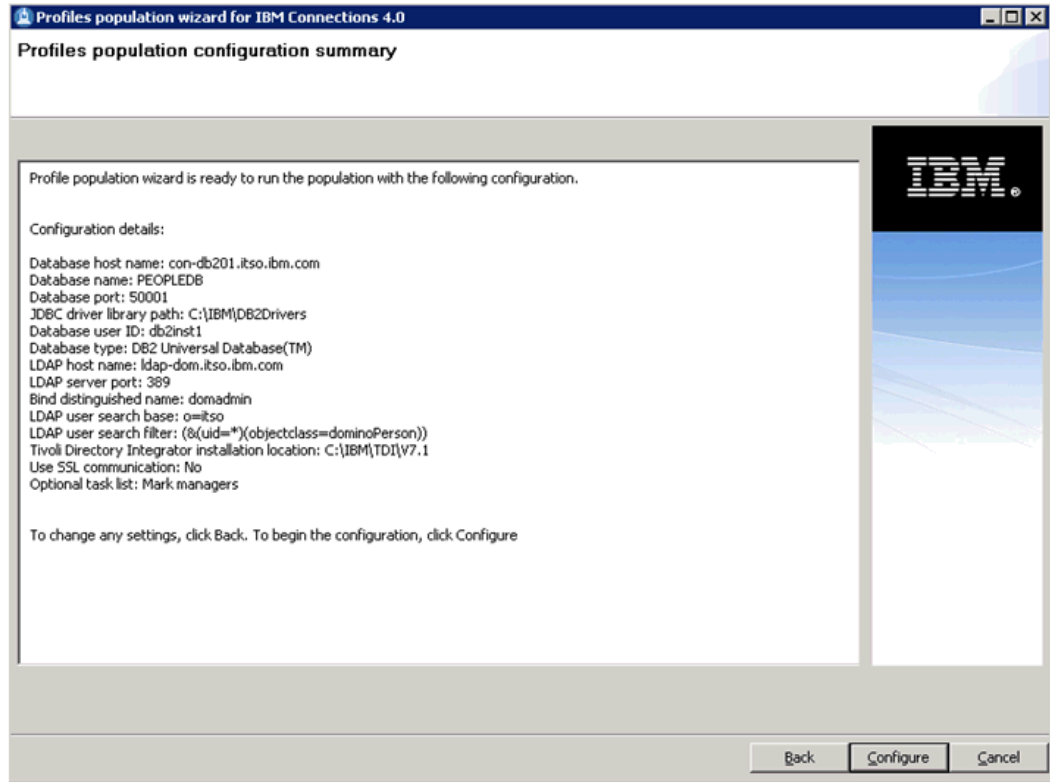
1. Start the population wizard. For example, go to C:\IBM\Wizards directory and run the **populationWizard.bat** script file
2. Select the TDI server location as **C:\IBM\TDI\7.1** and click **Next**,
3. Select a database type as DB2 and click **Next**,
4. Provide the value for DB2 server hostname, port, database name, username, and password and db2 jdbc driver location.

|  |                        |  |
|--|------------------------|--|
| Host name:                                   | con-db201.itso.ibm.com |  |
| Port:  | 50001                  |  |
| Database name:                               | PEOPLED8               |  |
| JDBC driver library path:                    | C:\IBM\DB2Drivers      | <input type="button" value="Browse..."/> |
| User ID (Account used to write to database): | db2inst1               |  |
| Password:                                    | *****                  |  |

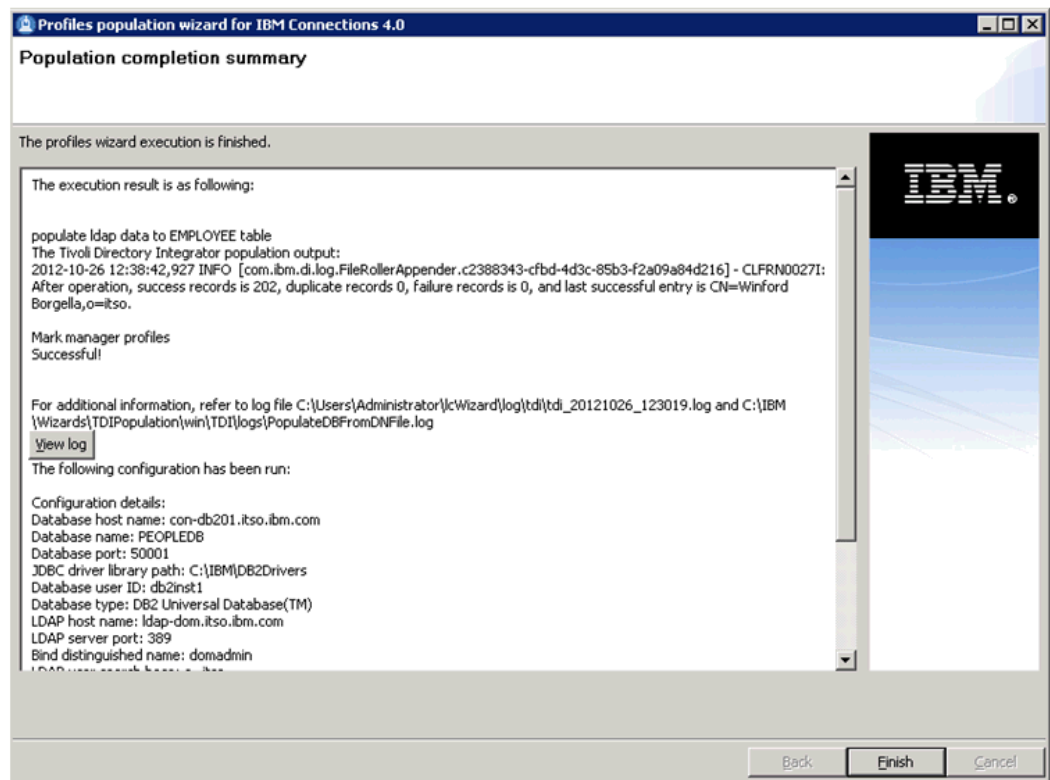
5. Provide LDAP server host name and port number.

|  |                       |
|--|-----------------------|
| LDAP server name:                                  | ldap-dom.itso.ibm.com |
| LDAP server port:                                  | 389                   |
| Select to use SSL communication for secured access |                       |
| <input type="checkbox"/>                           | Use SSL communication |

6. Enter the LDAP bind ID for example, **domadmin**.
7. Provide the value for search base, for example o=itso. If the value specified at the organization level, user is searched from the organization level.
8. Accept the default values for database mapping.
9. Accept the default values for optional database tasks.
10. The configuration summary shows. Click **Configure** to continue.



11. After successful user population, the following screen is displayed. Click **Finish** to complete the task.



## 6.7 Installing Cognos Business Intelligence

Cognos Business Intelligence (BI) server collects data for Metrics Application to provide statistical information about IBM Connections server. This involves setting up WebSphere Application Server Network Deployment and Cognos components. The setup steps for Cognos BI server are as follows:

1. Installing WebSphere Application Server for Cognos BI
2. Preparing database client for IBM Cognos BI Transformer
3. Preparing databases for Cognos BI Server
4. Installing Cognos BI Server
5. Federating Cognos BI Server to the Deployment Manager
6. Validating Cognos BI Server

### 6.7.1 Required software

The following software components must be available prior to starting the installation. You can download these software from IBM Passport advantage or contact IBM representative to purchase the software products.

| Name   | Software part Number                 |
|--|--------------------------------------|
| WebSphere Application Server V7.0 Network Deployment | C1G2JML_WAS7ND_WIN_x86-64            |
| WebSphere Update Installer                           | 7.0.0.25-WS-UPDI-WinAMD64            |
| JDK Update for WebSphere Fix pack                    | 7.0.0-WS-WASSDK-WinX64-FP0000021.pak |
| WebSphere Application Server Fix pack                | 7.0.0-WS-WAS-WinX64-FP0000021.pak    |
| Cognos BI Transformer                                | bitsrfrmr_win32_10.1.1_ml.tar        |
| Cognos BI Server                                     | bisrvr_win64h_10.1.1_ml.tar          |
| Cognos BI Server Fix pack                            | CBI_10.1.1_Win64_FP001.tar.gz        |
| IBM Connections 4.0 Server for Windows               | IBM_Connections40_WIN_CIA3DML        |

### 6.7.2 Installing WebSphere Application Server for Cognos BI

For WebSphere Application Server installation, see 6.4, “Installing WebSphere Application Server” on page 70. Apply the appropriate settings for Windows platform.

Run the following command to create an Application Server profile:

```
C:\IBM\WebSphere\AppServer\bin>manageprofiles.bat -create -templatepath WAS_install_root/profileTemplates/default -adminUser  
name wsadmin -adminPassword wsadmin  
NSTCONFPSUCCESS: Success: Profile AppSrv01 now exists. Please consult C:\IBM\WebSphere\AppServer\profiles\AppSrv01\logs>About  
hisProfile.txt for more information about this profile.
```

### 6.7.3 Preparing database client for IBM Cognos BI Transformer

IBM Cognos BI Transformer component requires database client locally on the server. For Oracle, install only standard 32 bit client as 64 bit is not supported by Cognos. For SQL server, install SQL Client only. Run the following steps to install and configure DB2 Client.

1. Extract the DB2 Runtime client executable file DB2\_RTC\_97\_Win\_x86-64.exe into a temporary directory.

2. Go to `/RTCL\image\Install\en_US` directory and select **Setup.exe**.
3. Welcome screen is displayed. Click **Next**,
4. Accept the license and terms and conditions. Click **Next**,
5. Select the installation type as **Custom**.
6. Select the installation directory as `C:\IBM\SQLLIB`
7. Select the value for DB2 copy name as `DB2Copy1` and click **Next**.
8. Install summary is displayed. Click **Install** to continue.
9. Click **Finish** to complete the installation.
10. Launch the **DB2** Command Line processor from the startup menu.
11. Run the following command to catalog the node to connect to the DB2 server.

```
db2 => catalog tcpip node db2node remote con-db201.itso.ibm.com server 50001
DB20000I The CATALOG TCPIP NODE command completed successfully.
DB21056W Directory changes may not be effective until the directory cache is
refreshed.
```

12. Run the following command to catalog the database for metrics and cognos  
 For Metrics: **db2 catalog db metrics as metrics at node db2 node**  
 For Cognos: **db2 catalog db cognos as cognos at node db2 node**
13. To validate a metrics database, execute the following command.  
**db2 connect to metrics user db2inst1 using db2inst1**

```
db2 => connect to metrics user db2inst1 using db2inst1

Database Connection Information

Database server          = DB2/LINUX8664 9.7.6
SQL authorization ID     = DB2INST1
Local database alias     = METRICS

db2 =>
```

## 6.7.4 Preparing databases for Cognos BI Server

Cognos requires two databases, cognos and metrics. These databases are created during IBM Connections database setup. For Oracle and SQL server, supply the appropriate value for server name, port number, username and password. The DB2 database details are as follows:

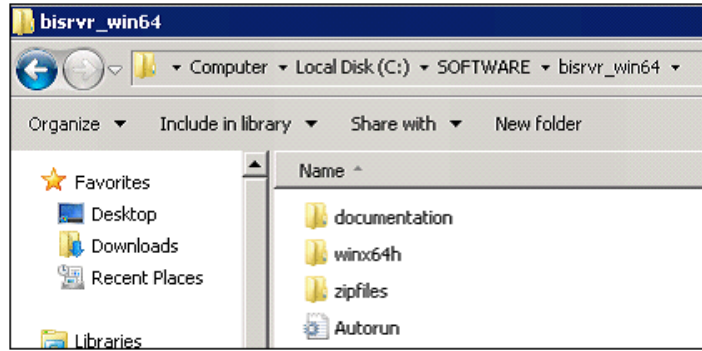
- ▶ Database server Name: `con-db201.itso.ibm.com`
- ▶ Port Number: `50001`
- ▶ DB2 Admin UserId: `db2inst1`
- ▶ DB2 Admin Password: `db2inst1s`
- ▶ Databases: `cognos, metrics`

## 6.7.5 Installing Cognos BI Server

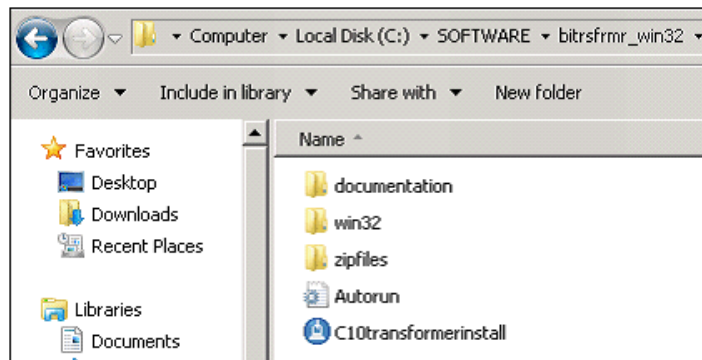
Use the follow steps to install Cognos BI Server:

1. Make sure that WebSphere Application Server and the database server are running.
2. Create a directory to store Cognos installation files, for example `C:\SOFTWARE`.
3. Extract the Cognos BI Server setup file, "`bisrvr_win64h_10.1.1_ml.tar`", to the `C:\SOFTWARE\bisrvr_win64` directory.

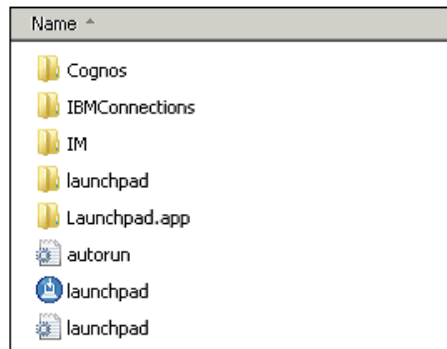





















4. Extract the Cognos BI transformer file "bitsrvmr\_win32\_10.1.1\_ml.tar" to the C:\SOFTWARE\ bitsrvmr\_win32 directory.



5. Extract the Connection Server file "IBM\_Connections40\_WIN\_CIA3DML" into a temporary directory. There is a folder called Cognos.



6. Extract the CognosConfig.zip file from the Cognos directory to C:\IBM\CognosSetup.

| Name  |
|---|
|  cognos-setup                        |
|  cognos-setup                        |
|  cognos-configure-update             |
|  cognos-configure                    |
|  cognos-configure                    |
|  cogconf                             |
|  cognos-setup-update                 |
|  cognos-setup                        |
|  BI-Customization                    |
|  bin                                 |
|  configurationTemplate               |
|  g11n                                |
|  lib                                 |
|  MetricsPkg                          |
|  models                              |
|  Transformer-Customization           |
|  up_bisrvr_winx64h_10.1.6235.1007_ml |

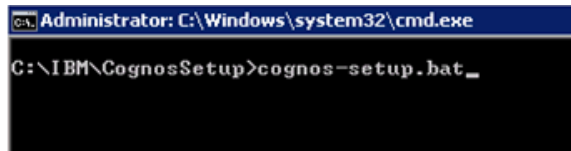
7. Copy the following DB2 jar files from DB2 Server to the C:\IBM\CognosSetup\BI-Customization\JDBC directory.
  - db2jcc.jar
  - db2jcc\_license\_cu.jar
8. Go to C:\IBM\CognosSetup folder and prepare the cognos-setup.properties. Enter the following values:

| Name                            | value   |
|---------------------------------|---|
| was.install.path                | C:\IBM\WebSphere\AppServer                    |
| was.profile.name                | AppSrv01                                      |
| was.local.admin                 | wsadmin                                       |
| was.local.admin.password        | wsadmin                                       |
| was.fqdn.hostname               | cog-srv01.itso.ibm.com                        |
| cognos.was.node.name            | lo2w04-w7Node01                               |
| cognos.was.server.name          | cognos_server                                 |
| cognos.biserver.issetup         | C:\SOFTWARE\bisrvr_win64\winx64h\issetup.exe  |
| cognos.transformer.issetup      | C:\SOFTWARE\bitrsfrmr_win32\win32\issetup.exe |
| cognos.biserver.install.path    | C:\IBM\Cognos64                               |
| cognos.transformer.install.path | C:\IBM\Cognos                                 |
| cognos.locale                   | EN  |
| cognos.contextroot              | cognos  |
| cognos.admin.username           | domadmin                                      |
| cognos.admin.password           | itsoadmin                                     |
| cognos.contextroot              | cognos  |
| cognos.namespace                | IBMConnections                                |
| cognos.cube.path                | C:\IBM\CognosShare                            |
| cognos.db.type                  | db2   |
| cognos.db.host                  | con-db201.itso.ibm.com:50001                  |
| cognos.db.name                  | COGNOS  |
| cognos.db.user                  | db2inst1                                      |
| cognos.db.password              | db2inst1                                      |
| metrics.db.type                 | db2   |
| metrics.db.host                 | con-db201.itso.ibm.com:50001                  |
| metrics.db.name                 | METRICS                                       |
| metrics.db.user                 | db2inst1                                      |
| metrics.db.password             | db2inst1                                      |

**Note:**

- ▶ *cognos.admin.username* must be a valid LDAP user for Cognos administrator.
- ▶ Password is removed from *cognos-setup.properties* after the configuration task is run. You can supply a password from command line.
- ▶ *cognos.cube.path* is a shared folder to access the reports in case of Cognos server is running in multiple node.

9. Run the *cognos-setup.bat* to set up the Cognos BI server. Upon completion, the logs are stored at *cognos-setup.log*. If there are any error occurs, correct the value and re-run the task again.



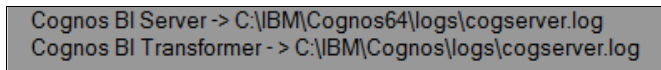
```
Administrator: C:\Windows\system32\cmd.exe
C:\IBM\CognosSetup>cognos-setup.bat _
```

10. Run the *cognos-configure.bat* to configure the Cognos BI Server. The log file *cognos-config.log* is created in the same directory. If there are any error occurs while running the *cognos-configure.bat*, fix the errors and run it again.



```
Administrator: Command Prompt
C:\IBM\CognosSetup>cognos-configure.bat -was.local.admin.password=wsadmin -cognos.admin.password=itsoadmin -cognos.db.password=db2inst1 -metrics.db.password=db2inst1 _
```

11. The Cognos BI Server and Transformer logs are stored in the following directory.



```
Cognos BI Server -> C:\IBM\Cognos64\logs\cogserver.log
Cognos BI Transformer -> C:\IBM\Cognos\logs\cogserver.log
```

12. Cognos configuration is completed successfully. Start the server after federating Cognos BI server into the Deployment Manager running on *con-dmgr.itso.ibm.com*.

## 6.7.6 Federating Cognos BI Server to the Deployment Manager

1. Make sure that the Deployment Manager is accessible from Cognos BI Server.
2. Run the following command to add the Cognos node into the Deployment Manager.  

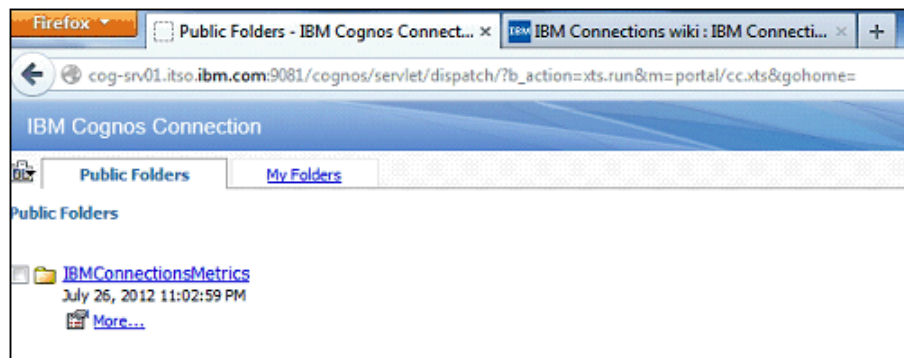
```
C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin>addNode.bat
con-dmgr-itso.ibm.com 8879 -username domadmin -password itsoadmin -includeapps
```
3. After the Cognos node is federated, *nodeagent* is started on the Cognos BI Server.
4. Synchronize the Cognos node to the deployment manager (DMGR).
5. Log into the Deployment Manager with user ID *domadmin*.
6. Go to **System Administration** → **Nodes**.
7. Select the Cognos node, *lo2w04-w7Node01* in our example, and click **Synchronize**.
8. Start the *cognos\_server* application server.

## 6.7.7 Validating Cognos BI Server

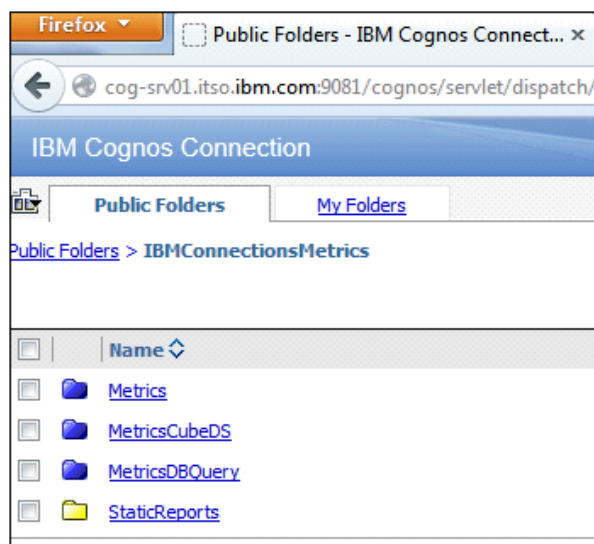
1. Enter the following URL to validate Cognos Content Store.  
<http://cog-srv01.itso.ibm.com:9081/cognos/servlet>



2. Enter the following URL to validate the Cognos BI Dispatcher  
<http://cog-srv01.itso.ibm.com:9081/cognos/servlet/dispatcher/>



3. Click the IBMConnectionsMetrics folder, the following sub-folders are displayed.

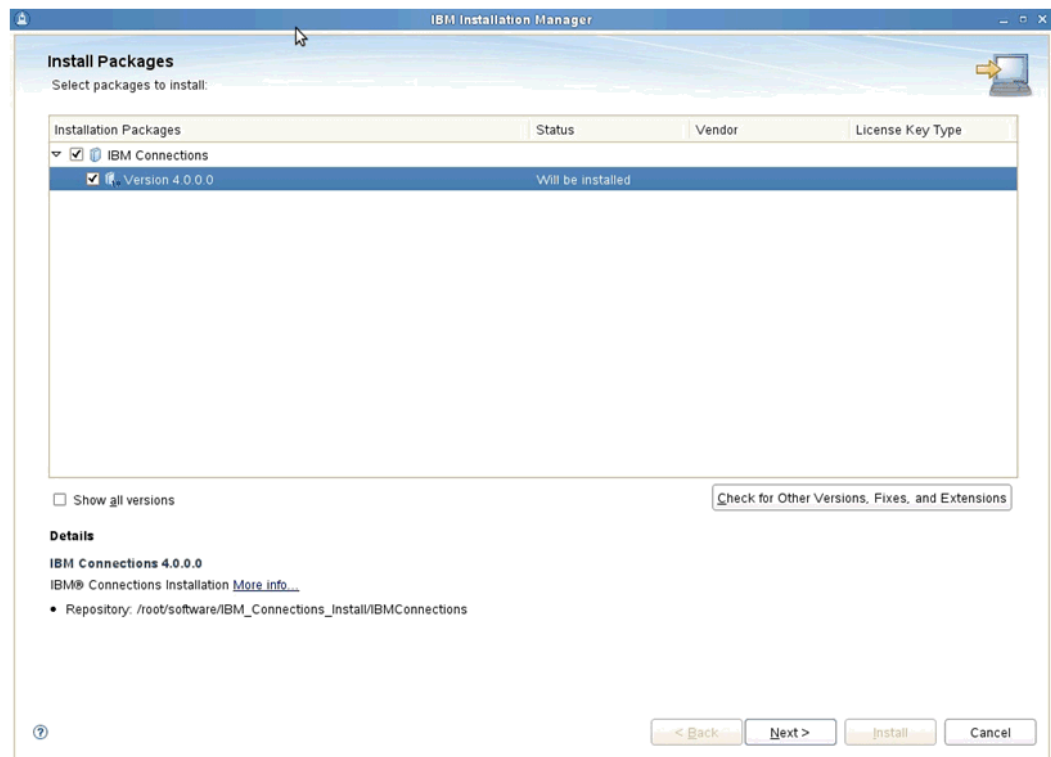


## 6.8 Installing IBM Connections applications

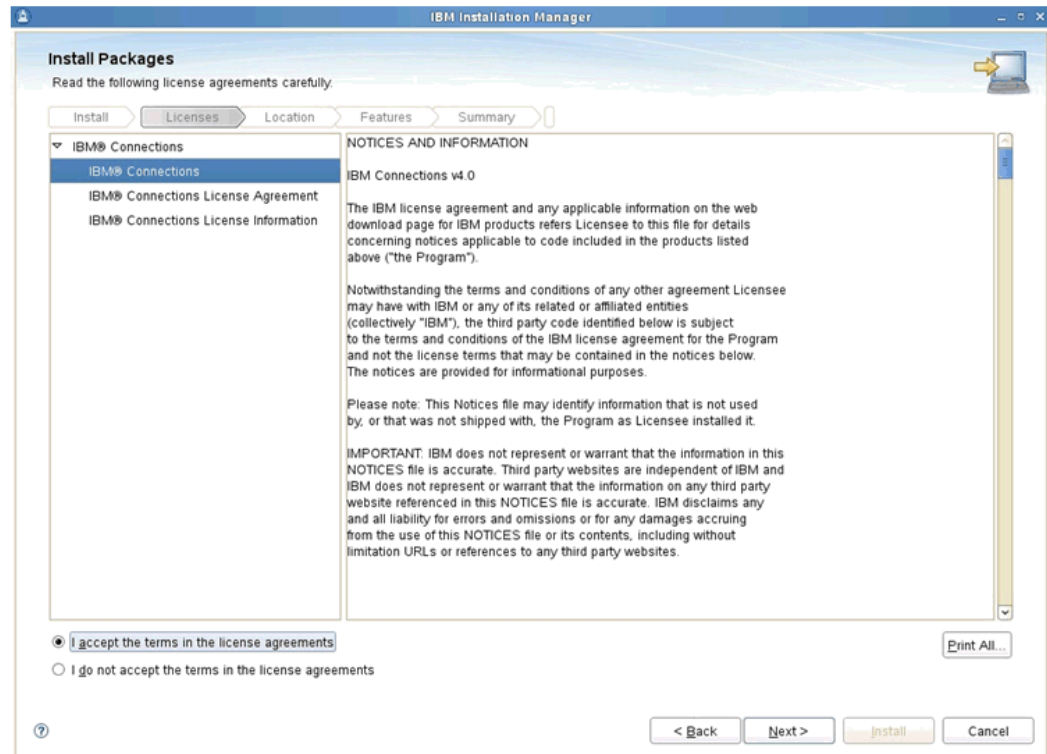
In this section, we describe the IBM Connections installation. Before installing IBM Connections, you must complete the preinstallation steps described in

You can use Installation Manager (6.1, “Setting up the Installation Manager” on page 52) to install IBM Connections and update the packages. Complete these steps to install IBM Connections 4:

1. Start the Installation Manager by running **/opt/IBM/InstallationManager/eclipse/launcher** on Deployment Manager server. Ensure that the IBM Connections version 4.0.0.0 is selected.

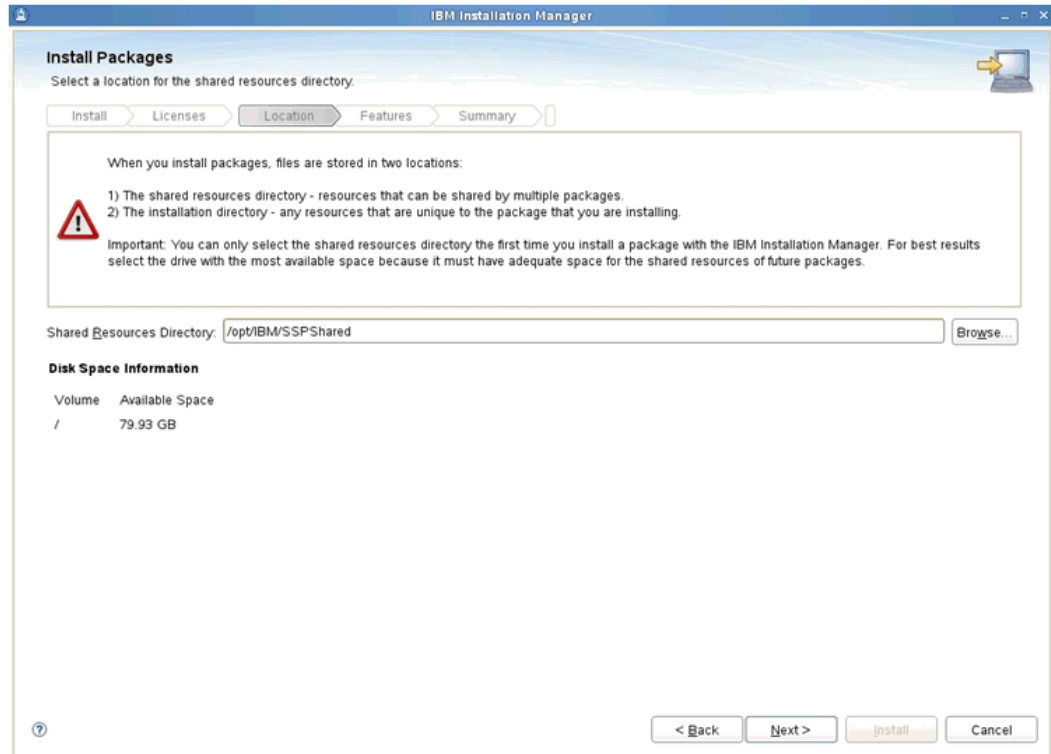


2. Read the notice and information, license agreement, and License information, select **I accept the terms in the license agreements**.

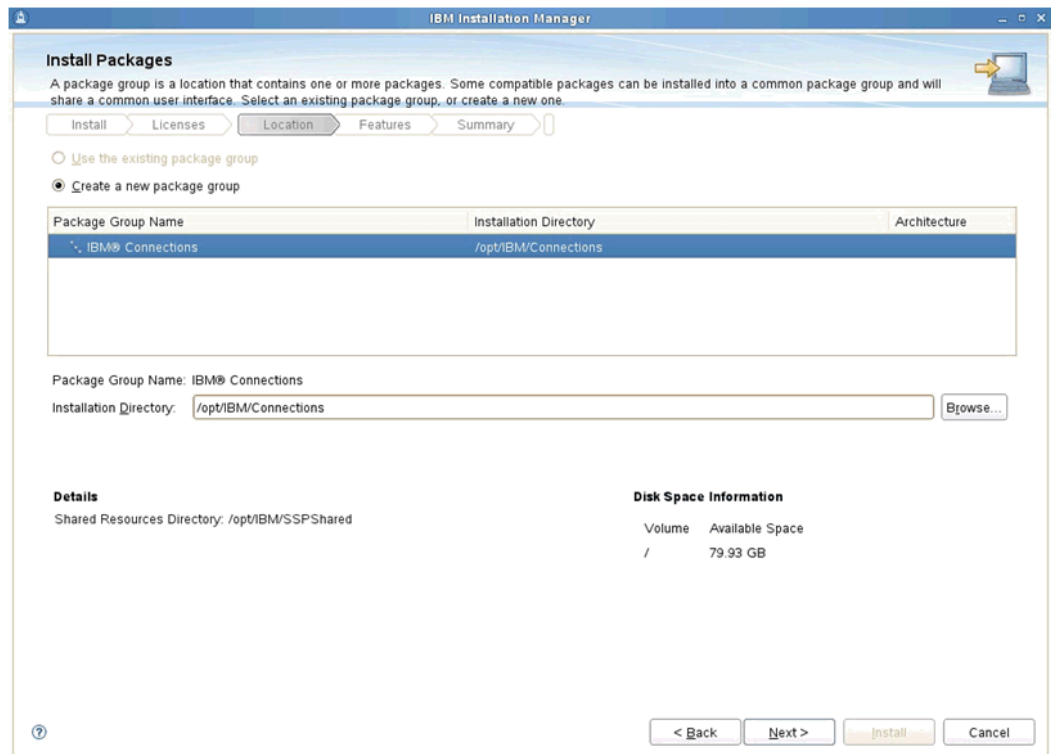


3. Define the shared resources directory.

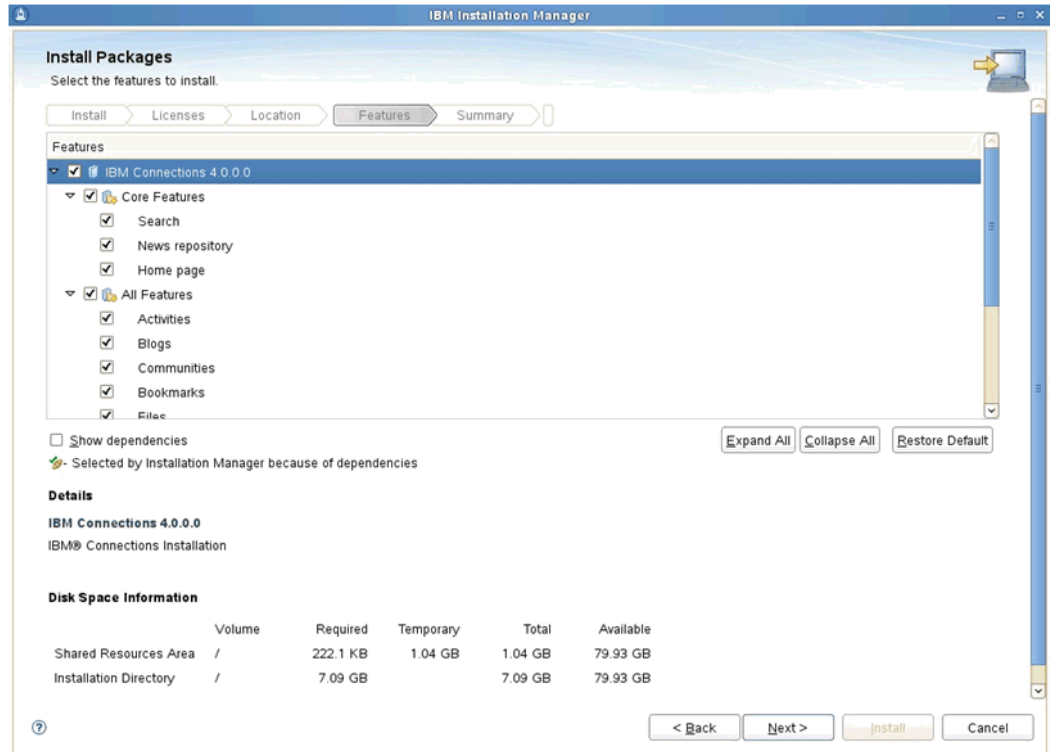
**Note:** For medium and large environments that have more than one WebSphere Application Server, the shared resources directory must be a shared file system (NFS, shared drive for Windows) because all IBM Connections libraries are installed on these directory. In our lab, it is /opt/IBM/SSPShared.



4. Select the location where the IBM Connections binary files will be installed.



5. Select the features that will be installed on your environment.



6. IBM Connections installation wizard starts the checking process to verify if the pre-requirement components (WebSphere, database, Cognos, and the setup environment) are correctly defined. The first component to be check is the WebSphere Application Server. You must provide the information bellow for verification:

- *Installation location:* Provide the WebSphere Application Server location.
- *Deployment Manager profile:* The profiles are loaded automatically. Select the Deployment Manager profile (Dmgr01).
- *Host name:* Provide the Deployment Manager host name using full qualified domain name (FQDN), for example, con-dmgr.itso.ibm.com.
- *Administrator user ID:* Provide the user id configured on WebSphere Application Server (domadmin).
- *Administrator password:* Pprovide de password for Administrator user.

Click **Validate** to check the information provided. The validation successful message is shown in another window.



**Install Packages**  
Fill in the configurations for the packages.

Install | Licenses | Location | **Features** | Summary

**Common Configurations**

- WebSphere
- Topology
- Database
- Cognos
- Content Store
- Notification

**WebSphere Application Server Selection**

Installation location:  
/opt/IBM/WebSphere/AppServer

Deployment manager profile:  
Dmgr01

Host name:  
con-dmgr.itso.ibm.com

**Deployment Manager Credentials**

These credentials must exist for the selected Profile.

Administrator user ID:  
domadmin

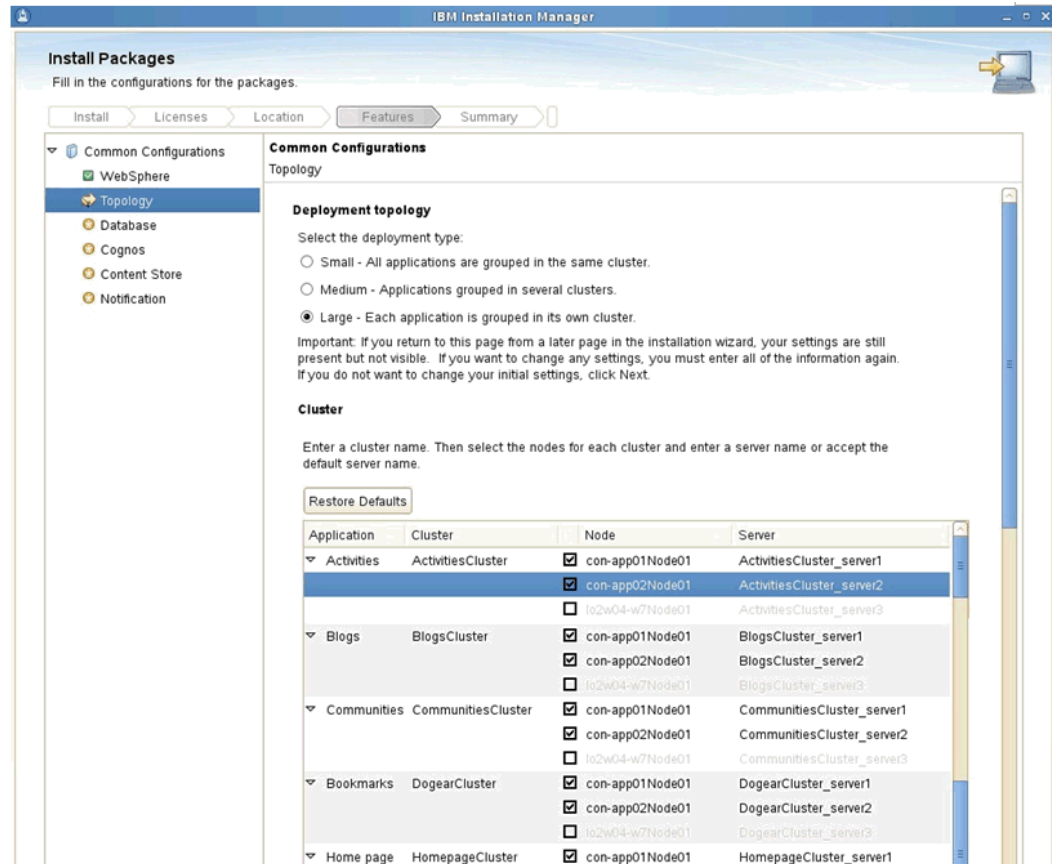
Administrator password:  
\*\*\*\*\*

SOAP port number:  
8879

Validate credentials before proceeding.

< Back | Next > | Install | Cancel

7. Select the topology for installation. For each application, select the servers that will be part of the cluster. On our lab, we used the large topology where all applications have their own cluster. We mark con-app01Node01 and con-app02Node01 for all applications.



8. Defining IBM Connections database. On our lab, we use DB2 database to store all the IBM Connections information. Provide the database information:

- *Database Type*: Select DB2 Universal Database(TM)
- *Database server host name*: provide the DB2 host name using FQDN (con-db201.itso.ibm.com)
- *Port*: provide the TCP port configured on DB2 (50001)
- *JDBC driver location*: provide the JDBC driver location. (/usr/ibmdb2/V9.7/java)

**Note:** JDBC driver must exist on all WebSphere Application Server servers at the same place.

**Install Packages**  
Fill in the configurations for the packages.

Install | Licenses | Location | **Features** | Summary

**Common Configurations**

- WebSphere
- Topology
- Database**
- Cognos
- Content Store
- Notification

**Common Configurations**  
Database

**Database Location**

Are all IBM Connections applications using the same database instance?

☒ Yes, the applications are on the same database instance.

☐ No, the applications are not on the same database instance.

Important: If you return to this page from a later page in the installation wizard, your settings are still present but not visible. If you want to change any settings, you must enter all of the information again. If you do not want to change your initial settings, click Next.

**Database Type**

Database type:

DB2 Universal Database(TM)

**Database Server Information**

Database server host name:

con-db201.itso.ibm.com

Port:

50001

JDBC driver location:

/opt/ibm/db2/V9.7/java

Browse

**Application Database Information**

☒ Use the same password for all applications.

| Application | Database Name | User ID | Password |
|-------------|---------------|---------|----------|
| Activities  | OPNACT        | LCUSER  | *****    |
| Blogs       | BLOGS         | LCUSER  | *****    |

< Back | Next > | Install | Cancel

9. On the database definition, select **Use the same password for all applications**, and click **Validate** to confirm if the information provided on steps 8 and 9 are defined correctly. The validation successful information is shown in a pop-up window.

| Application | Database Name | User ID | Password |
|-------------|---------------|---------|----------|
| Activities  | OPNACT        | LCUSER  | *****    |
| Blogs       | BLOGS         | LCUSER  | *****    |
| Communities | SNCOMM        | LCUSER  | *****    |
| Bookmarks   | DOGEAR        | LCUSER  | *****    |
| Metrics     | METRICS       | LCUSER  | *****    |
| Mobile      | MOBILE        | LCUSER  | *****    |
| Files       | FILES         | LCUSER  | *****    |
| Forums      | FORUM         | LCUSER  | *****    |
| Home page   | HOMEPAGE      | LCUSER  | *****    |
| Profiles    | PEOPLEDDB     | LCUSER  | *****    |
| Wikis       | WIKIS         | LCUSER  | *****    |

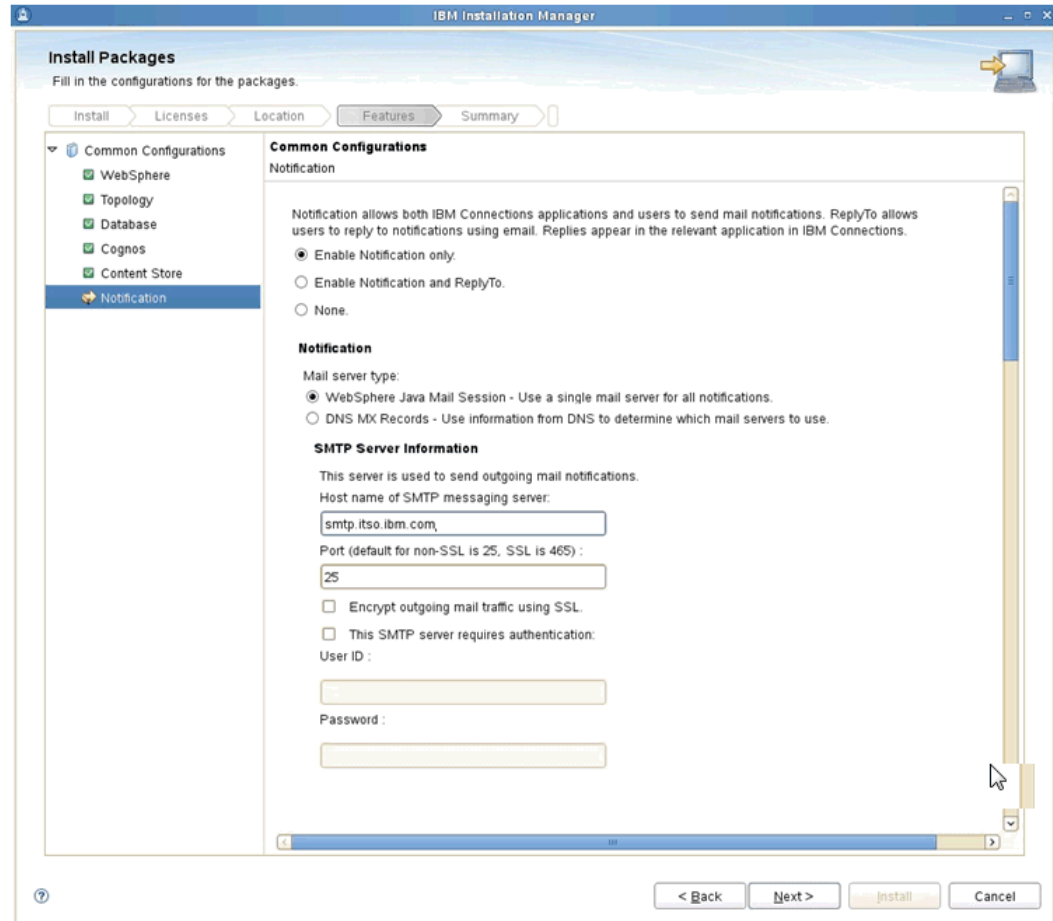
Validate

10. On Cognos configuration step, provide the information from Cognos server installation. We enter the information from 6.7, "Installing Cognos Business Intelligence" on page 102.
- *Administrator user ID*: Provide the Cognos user ID (cogadmin).
  - *Administrator password*: Provide the password for the Administrator user ID.

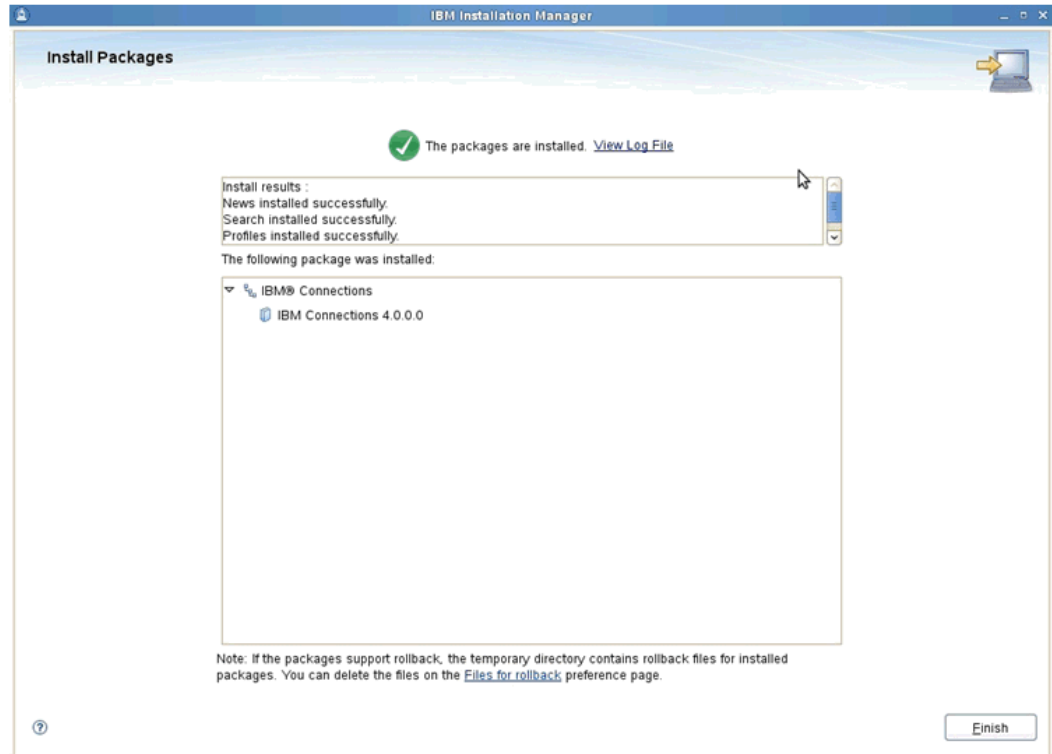
In **Node** section, click on **Load node info button** and select the WebSphere Application Server node where the Cognos was installed (**IO2w04-w7Node01**). Select the server name from Cognos Server (**cognos\_server**) and provide the web context root from Cognos (**cognos**). Click **Validate**. After receiving the Success Validation message. click **Next** to continue.

The screenshot shows the 'IBM Installation Manager' window with the 'Install Packages' tab selected. The 'Common Configurations' section is expanded, showing the 'Cognos' configuration. The 'Cognos Credentials' section has fields for 'Administrator user ID' (cogadmin) and 'Administrator password' (masked). The 'Node' section has fields for 'Name' (IO2w04-w7Node01), 'Host name' (IO2w04-w7), 'Server name' (cognos\_server), 'Port' (9081), and 'Web context root' (cognos). A 'Load node info' button is next to the 'Name' field. A 'Validate' button is at the bottom of the 'Node' section. At the bottom of the window are buttons for '< Back', 'Next >', 'Install', and 'Cancel'.

11. On Common Configurations, you can enable the notifications to allows IBM Connections to send e-mail. On our lab environment, we just define the notifications by providing the following information:
- Mark **Enable Notification only**.
  - *Mail server type*: Select **WebSphere Java Mail Session - Use a single mail server for all notifications**.
  - *Host name of SMTP messaging server*: Provide the host name of the SMTP (Simple Mail Transport Protocol) server (smtp.itso.ibm.com).
  - *Port*: Provide de TCP port from the SMTP server (25).



12. Check if your IBM Connections was installed successfully and click **Finish**.



## 6.9 Installing IBM HTTP Server

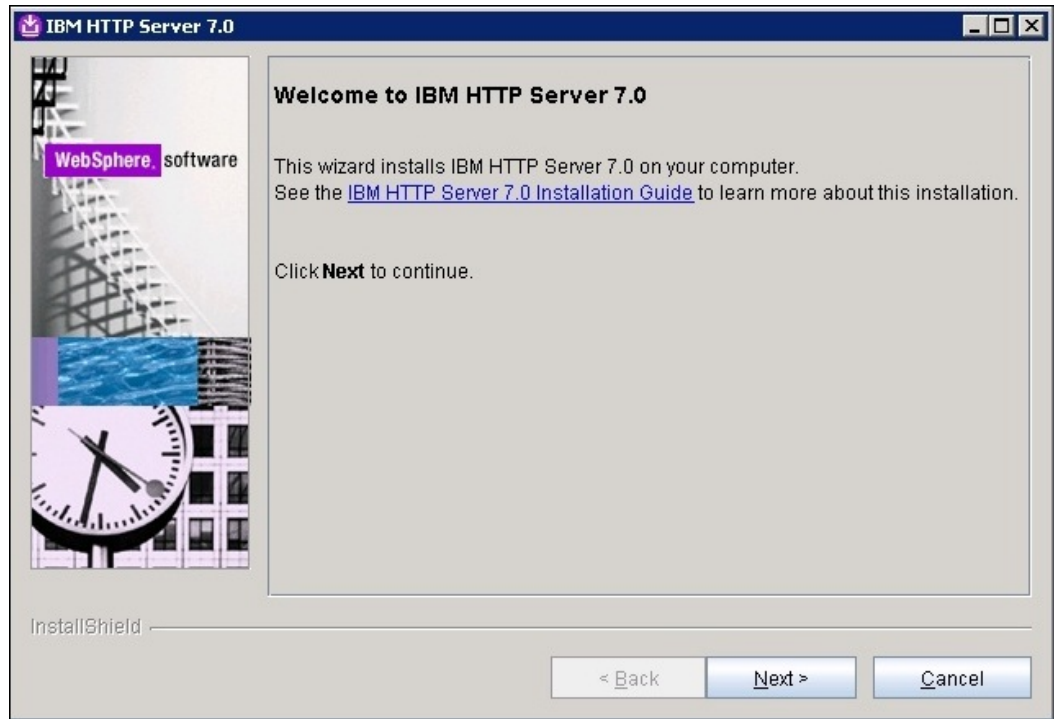
IBM Connections 4 requires a front-end web server to access the IBM Connections 4 functions. IBM WebSphere Application Server bundles the IBM HTTP Server and WebSphere Plugin on the supplemental packages. The WebSphere Plugin forwards the HTTP requests from web server (IBM HTTP Server) to the application on WebSphere Application server and provides the secure connection (HTTP over SSL) and high availability for the applications cluster.

In this section, we describe the procedure to install, configure, and federated IBM HTTP Server on a WebSphere Application Server Network Deployment server.

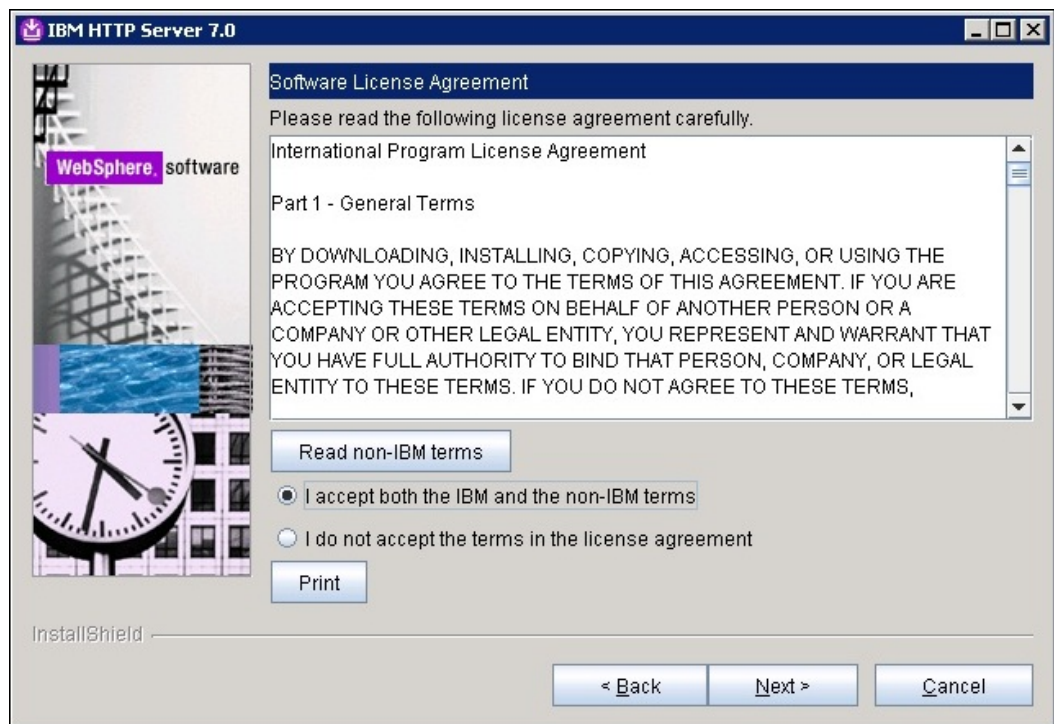
### 6.9.1 Installing IBM HTTP Server

Follow these steps to install IBM HTTP Server:

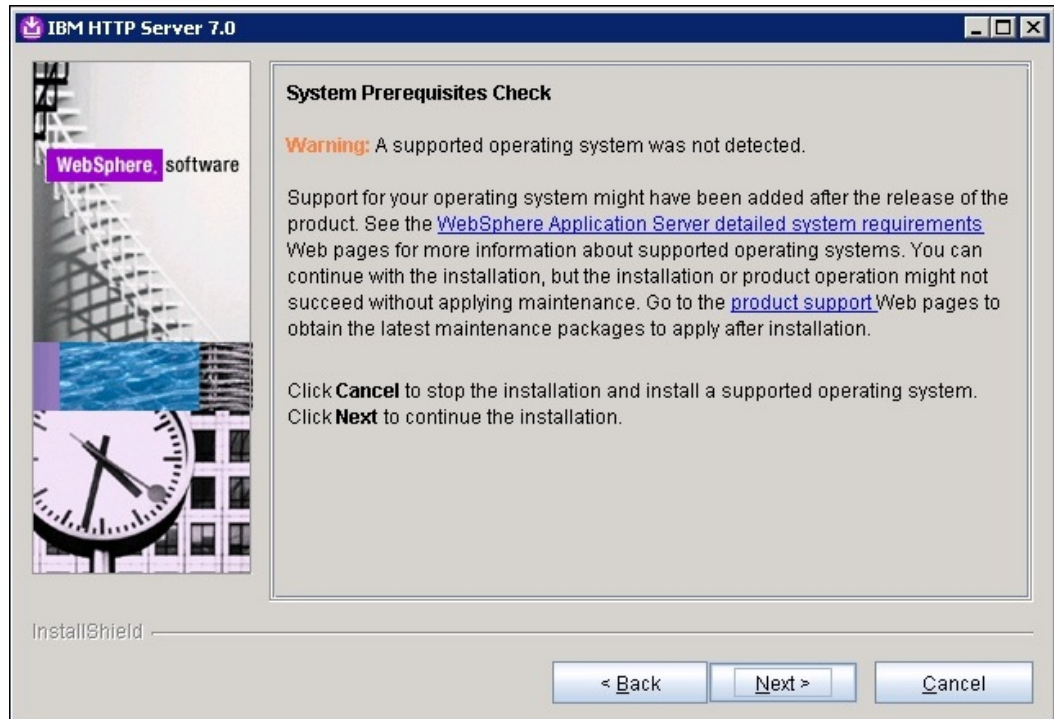
1. Unzip the WebSphere Supplementals source on a temporary directory ( for example, c:\temp) and run **install** on the *IHS directory* to launch the installation wizard.



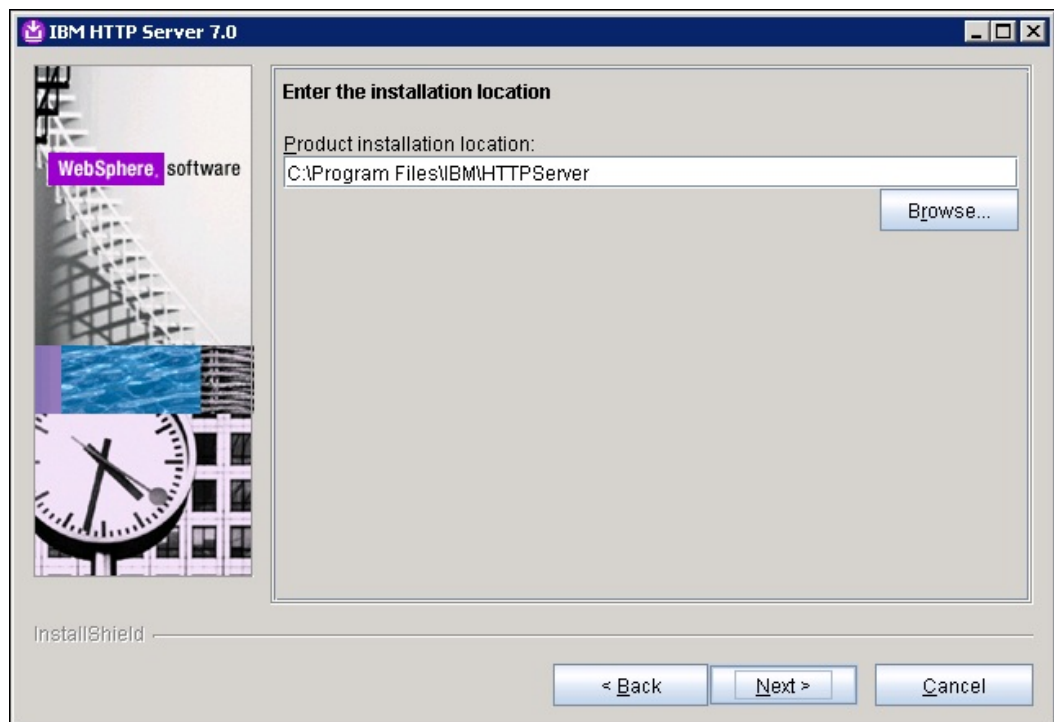
2. On the Software License Agreement read and select **I accept both the IBM and the non-IBM terms**.



3. The wizard checks the system prerequisites requirements on your server. If the operating system is added to the supported system list after the product was released, you might receive the following message. Click **Next** to continue.

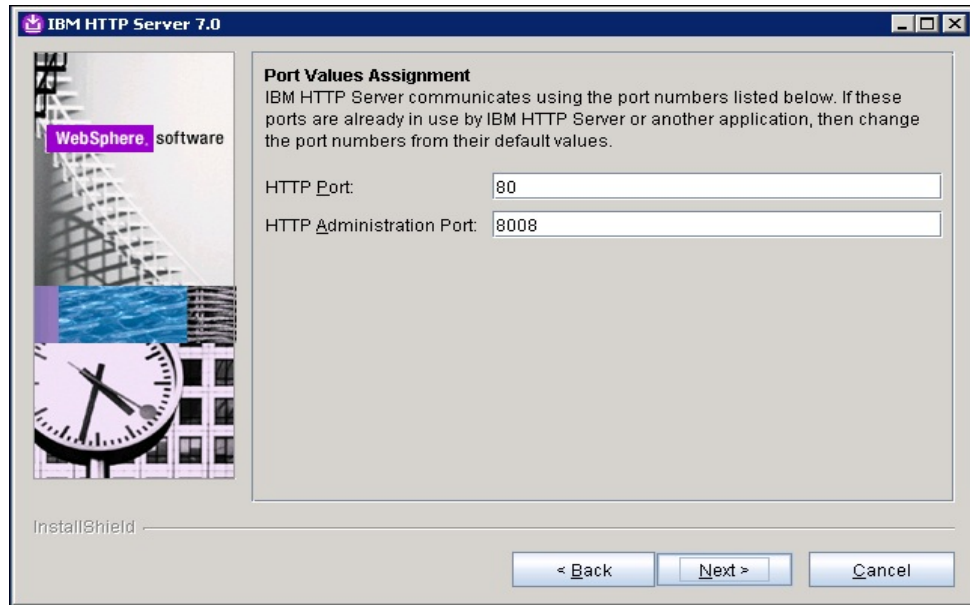


4. Select the directory to install the product. The default directory is shown. We recommend removing Program Files and making the path shorter, e.g. C:\IBM\HTTPServer

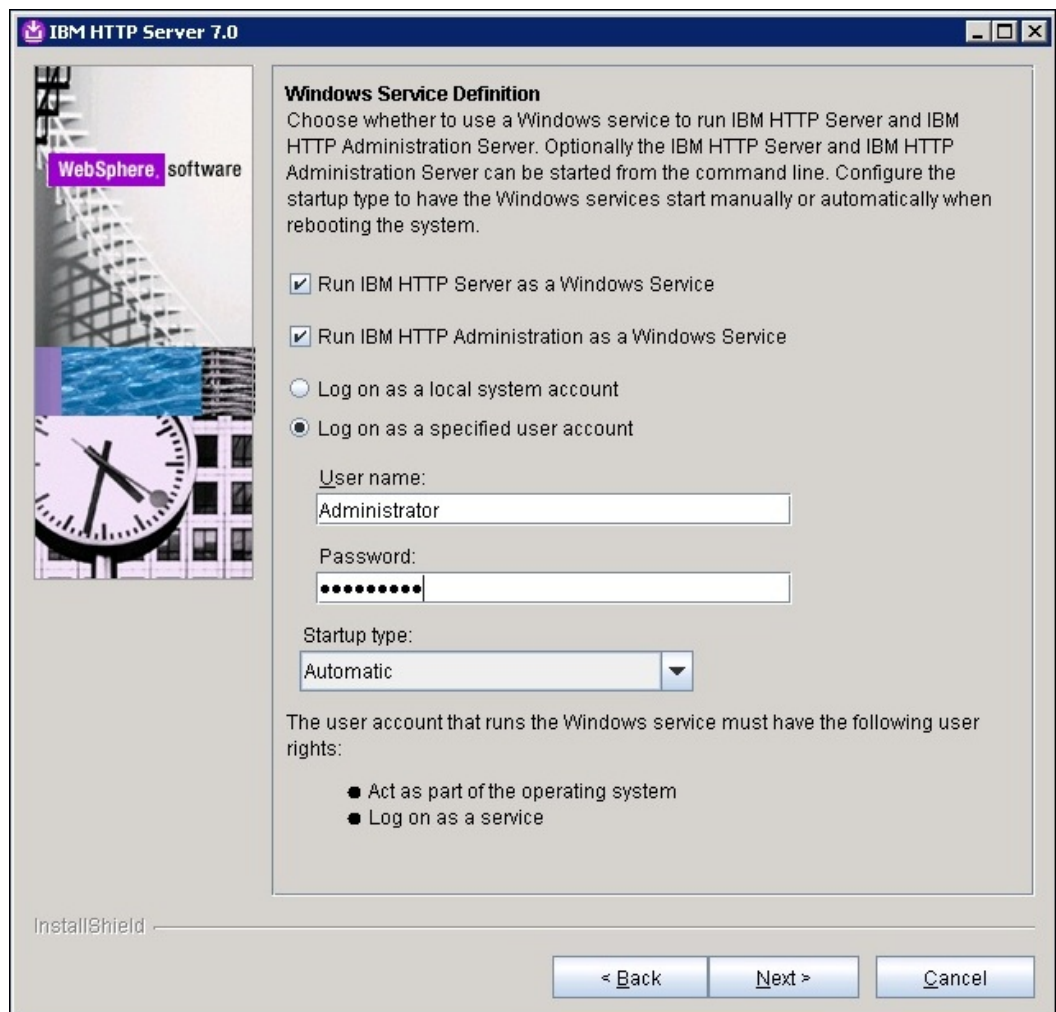


5. You can choose the TCP port to be used by IBM HTTP Server and Administration, leave the default option.





6. Select both options to run IBM HTTP Server and IBM HTTP Server Administration as Windows services, and define an account name and password to start the process.



7. The IBM HTTP Server Administration user ID is for managing the IBM HTTP Server over the WebSphere Integrated Console Solution (ISC). Select the option to have the installer create the ID.

**IBM HTTP Server 7.0**

WebSphere software

### HTTP Administration Server Authentication

Create a user ID and password to authenticate to the IBM HTTP Server administration server using the WebSphere Application Server administrative console. The newly-created user ID and password is encrypted and stored in the `conf/admin.passwd` file. You can create additional user IDs after the installation by using the `htpasswd` utility.

☒ Create a user ID for IBM HTTP Server administration server authentication.

User ID:

Password:

Confirm Password:

InstallShield

< Back    Next >    Cancel

8. Select install the **IBM HTTP Server Plug-in for IBM WebSphere application Server** to create plug-in configuration file. Define the web server name and host name from IBM HTTP Server.

**IBM HTTP Server 7.0**

WebSphere software

### IBM HTTP Server Plug-in for IBM WebSphere Application Server

Silently install the plug-in using the remote installation scenario. The host name and web server definition are used when creating the default plug-in configuration file. This file is used to route requests to the Application Server. If there are multiple Application Servers, then select one of the servers and specify the machine's host name.

☒ Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server

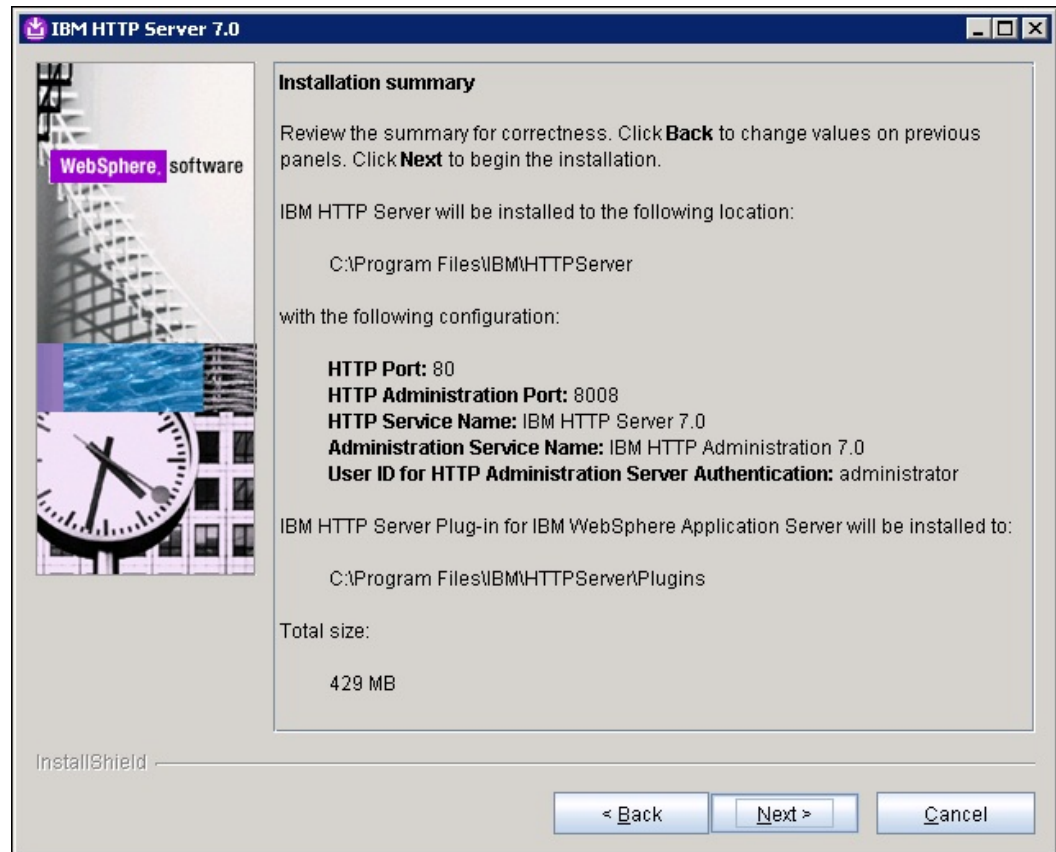
Web server definition:

Host name or IP address for the Application Server:

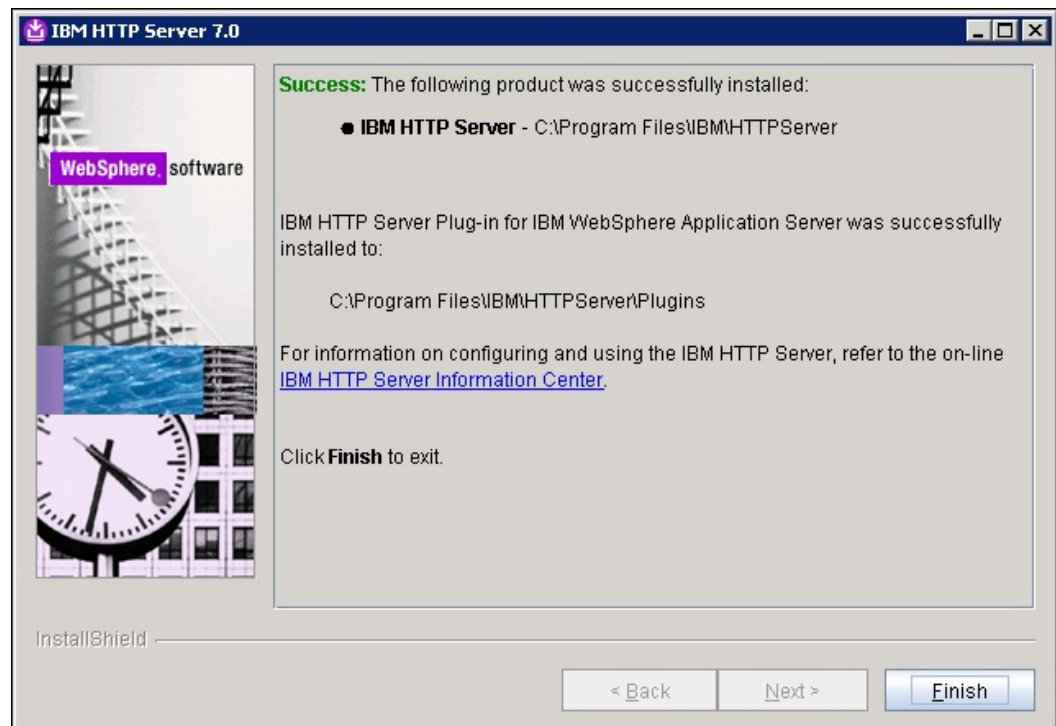
InstallShield

< Back    Next >    Cancel

9. Validate if all parameters defined are correct, and click **Next** to continue the installation.



10. The installation wizard shows that both IBM HTTP Server and Plug-in are installed successfully.

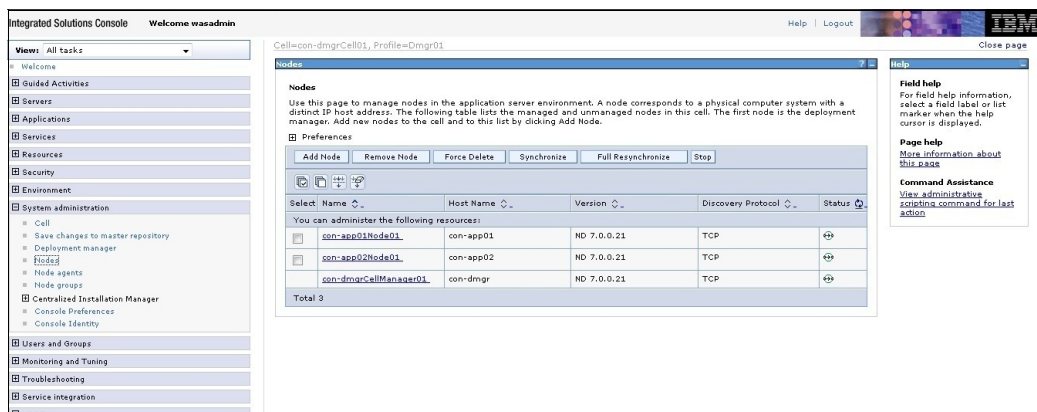


After the IBM HTTP Server is installed, you must apply the latest fix pack. See the fix pack installation procedure in 6.4, “Installing WebSphere Application Server” on page 70.

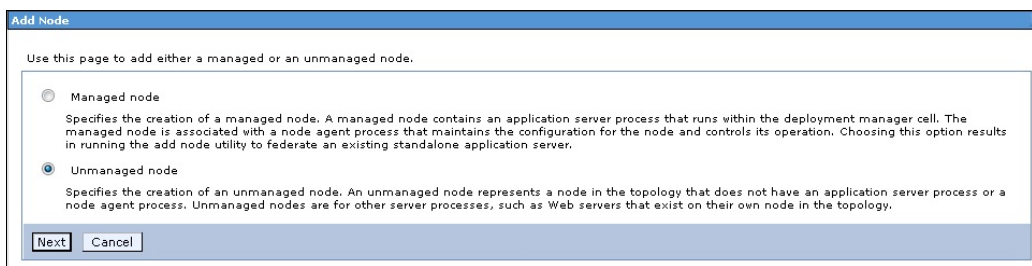
## 6.9.2 Federating IBM HTTP Server on WebSphere Application Server

You must add the new installed IBM HTTP Server as an unmanaged node on a WebSphere Application Server Deployment Manager server to manage the IBM HTTP Server from the Integrated Solutions Console, creating a single point of administration for your environment. Complete the following steps to add an IBM HTTP Server on a WebSphere Application Server Deployment Manager server:

1. Access the Integrated Solutions Console <https://:9043/ibm/console/> on a web browser. On the left menu under System administration, choose **Nodes** then click **Add Node**.



2. Select **Unmanaged node** and click **Next**.



3. Define the the following parameters, and click **OK**.
  - **Name:** This value is to identify the unmanaged server on the Integrated Solutions Console.
  - **Host Name:** Enter the full qualified domain name (FQDN) of the node to be added.
  - **Platform Type:** Enter the platform type where the node was installed.

**Nodes**

**Nodes > New**

Use this page to view or change the configuration for an unmanaged node. An unmanaged node is a node defined in the cell topology that does not have a node agent running to manage the process. Unmanaged nodes are typically used to manage Web servers.

Configuration

**General Properties**

\* Name  
con-ihs01

\* Host Name  
con-ihs01.itso.ibm.com

\* Platform Type  
Windows

Apply OK Reset Cancel

The additional properties will not be available until the general properties for this item are applied or saved.

**Additional Properties**

■ Custom Properties

4. Verify if the node that you have added are listed on the Nodes on the Integrated Solutions Console. Click **Save** to save the configuration.

**Nodes**

☐ Messages

⚠ Changes have been made to your local configuration. You can:

- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

⚠ The server may need to be restarted for these changes to take effect.

**Nodes**

Use this page to manage nodes in the application server environment. A node corresponds to a physical computer system with a distinct IP host address. The following table lists the managed and unmanaged nodes in this cell. The first node is the deployment manager. Add new nodes to the cell and to this list by clicking Add Node.

☐ Preferences

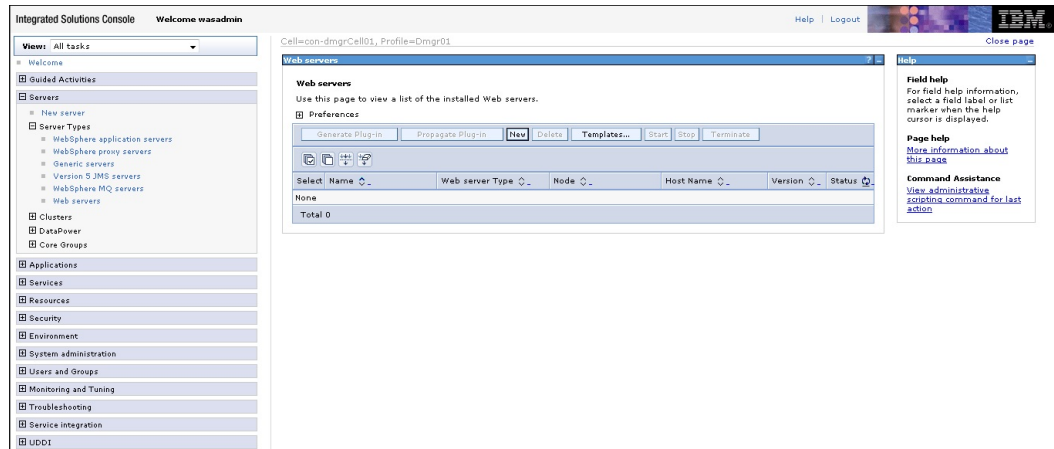
Add Node Remove Node Force Delete Synchronize Full Resynchronize Stop

| Select                                      | Name                                  | Host Name              | Version        | Discovery Protocol | Status |
|---|---------------------------------------|------------------------|----------------|--------------------|--------|
| You can administer the following resources: |                                       |                        |                |                    |        |
| <input type="checkbox"/>                    | <a href="#">con-app01Node01</a>       | con-app01              | ND 7.0.0.21    | TCP                | ↔      |
| <input type="checkbox"/>                    | <a href="#">con-app02Node01</a>       | con-app02              | ND 7.0.0.21    | TCP                | ↔      |
| <input type="checkbox"/>                    | <a href="#">con-dmgrCellManager01</a> | con-dmgr               | ND 7.0.0.21    | TCP                | ↔      |
| <input type="checkbox"/>                    | <a href="#">con-ihs01</a>             | con-ihs01.itso.ibm.com | Not applicable | TCP                |        |
| Total 4                                     |                                       |                        |                |                    |        |

Repeat this the add node step to add additional nodes on the Integrated Solutions Console.

5. After you have added the node on WebSphere Application Server, add web servers on the servers management on the Integrated Solutions Console.
6. Under **Servers** on the left menu, expand **Server Types** and click **Web servers**. Click **New** to add the IBM HTTP Server on the console.





7. Choose the web server node to be added from the select node field drop-down list. The **Server name** is displayed for you. Select the corresponding web server type.

8. Select the web server template.

9. Enter the following properties for this web server:
  - **Port:** Enter the TCP port that web server is listening.
  - **Web server installation location:** Provide the location where the IBM HTTP Server was installed.
  - **Service name:** Inform the name of the IBM HTTP Server services on Windows.
  - **Plug-in installation location:** Provide the location where the Plug-in was installed.

- *Application mapping to the web server:* Select All to support the application mapping on WebSphere.
- *Administration Server Port:* Enter the TCP port for the Administration process.
- *Username:* Enter the name of the Administration user that you have defined during the IBM HTTP Server installation.
- *Password:* Enter the password defined.
- *Confirm Password:* Confirm the password.
- *Use SSL:* Do not check the SSL.

**Create new Web server definition**

Use this page to create a new Web server.

**Step 3: Enter the properties for the new Web server**

Enter the Web server properties.

- \* Port: 80
- \* Web server installation location: C:\Program Files\IBM\HTTPServer
- \* Service name: IBMHTTPServer7.0
- \* Plug-in installation location: c:\Program Files\IBM\HTTPServer\Plugins
- Application mapping to the Web server: All

Enter the IBM Administration Server properties.

- \* Administration Server Port: 8008
- \* Username: wasadmin
- \* Password: .....
- \* Confirm password: .....
- ☐ Use SSL

Previous Next Cancel

10. Review the summary and click **finish** if the information provided is correct to complete the configuration process.

**Create new Web server definition**

Use this page to create a new Web server.

**Step 4: Confirm new Web server**

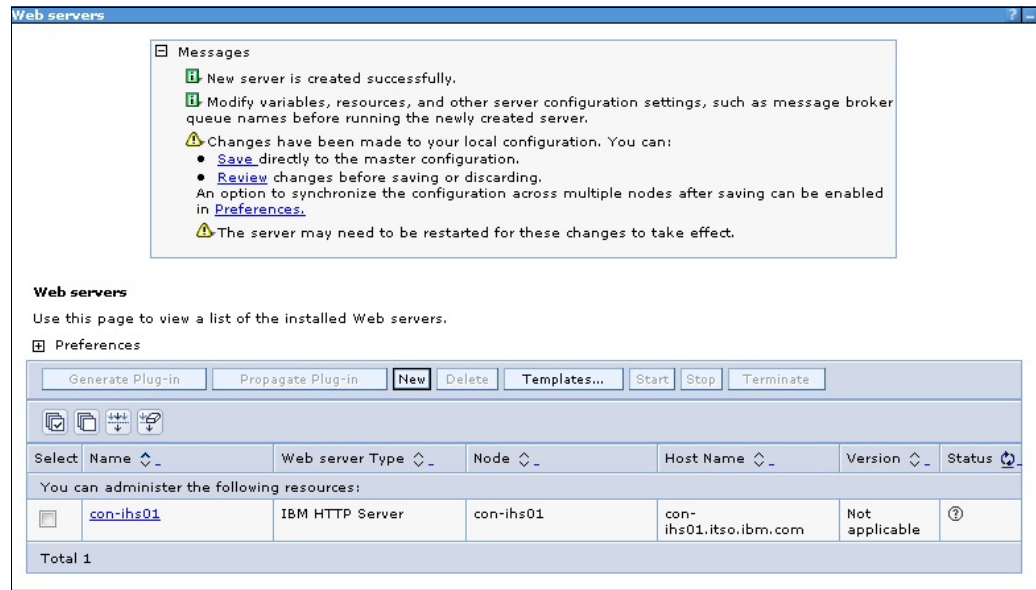
The following is a summary of your selections. Click the Finish button to complete the Web server creation. If there are settings you wish to change, click on Previous button to review the server settings.

Summary of actions:

- New Web server entry "con-ihs01" will be created on node "con-ihs01"
- Platform Type "Windows"
- Web server installation root "C:\Program Files\IBM\HTTPServer"
- Plug-in installation root "c:\Program Files\IBM\HTTPServer\Plugins"

Previous Finish Cancel

11. Confirm that you have the web server listed on the console and click **Save**.



Run this procedure for each additional web server on your environment.

You can now manage your IBM HTTP Server from the ISC.

## 6.10 Post installation environment configuration

After product installation, you can configure the IBM Connections environment. The configuration tasks including the following:

- ▶ Configuring IBM HTTP Server
- ▶ Setting the single sign-on domain for future integration
- ▶ Secure Sockets Layer encryption
- ▶ Setting the Java Virtual Machine heap size
- ▶ Creating additional administrator with the WebSphere Integrate Console Solution
- ▶ Configuring Cognos Business Intelligence

### 6.10.1 Configuring IBM HTTP Server

This section provides information about configuring HTTPS (HTTP protocol over SSL), mapping applications module to be used on web server, and redirecting your web server to IBM Connections applications.

#### Enabling SSL

In our example, we use self-sign certificate to enabling SSL. With SSL enabled, all the communications are encrypted and the connections between the client browsers and the web server are secured.

To enabling SSL on the IBM HTTP server, you must use the key management utility, iKeyman, to create a key for securing your network communication. This key is installed on IBM HTTP Server configuration file.

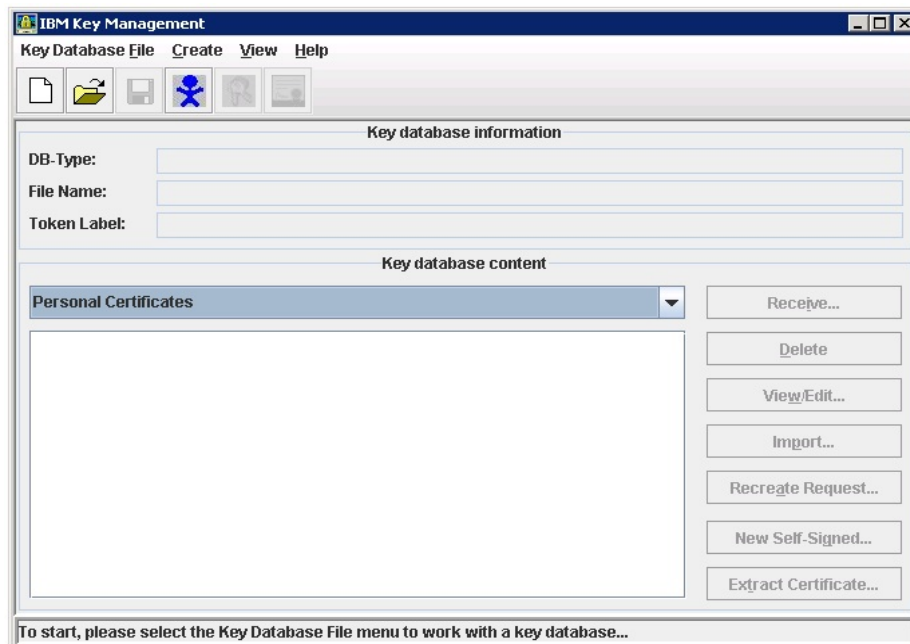


**Note:** For more information about enabling SSL on the IBM HTTP server, see WebSphere Application Server Information Center ([http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=%2Fcom.ibm.websphere.ihs.doc%2Finfo%2Fihs%2Fihs%2Fwelc\\_ikeymangui.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=%2Fcom.ibm.websphere.ihs.doc%2Finfo%2Fihs%2Fihs%2Fwelc_ikeymangui.html)).

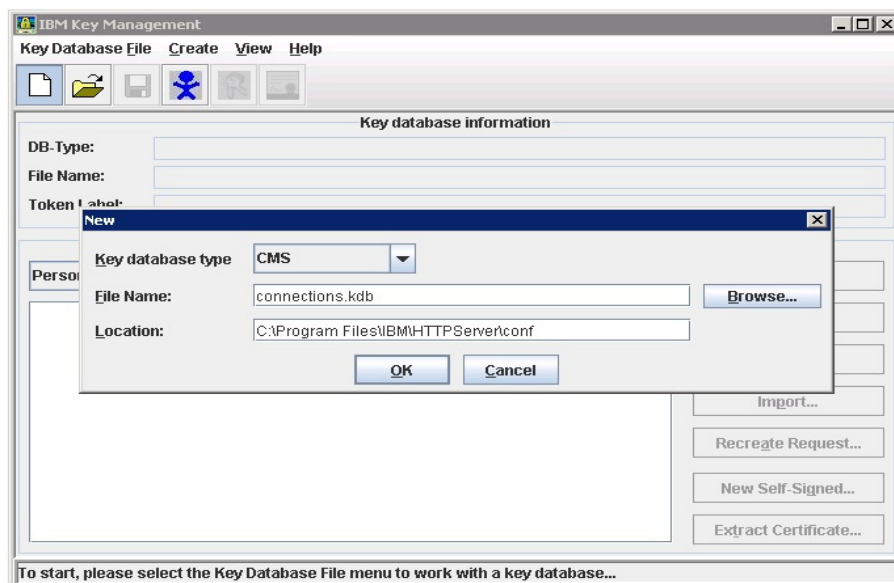
### Creating SSL key

Complete the following steps:

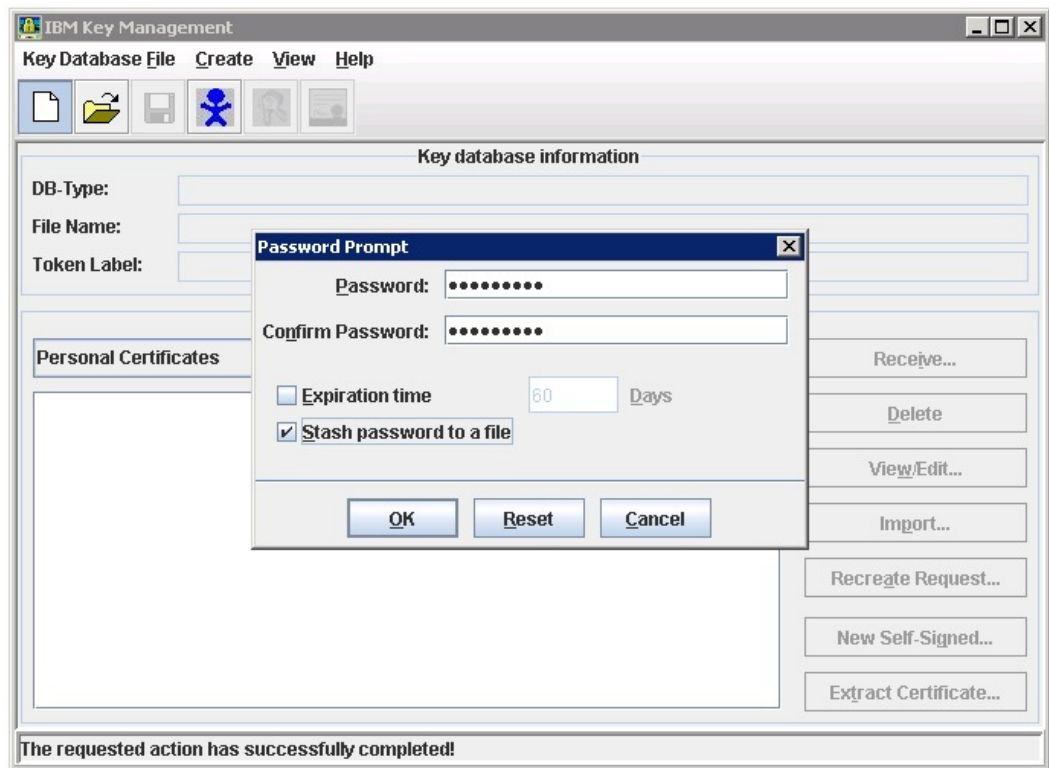
1. From the IBM HTTP Server installation directory, run `C:\IBM\HTTPServer\bin\ikeyman` to open the key management utility.



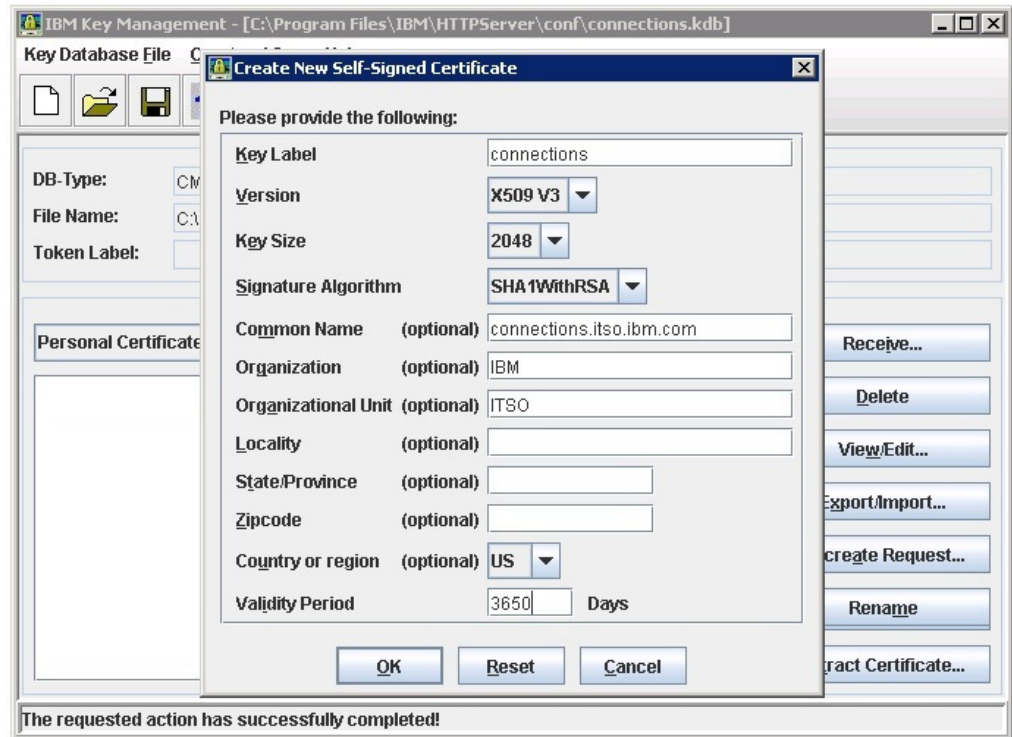
2. From the menu bar, select **Key Database File** → **New**. Select **CMS** for Key database type. Enter a name for the key file on **File Name** (connections.kdb) and the path on the **Location** (C:\Program Files\IBM\HTTPServer\conf).



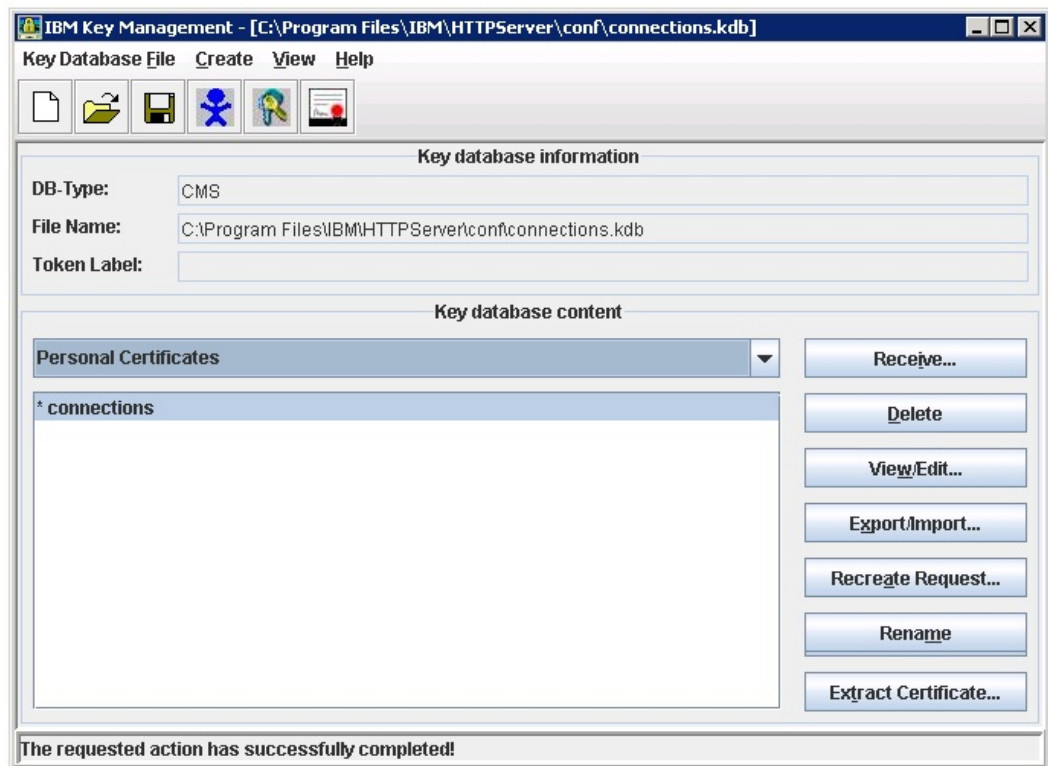
3. On the password prompt, define and confirm a password. Check **Stash password to a file**.



4. From menu bar, select **Create** → **New** → **Self- Sign Certificate** and fill the following options:
  - *Key Label*: Define a label to identify your certificate on the key file, for example, **connections**.
  - *Version*: Define the SSL version to **X509 V3**.
  - *Key Size*: Set the size to **2048**.
  - *Signature Algorithm*: Define the signature to **SHA1WithRSA**.
  - *Common Name*: Define the full qualified domain name (FQDN) that you choose to access your IBM Connections, for example, **connections.itso.ibm.com**.
  - *Organization Name*: Define the organization name, for example, **IBM**.
  - *Organization*: Define your unit, for example, **ITSO**.
  - *Country or region*: Select your country, for example, **US**.
  - *Validity period*: Set the days that the certificate is valid, for example, **3650** days.

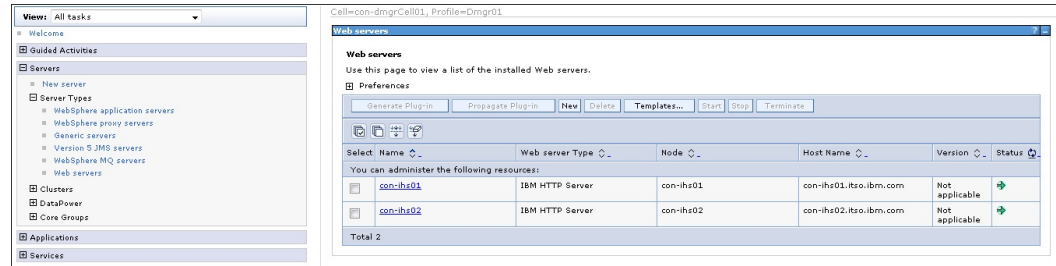


5. You have created an SSL key add to your IBM HTTP Server configuration file to secure your connection.

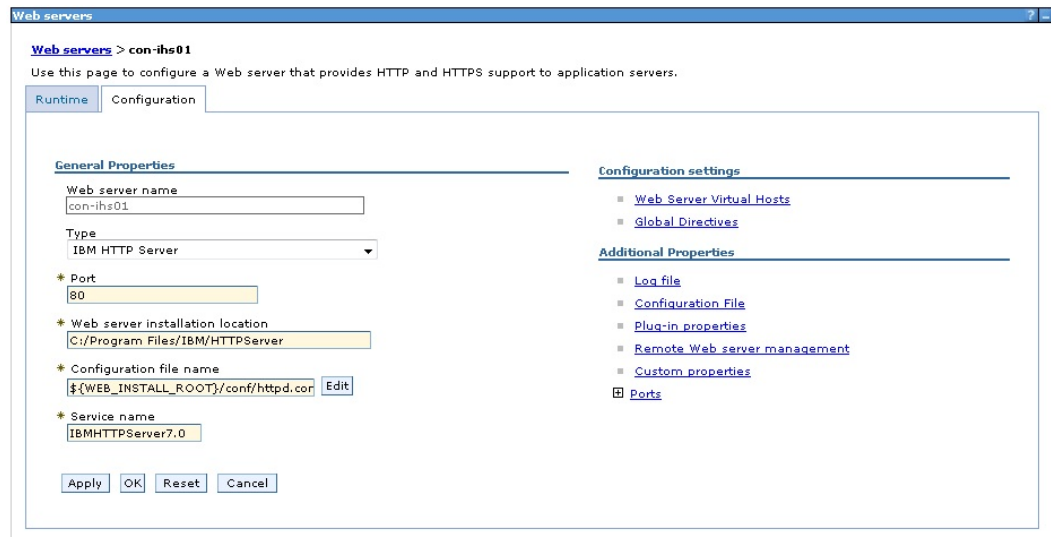


## Enabling HTTPS

1. On the WebSphere console, click **Servers** on the left menu and expand **Server Types**. Click **Web servers** and choose the server that you want to configure. In our example, it is **con-ih01**.



2. On Additional Properties, click **Configuration File** to edit the IBM HTTP Server configuration file.



3. Add the following lines before "LoadModule was\_app22\_module..." at the end of the file, and click **OK**.

---

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
```

```
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName server_name
SSLEnable
</VirtualHost>

</IfModule>
SSLDisable
Keyfile "path_to_key_file"
SSLStashFile "path_to_stash_file"
```

---

where

- **server\_name**: Host name of the IBM HTTP Server, for example, **con-ih01**

- *veyfile*:The path and the SSL key file that you create using the iKeyman utility, for example, **C:\IBM\HTTPServer\conf\connections.kdb**
- *SSLStashFile*:The path and the stash file that you associate the stash using the iKeyman utility, for example, **C:\IBM\HTTPServer\conf\connections.sth**

```

Configuration file

#
#
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so

<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443

<VirtualHost *:443>
    ServerName con-ih01

    SSLEnable
</VirtualHost>

</IfModule>

SSLDisable

Keyfile "C:\Program Files\IBM\HTTPServer\conf\connections.kdb"
SSLStashFile "C:\Program Files\IBM\HTTPServer\conf\connections.sth"

LoadModule was_ap22_module "C:\Program
Files\IBM\HTTPServer\Plugins\bin\32bits\mod_was_ap22_http.dll"
WebSpherePluginConfig "C:\Program Files\IBM\HTTPServer\Plugins\config\con-ih01
\plugin-cfg.xml"

```

4. Click **Save** to save the configuration.

Messages

⚠ Changes have been made to your local configuration. You can:

- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

⚠ The server may need to be restarted for these changes to take effect.

5. After finishing the configuration, you must restart the web server. Select the web server (**con-ih01**) that you edited and click **Stop**. Check if the server is down and then click **Start** to start the web server.

Web servers

Web servers

Use this page to view a list of the installed Web servers.

Preferences

Generate Plug-in

Propagate Plug-in

New

Delete

Templates...

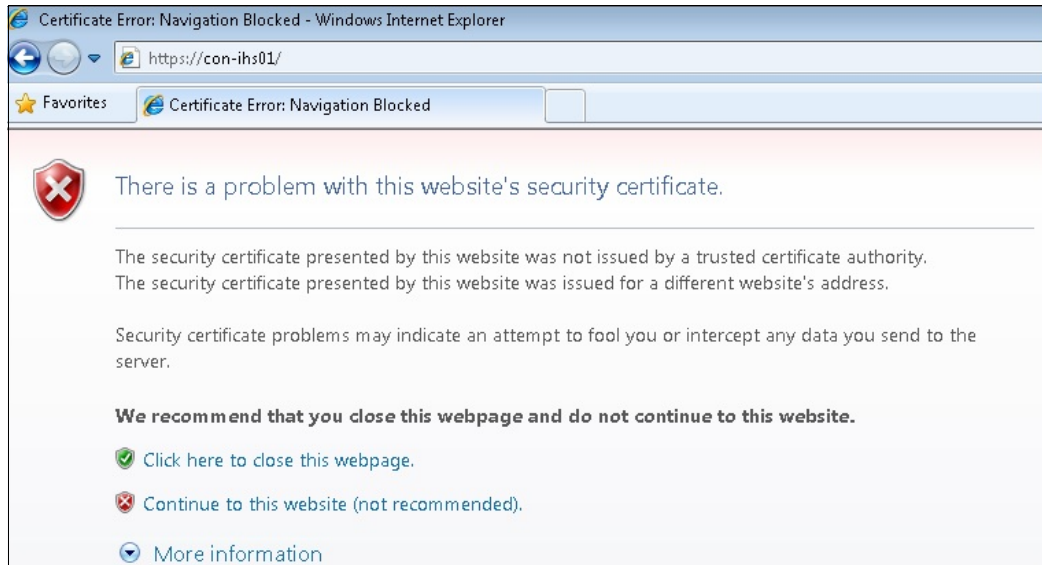
Start

Stop

Terminate

| Select                              | Name     | Web server Type | Node     | Host Name             | Version        | Status |
|-------------------------------------|----------|-----------------|----------|-----------------------|----------------|--------|
| <input checked="" type="checkbox"/> | con-ih01 | IBM HTTP Server | con-ih01 | con-ih01.itso.ibm.com | Not applicable |        |
| <input type="checkbox"/>            | con-ih02 | IBM HTTP Server | con-ih02 | con-ih02.itso.ibm.com | Not applicable |        |
| Total 2                             |          |                 |          |                       |                |        |

6. Access the web server using https from a web browser, in our example, <https://con-ih01.itso.ibm.com/> Because we use a self signed certificate, a warning is displayed informing you that the certificate is not trusted by a Certificate Authority (CA). Click **Continue to this website (not recommended)**,

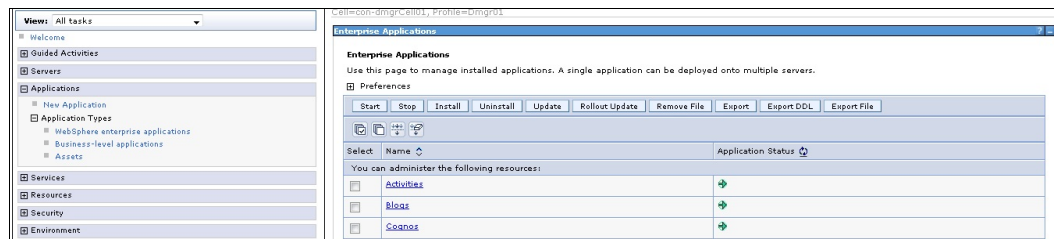


This concludes the SSL configuration on IBM HTTP Server. The network connection security between your browser and the web server is enabled.

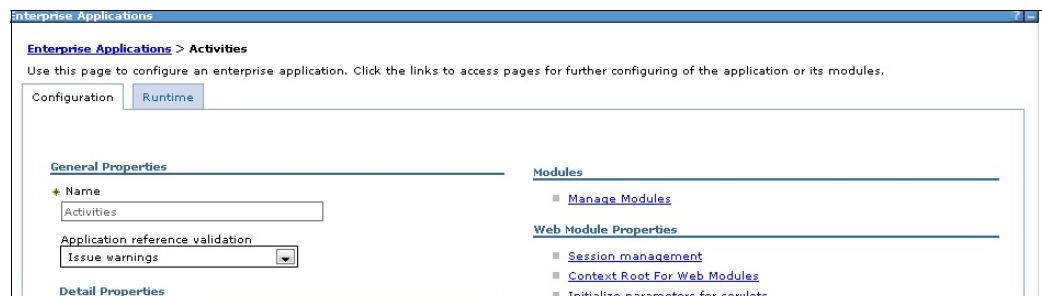
## Verifying module mappings

You must configure the web address that IBM HTTP Server uses to access IBM Connections applications. Follow the steps below to configure IBM HTTP Server:

1. Log into the WebSphere Application Server Console using administration user, expand **Applications** on the left menu, expand **Applications Type** and select **WebSphere enterprise applications**. Select an application, for example, Activities.



2. On Modules area, select **Manage Modules**.



3. Verify each cluster that your applications is assigned on the Server column, for example, WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster
4. On *Clusters* and *servers*, select the corresponding cluster (WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster) that is responsible for the application that you are configuring (Activities) and the web servers



(WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02  
 WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih0).

Using Ctrl key on your keyboard, select all modules as shown in the following figure. Click **Apply**.

Enterprise Applications > Activities > Manage Modules

Manage Modules

Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispersed among several application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based on the applications that are routed through.

Clusters and servers:

WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster

WebSphere:cell=con-dmgrCell01,cluster=ProfilesCluster

WebSphere:cell=con-dmgrCell01,cluster=SearchCluster

WebSphere:cell=con-dmgrCell01,cluster=CommunitiesCluster

WebSphere:cell=con-dmgrCell01,cluster=ModerationCluster

WebSphere:cell=con-dmgrCell01,cluster=MetricsCluster

WebSphere:cell=con-dmgrCell01,cluster=WikisCluster

WebSphere:cell=con-dmgrCell01,cluster=MobileCluster

WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01

WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02

Apply

Remove

Update

Remove File

Export File

| Select                              | Module                    | URI   | Module Type | Server  |
|-------------------------------------|---------------------------|---|-------------|---|
| <input checked="" type="checkbox"/> | EventPublisher            | lc.events.publish.jar,META-INF/ejb-jar.xml        | EJB Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input checked="" type="checkbox"/> | Iconn.scheduler.ejb       | lconn.scheduler.ejb.jar,META-INF/ejb-jar.xml      | EJB Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input checked="" type="checkbox"/> | Platform Command Consumer | platformCommand.consumer.jar,META-INF/ejb-jar.xml | EJB Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input checked="" type="checkbox"/> | FollowingEJB              | lc.following.ejb.jar,META-INF/ejb-jar.xml         | EJB Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input checked="" type="checkbox"/> | Activities Web UI         | oawebui.war,WEB-INF/web.xml                       | Web Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input checked="" type="checkbox"/> | Quickr Document Picker    | qkr.docpicker.war,WEB-INF/web.xml                 | Web Module  | WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |

OK

Cancel

- Verify if all modules are configured with both servers that you have selected on the previous step and click **OK**.

Remove

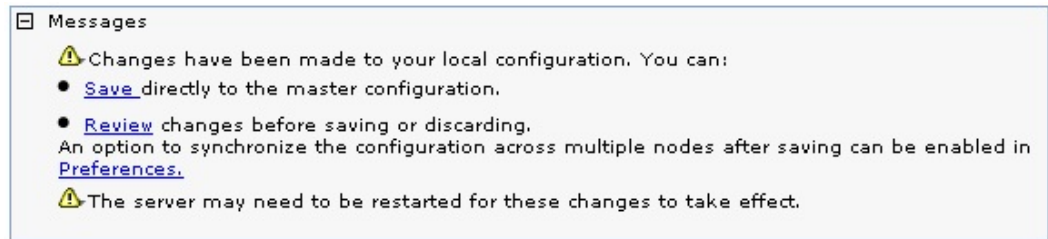
Update

Remove File

Export File

| Select                   | Module                    | URI   | Module Type | Server  |
|--------------------------|---------------------------|---|-------------|---|
| <input type="checkbox"/> | EventPublisher            | lc.events.publish.jar,META-INF/ejb-jar.xml        | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input type="checkbox"/> | Iconn.scheduler.ejb       | lconn.scheduler.ejb.jar,META-INF/ejb-jar.xml      | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input type="checkbox"/> | Platform Command Consumer | platformCommand.consumer.jar,META-INF/ejb-jar.xml | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input type="checkbox"/> | FollowingEJB              | lc.following.ejb.jar,META-INF/ejb-jar.xml         | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input type="checkbox"/> | Activities Web UI         | oawebui.war,WEB-INF/web.xml                       | Web Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |
| <input type="checkbox"/> | Quickr Document Picker    | qkr.docpicker.war,WEB-INF/web.xml                 | Web Module  | WebSphere:cell=con-dmgrCell01,node=con-ih02,server=con-ih02<br>WebSphere:cell=con-dmgrCell01,node=con-ih01,server=con-ih01<br>WebSphere:cell=con-dmgrCell01,cluster=ActivitiesCluster |

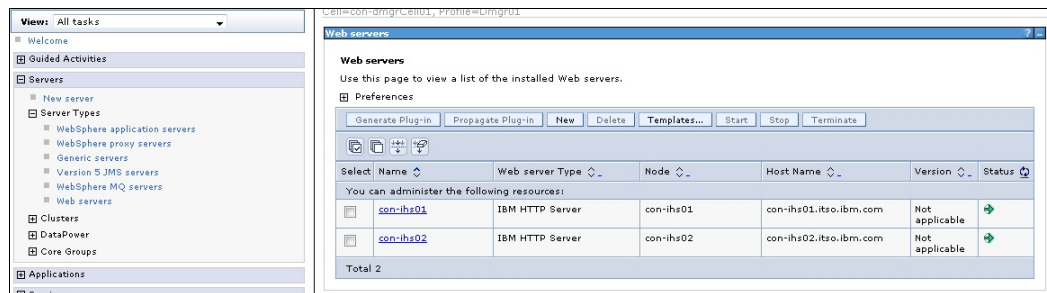
6. Save the configuration



7. Repeat step 1 to step 6 for all IBM Connections applications:

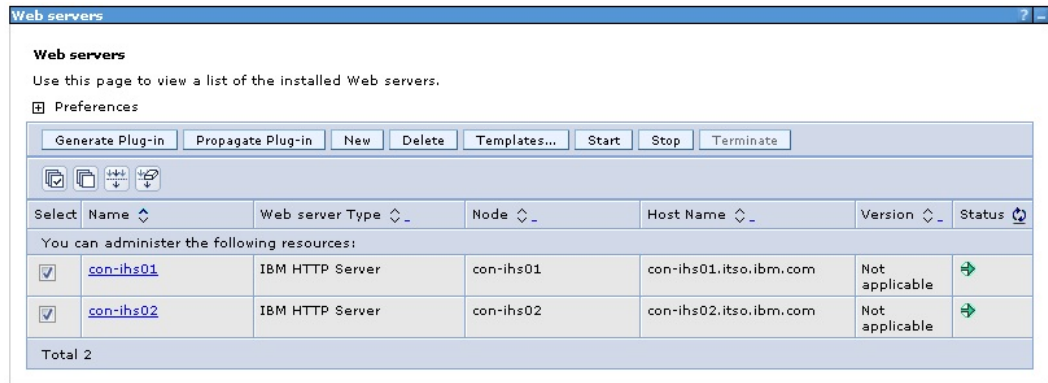
- Activities
- Blogs
- Common
- Communities
- Dogear
- Files
- Forum
- Help
- Homepage
- Metrics
- Mobile
- Mobile Administration
- Moderation
- News
- Profiles
- Search
- WebSphereOAuth20SP
- WidgetContainer
- Wikis

8. On the left menu, expand **Servers** and **Server Types**, and select **Web Servers**.



9. Check the web servers listed and click **Generate Plug-in** then **Propagate Plug-in**. Restart the web servers.





10. From WebSphere Application Server console, stop all application servers.
11. On the Deployment Manager host server, edit *LotusConnections-config.xml* to update the URL for each application. For example: change

`http://con-dmgr.itso.ibm.com:<port>`

to

`http://connections.itso.ibm.com/`

To secure connection, change

`https://con-dmgr.itso.ibm.com:<port>`

to

`https://connections.itso.ibm.com/`

Change

---

```
<sloc:href>
  <sloc:hrefPathPrefix>activities</sloc:hrefPathPrefix>
  <sloc:static href="http://con-dmgr.itso.ibm.com:9083" ssl_href="https://con-dmgr.itso.ibm.com:9446"/>
  <sloc:interService href="https://con-dmgr.itso.ibm.com:9446"/>
</sloc:href>
```

---

to

---

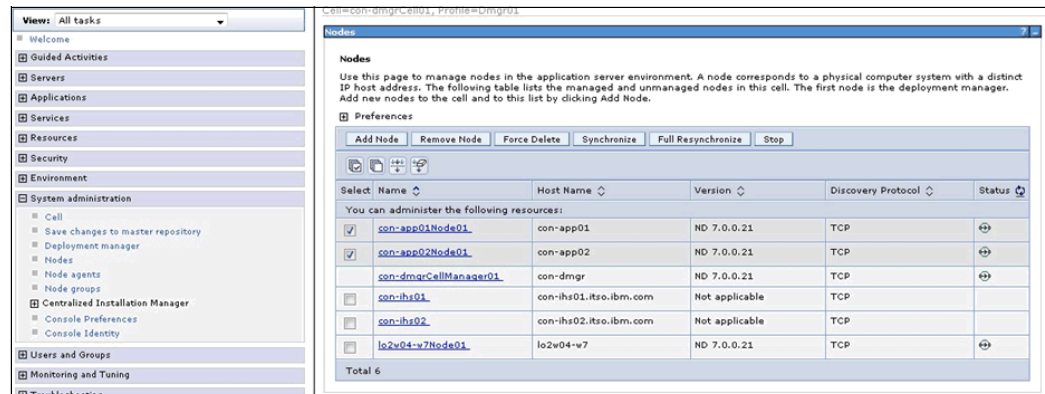
```
<sloc:href>
  <sloc:hrefPathPrefix>activities</sloc:hrefPathPrefix>
  <sloc:static href="http://connections.itso.ibm.com" ssl_href="https://connections.itso.ibm.com"/>
  <sloc:interService href="https://connections.itso.ibm.com"/>
</sloc:href>
```

---

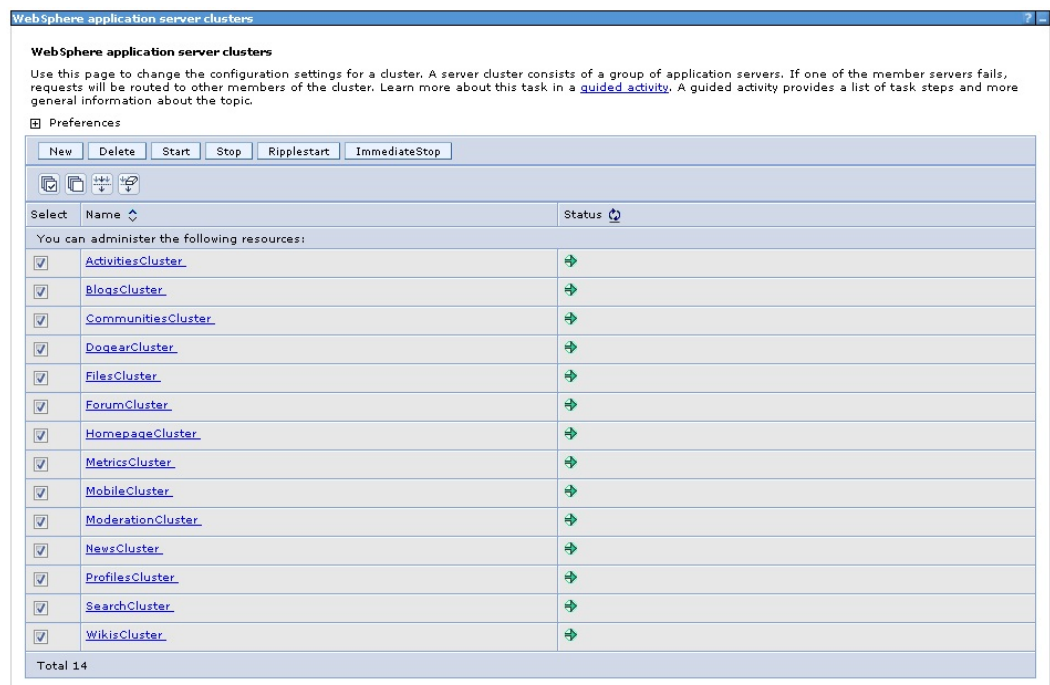
On Linux systems the configuration file directory is:

`/opt/IBM/WebSphere/AppServer/profiles//config/cells//LotusConnections-config/LotusConnections-config.xml`.

12. On WebSphere Application Server console, expand **System administration** and click **Node**. Select the application server nodes responsible for IBM Connections (**con-app01** and **con-app02**) and click **Full Resynchronize**.



- On left menu, expand **Serves** and **Clusters**, click **WebSphere application server** clusters and restart all applications clusters by clicking **Stop** then **Start**.



Upon complete these steps, your environment is ready for users using the URL that you defined. On our lab environment, it is <http://connections.itso.ibm.com/homepage/> and , for secure connections, <https://connections.itso.ibm.com>.

## Homepage redirection

IBM Connections creates its own application context to be accessed (/homepage, /blogs, /news, and so on). You can configure IBM HTTP Server to redirect users to IBM Connections applications. For example, a user visiting <http://connections.itso.ibm.com> can be redirected to <http://connections.itso.ibm.com/homepage>. Follow these steps to set up this redirecting:

- On Web server hosts (con-ihs01.itso.ibm.com and con-ihs02.itso.ibm.com), edit httpd.conf on C:\Program Files\IBM\HTTPServer\conf directory.

2. Uncomment the following line if it is commented out:

---

```
LoadModule rewrite_module modules/mod_rewrite.so
```

---

3. Add a rewrite rule for HTTP:

---

```
RewriteEngine on
RewriteRule ^/$ http://<host_name>/<feature> [R,L]
```

---

host\_name: is the URL that you defined to access IBM Connections, entered the Full Qualified Domain Name (FQDN).

feature: is the IBM Connections application that could be (Homepage, News, Blogs, etc)

On our lab the rewrite rule is defined as:

---

```
RewriteEngine on
RewriteRule ^/$ http://connections.itso.ibm.com/homepage [R,L]
```

---

4. Add a rule for HTTPS placed within the SSL VirtualHost section, defined in Enabling HTTPS .

**Note:** The rule is almost the same added previously, except by the use of https (HTTP over SSL) instead of http.

---

```
RewriteEngine on
RewriteRule ^/$ https://connections.itso.ibm.com/homepage [R,L]
```

---

5. Save and close file.
6. Restart the IBM HTTP Server

Now you can access your environment by typing the URL and you are automatically redirect to the IBM Connections application.

## 6.10.2 Setting the single sign-on domain for future integration

Single sign-on (SSO) on IBM Connections is enabled during the installation process. However, it is necessary to review the information configured on WebSphere Application Server. Follow the steps below to complete the review:

1. Log in to the WebSphere Application Server Integrated Solutions Console on the Deployment Manager.
2. On the left menu, expand **Security** and click **Global security**. On Authentication area, expand **Web and SIP security** and click **Single sign-on (SSO)**.

**Global security**

Use this panel to configure administration and the default application security policy. This security configuration applies to the security policy for all administrative functions and is used as a default security policy for user applications. Security domains can be defined to override and customize the security policies for user applications.

[Security Configuration Wizard](#) [Security Configuration Report](#)

**Administrative security**

☒ Enable administrative security

- [Administrative user roles](#)
- [Administrative group roles](#)
- [Administrative authentication](#)

**Application security**

☒ Enable application security

**Java 2 security**

☐ Use Java 2 security to restrict application access to local resources

- ☐ Warn if applications are granted custom permissions
- ☐ Restrict access to resource authentication data

**User account repository**

Current realm definition  
Federated repositories

Available realm definitions  
Federated repositories

[Configure...](#) [Set as current](#)

[Apply](#) [Reset](#)

**Authentication**

Authentication mechanisms and expiration

☒ LTPA

☐ Kerberos and LTPA

- [Kerberos configuration](#)
- [Authentication cache settings](#)

☐ Web and SIP security

- [General settings](#)
- [Single sign-on \(SSO\)](#)
- [SPNEGO Web authentication](#)
- [Trust association](#)
- [SIP digest authentication](#)

☐ RMI/IIOP security

☐ Java Authentication and Authorization Service

- ☐ Use realm-qualified user names

- [Security domains](#)
- [External authorization providers](#)
- [Custom properties](#)

3. Enter a value for the SSO Domain name.

On Domain name, enter the domain that you are using, for example, itso.ibm.com

**Global security**

**Global security > Single sign-on (SSO)**

Specifies the configuration values for single sign-on.

**General Properties**

☒ Enabled

☐ Requires SSL

Domain name  
itso.ibm.com

☒ Interoperability Mode

☒ Web inbound security attribute propagation

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

4. Click **Apply** and then click **Save**.

**Messages**

⚠ Changes have been made to your local configuration. You can:

- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

⚠ The server may need to be restarted for these changes to take effect.

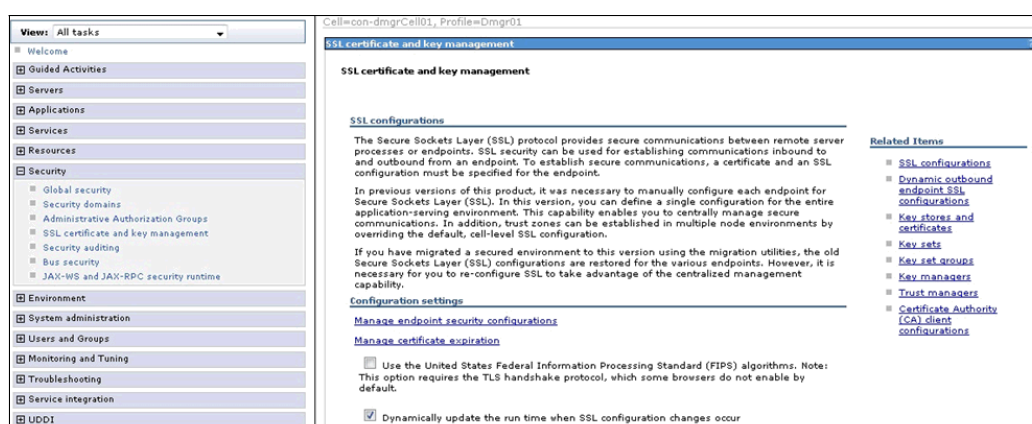
5. Perform a full synchronization of all the nodes.

You have enabled your SSO configuration on your IBM Connections environment.

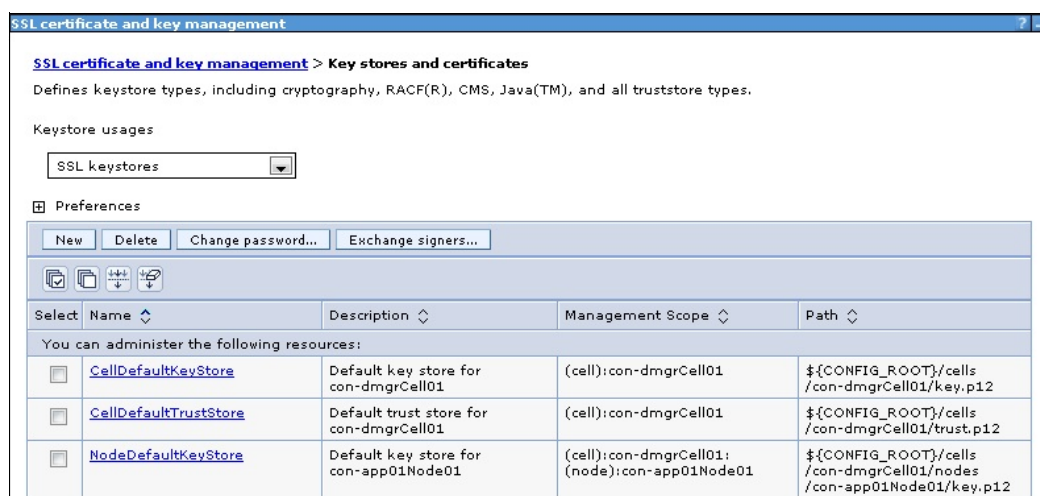
### 6.10.3 Secure Sockets Layer encryption

IBM Connections uses the WebSphere Application Server Integrated Solutions Console as administrator on the Deployment Manager. Here are the steps to manage the certificates on your IBM Connections environment.

1. Log in to the WebSphere Application Server Integrated Solutions Console as administrator on the Deployment Manager.
2. On the left menu, expand **Security** and click **SSL certificate and key management**.
3. On related items, click **key store and certificates**.



4. Select **CellDefaultTrustStore**.



5. On Additional Properties, click **Signer certificates**.

**SSL certificate and key management**

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#)

Defines keystore types, including cryptography, RACF(R), CMS, Java(TM), and all truststore types.

| General Properties  | Additional Properties  |
|---|--|
| <p>Name</p> <input type="text" value="CellDefaultTrustStore"/>                          | <ul style="list-style-type: none"> <li>■ <a href="#">Signer certificates</a></li> <li>■ <a href="#">Personal certificates</a></li> <li>■ <a href="#">Personal certificate requests</a></li> <li>■ <a href="#">Custom properties</a></li> </ul> |
| <p>Description</p> <input type="text" value="Default trust store for con-dmgrCell01"/>  |  |
| <p>Management scope</p> <input type="text" value="(cell):con-dmgrCell01"/>              |  |
| <p>Path</p> <input type="text" value="\${CONFIG_ROOT}/cells/con-dmgrCell01/trust.p12"/> |  |
| <p>★ Password</p> <input type="password"/>  |  |
| <p>Type</p> <input type="text" value="PKCS12"/>   |  |
| <input type="checkbox"/> Remotely managed   |  |

6. Click **Retrieve from port** to get the certificate straight from the server provider.

**SSL certificate and key management**

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#)

Manages signer certificates in key stores.

☒ Preferences

| Select                                      | Alias                     | Issued to  | Fingerprint (SHA Digest)                                    | Expiration                              |
|---|---------------------------|--|---|---|
| You can administer the following resources: |                           |  |   |   |
| <input type="checkbox"/>                    | <a href="#">datapower</a> | OU=Root CA, O="DataPower Technology, Inc.", C=US   | A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17 | Valid from Jun 11, 2003 to Jun 6, 2023. |
| <input type="checkbox"/>                    | <a href="#">default</a>   | CN=con-app01, OU=Root Certificate, OU=con-app01Node01Cell, OU=con-app01Node01, O=IBM, C=US | 6A:FE:66:73:0E:D5:46:51:75:D3:05:BC:84:39:6D:4C:00:5C:45:44 | Valid from Oct 7, 2012 to Oct 4, 2027.  |
| <input type="checkbox"/>                    | <a href="#">default_1</a> | CN=con-app01, OU=Root Certificate, OU=con-app01Node01Cell, OU=con-app01Node01, O=IBM, C=US | 4A:29:F4:70:FA:27:DA:AD:97:81:47:0F:56:67:18:36:74:DD:18:1D | Valid from Oct 7, 2012 to Oct 4, 2027.  |

7. On General Properties, provide the following information:

**Host:** Enter the host information that you want to get the SSL certificate. For example connections.itso.ibm.com

**Port:** Enter the SSL port, for example 443 for HTTPS, 636 for LDAPS

**SSL Configuration for outbound connection:** Select **CellDefaultSSLSettings**

**Alias:** Define a name do identify the certificate that you are importin, for exmple, Connections.

Click **Retrieve signer information**, and check if the information provided referrers to the right certificate and click **OK**.

**SSL certificate and key management**

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#) > [Retrieve from port](#)

Makes a test connection to a Secure Sockets Layer (SSL) port and retrieves the signer from the server during the handshake.

**General Properties**

\* Host  
connections.itso.ibm.com

\* Port  
443

SSL configuration for outbound connection  
CellDefaultSSLSettings

\* Alias  
Connections

[Retrieve signer information](#)

**Retrieved signer information**

Serial number  
1352894123

Issued to  
CN=connections.itso.ibm.com, O=IBM Connections 4 Redbook

Issued by  
CN=connections.itso.ibm.com, O=IBM Connections 4 Redbook

Fingerprint (SHA digest)  
28:94:ED:28:93:87:A5:44:1F:2F:72:14:76:0D:6E:DA:55:1E:FB:05

Validity period  
Nov 14, 2013

[Apply](#) [OK](#) [Reset](#) [Cancel](#)

8. Verify if the certificate that you have imported are on the list and click **Save**.

**SSL certificate and key management**

[SSL certificate and key management](#) > [Key stores and certificates](#) > [CellDefaultTrustStore](#) > [Signer certificates](#)

Manages signer certificates in key stores.

**Preferences**

[Add](#) [Delete](#) [Extract](#) [Retrieve from port](#)

**Messages**

- Changes have been made to your local configuration. You can:
  - [Save](#) directly to the master configuration.
  - [Review](#) changes before saving or discarding.
- An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).
- The server may need to be restarted for these changes to take effect.

**You can administer the following resources:**

| Select                   | Alias                       | Issued to  | Fingerprint (SHA Digest)                                    | Expiration                               |
|--------------------------|-----------------------------|--|---|--|
| <input type="checkbox"/> | <a href="#">connections</a> | CN=connections.itso.ibm.com, O=IBM Connections 4 Redbook                                   | 28:94:ED:28:93:87:A5:44:1F:2F:72:14:76:0D:6E:DA:55:1E:FB:05 | Valid from Nov 14, 2012 to Nov 14, 2013. |
| <input type="checkbox"/> | <a href="#">datapower</a>   | OU=Root CA, O="DataPower Technology, Inc.", C=US   | A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17 | Valid from Jun 11, 2003 to Jun 6, 2023.  |
| <input type="checkbox"/> | <a href="#">default</a>     | CN=con-app01, OU=Root Certificate, OU=con-app01Node01Cell, OU=con-app01Node01, O=IBM, C=US | 6A:FE:66:73:0E:D5:46:51:75:D3:05:8C:84:39:6D:4C:00:5C:45:44 | Valid from Oct 7, 2012 to Oct 4, 2027.   |
| <input type="checkbox"/> | <a href="#">default_1</a>   | CN=con-app01, OU=Root Certificate, OU=con-app01Node01Cell, OU=con-app01Node01, O=IBM, C=US | 4A:29:F4:70:FA:27:DA:AD:97:81:47:0F:56:67:18:36:74:DD:18:1D | Valid from Oct 7, 2012 to Oct 4, 2027.   |
| <input type="checkbox"/> | <a href="#">default_2</a>   | CN=con-app02, OU=Root  | F2:F7:5F:54:60:35:2D:15:38:DE:88:8A:4B:52:14:0A:3C:58:E8:06 | Valid from                               |

Now your IBM Connections are able to accept the SSL communication between the servers.

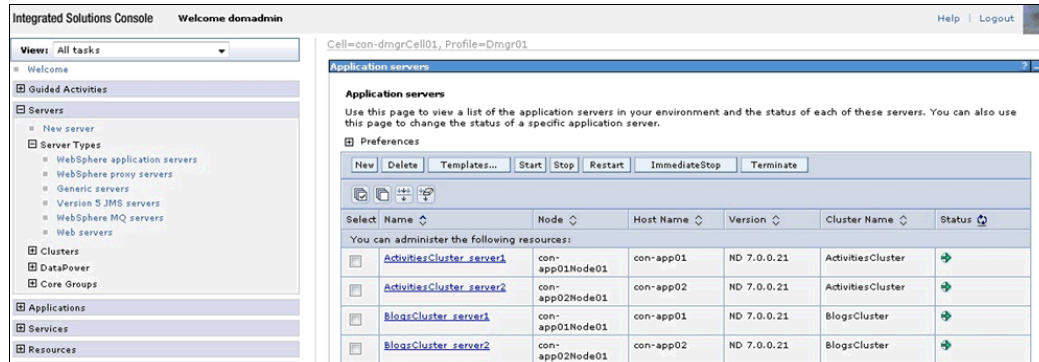


## 6.10.4 Setting the Java Virtual Machine heap size

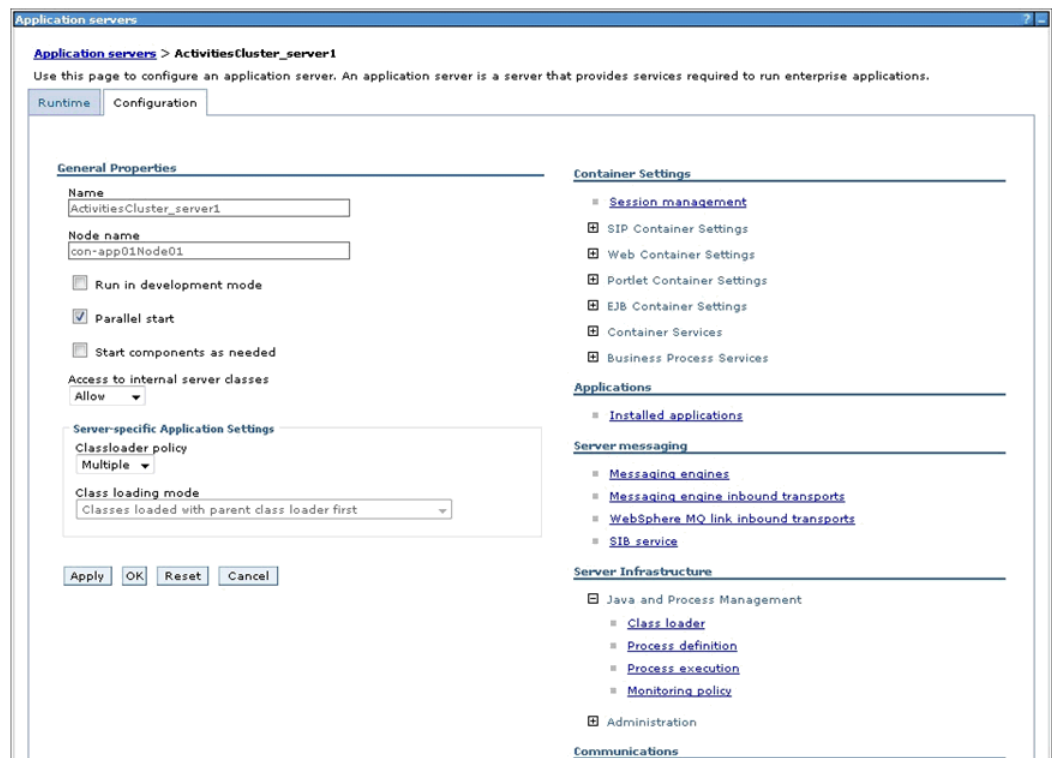
Review the heap size on each Java Virtual Machine (JVM) server to avoid out-of-memory errors on your environment. Ensure that the memory allocated does not exceed the physical memory available on your server.

Follow the steps below to configure JVM size:

1. Log into the WebSphere Application Server Console, expand **Server** on the left menu. Expand **Server Type** and select **WebSphere applications server** then select a JVM, for example, **ActivitiesCluster\_server1**.

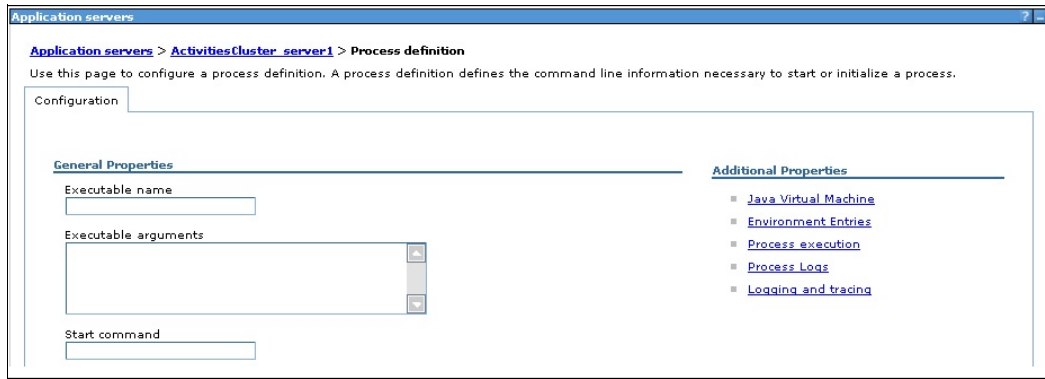


2. In the Server Infrastructure area, expand **Java and Process Management** and click **Process Definition**.



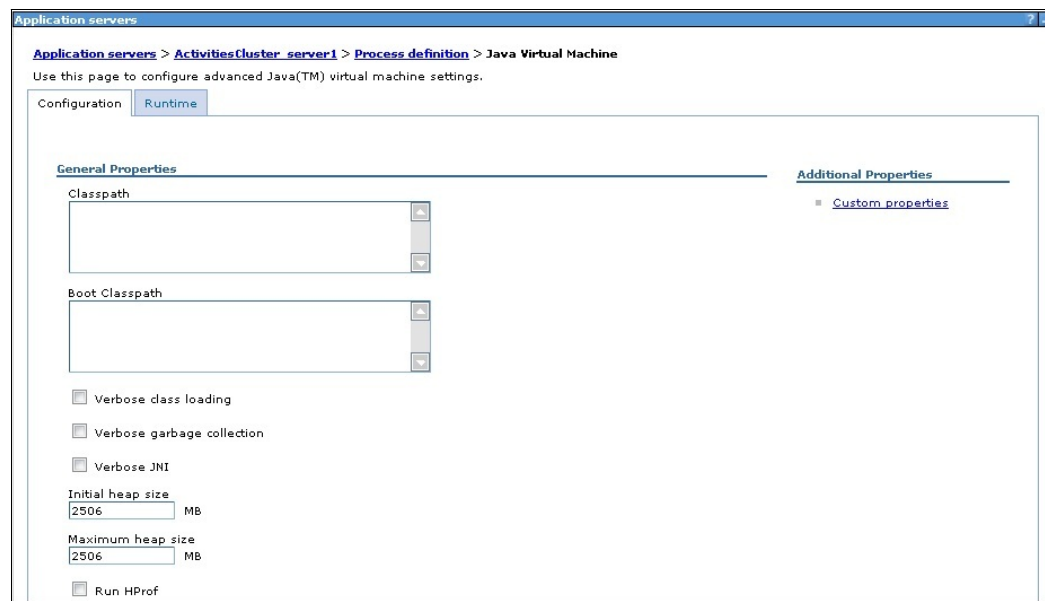
3. In Additional Properties, select **Java Virtual Machine**.



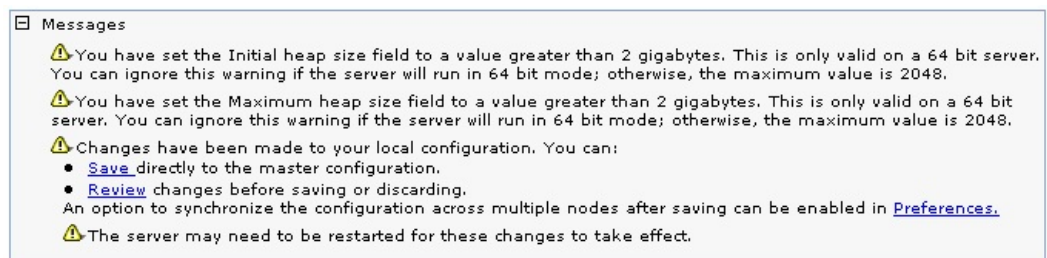


4. Set the Minimum Heap Size and Maximum Heap Size to 2506 MB (recommended).

**Note:** Ensure that you are not allocating more memory than the physical capacity of the system where the JVM is installed.



5. Click **OK** and then click **Save**.

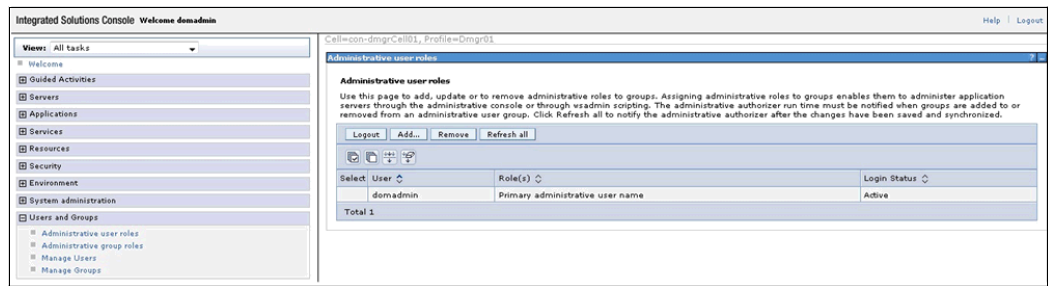


6. Restart the JVM selected.
7. Repeat these steps for any additional JVM in your environment.

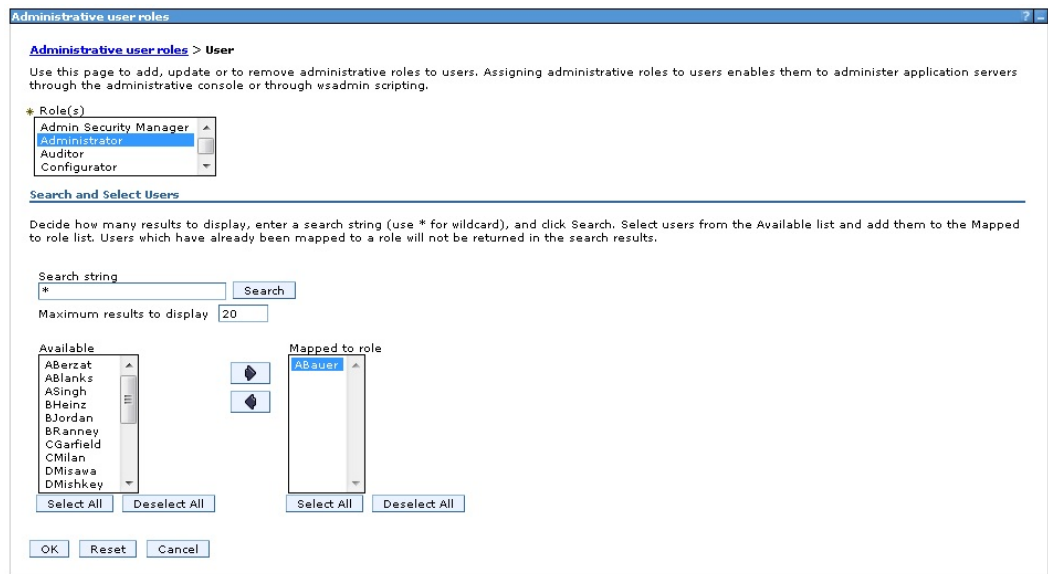
## 6.10.5 Creating additional administrator with the WebSphere Integrate Console Solution

The Integrated Solutions console (ISC) allows you to add more users to use ISC and you can also choose the rights that each users can have to access the ISC. Depending on the profile assigned, the user can just monitor the environment, can only stop and start the JVM, or can have full access using Administrator profile. Follow these steps to add more users on the ISC:

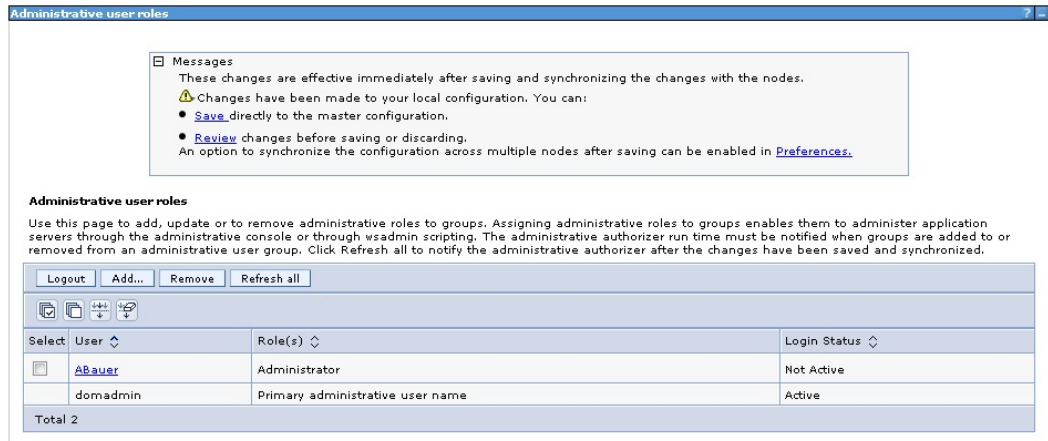
1. Log in to the WebSphere Application Server Integrated Solutions Console on the Deployment Manager.
2. On the left menu expand **Users and Groups**. Select **Administrative user roles** and click **Add**.



3. Select the **Role** on the list. Click **Search** and select the user or users (**Abauer**) that you to add the profile and click the right arrow then click **OK**.



4. Check if the user or users and roles that you selected are correct and click **Save**.



5. Log off from the ISC and try to log in using the users that you have added.

You have added more users with certain rights to access the ISC.

**Note:** For more information about the roles you can visit the WebSphere Application Server Information Center  
(<http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/index.jsp>)

## 6.10.6 Configuring Cognos Business Intelligence

By default, IBM Cognos Business Intelligence (BI) server uses database for authentication. To work with IBM Connections, Cognos BI server must use the same LDAP server as IBM Connections server.

The configuration steps for Cognos BI server are as follows:

1. Apply fix packs to update the Cognos Business Intelligence.
2. Configuring LDAP for Cognos BI Server
3. Grant access to global metrics role and Community metrics role
4. Configuring job scheduler for Cognos BI Transformer on windows
5. Configure IBM HTTP Server for Cognos Applications.

In this section, we demonstrate configuration steps of Cognos Business Intelligence on a Windows system

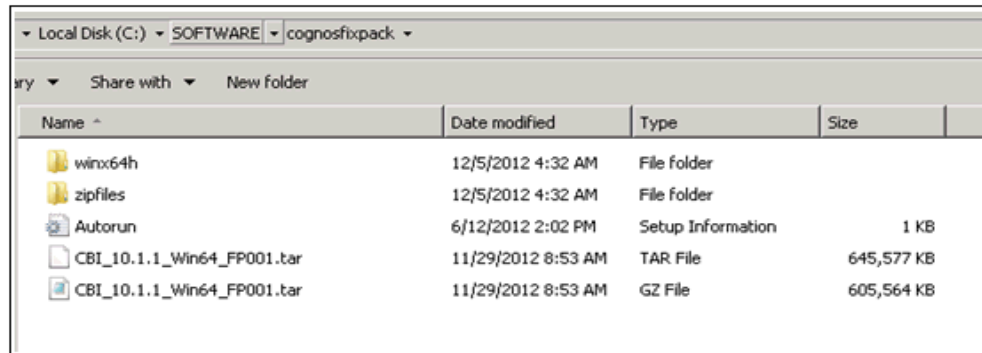
### Applying fix packs to update Cognos Business Intelligence

IBM periodically releases fix pack to resolve product related issues. Perform the following steps to install the fix pack on Cognos BI server:

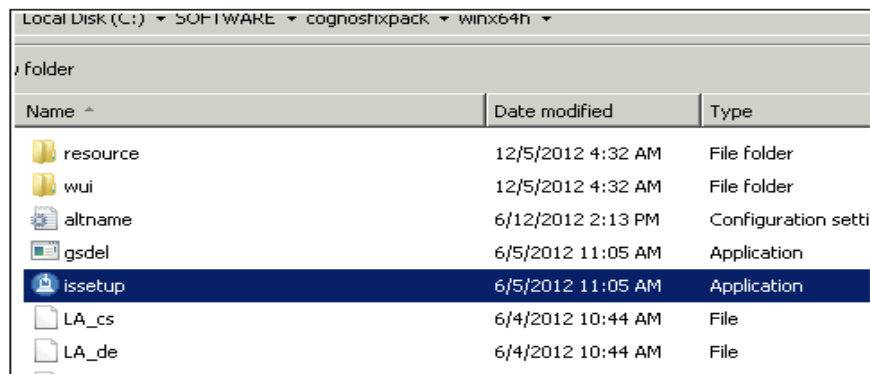
1. Download the fix pack from IBM Fix Central  
(<http://www-933.ibm.com/support/fixcentral/swg/selectFixes?parent=Cognos&product=ibm/Information+Management/Cognos+8+Business+Intelligence&release=10.1.1&platform=All&function=all>).

Select the fix pack for your operation system. We download *CBI\_10.1.1\_Win64\_FP001.tar*.

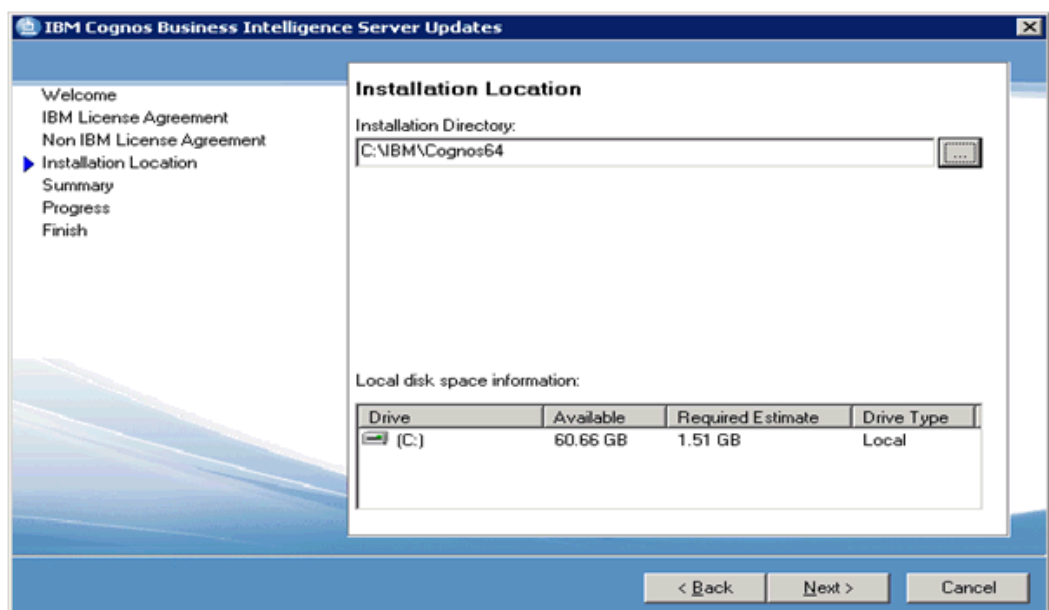
2. Extract the compressed file into a temporary directory, for example C:\SOFTWARE\cognosfixpack.



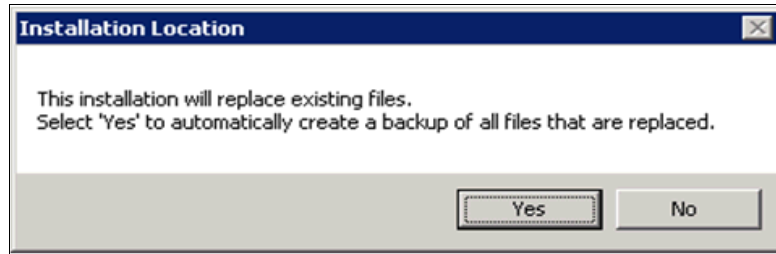
3. Run the following command to stop the cognos\_server application server  
`C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopServer.bat cognos_server -username domadmin -password xxxxx`
4. Go to C:\SOFTWARE\cognosfixpack\winx64h directory and run the **issetup.exe** application file.



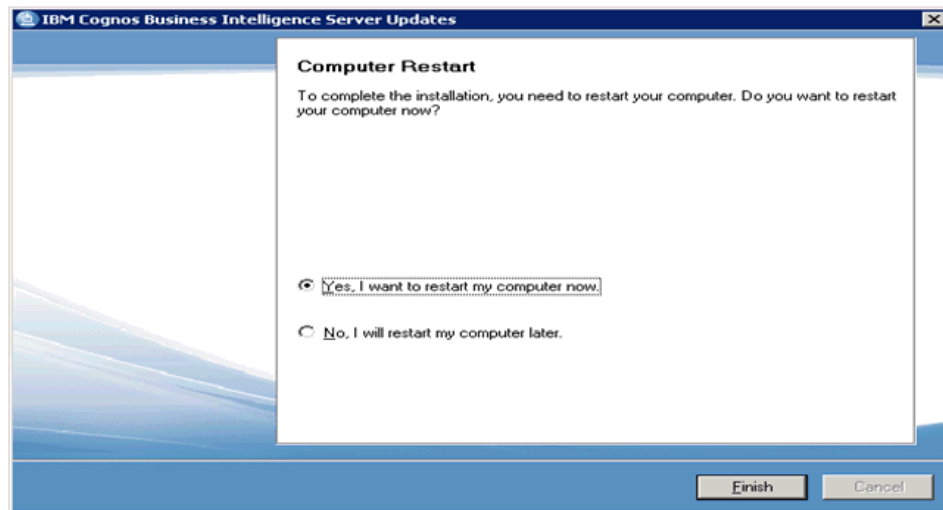
5. A welcome screen is displayed. Click **Next**,
6. Select the location where your Cognos BI Server is installed,



7. Select **YES** to create a backup of all files.



8. Installation Summary is displayed. Click **Next**,
9. Click **Yes, to restart computer now** and click **Finish**.



10. Start the Cognos BI server node agent using command line. Make sure that the password is present in cognos-setup.properties. If password is not there, supply the password as an arguments to the *cognos-setup-update.bat* script.
11. Generate the Cognos. ear file by running the following command:  
Windows: **Run the cognos-setup-update.bat.**  
UNIX: **Run cognos-setup-update.sh**  
The log file, cognos-setup-update.log is stored in same directory.

```
Administrator: Command Prompt
clean_war:
[delete] Deleting directory C:\IBM\Cognos64\temp\war\p2pd
[delete] Deleting: C:\IBM\Cognos64\temp\war\p2pd.war
clean:
BUILD SUCCESSFUL
Total time: 1 minute 39 seconds
POPD
... generating Cognos EAR completed
Removing passwords from C:\IBM\CognosSetup\cognos-setup.properties ...
"C:\IBM\WebSphere\AppServer\java\bin\java.exe" -classpath "C:\IBM\CognosSetup\lib\ScrubPwd.jar" com.ibm.connections.install.ScrubPasswords "C:\IBM\CognosSetup\cognos-setup.properties" "C:\IBM\CognosSetup\cognos-setup.properties_clean"
DEL "C:\IBM\CognosSetup\cognos-setup.properties"
MOVE /Y "C:\IBM\CognosSetup\cognos-setup.properties_clean" "C:\IBM\CognosSetup\cognos-setup.properties"
1 file(s) moved.
... removing passwords from C:\IBM\CognosSetup\cognos-setup.properties completed
C:\IBM\CognosSetup>
```

**Note:** Use LDAP user ID for was.local.username because it is federated to the WebSphere Application Server Deployment Manager.

12. Login to the WebSphere Application Server Deployment Manager Administration console
13. Go to **Applications** → **Application Types** → **WebSphere Enterprise Applications**.
14. Select Cognos application and click **Update**.
15. Select the fast path deployment options to deploy the application.
16. Start the cognos\_server application server.
17. Set the JAVA\_HOME variable by running the following command.

```
C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\setupCmdLine.bat
```

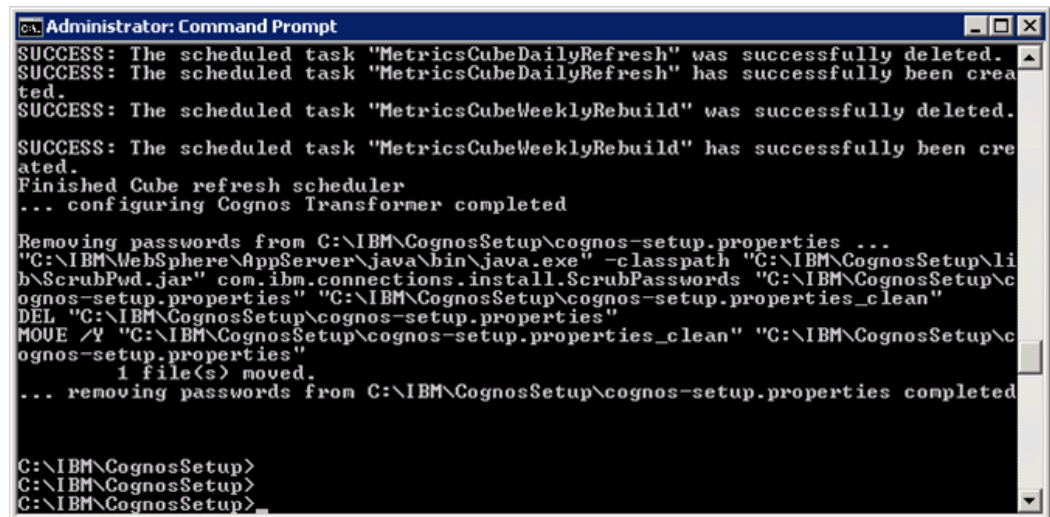
Run cognos-configure-update.bat to configure the Cognos BI server:

```
C:\IBM\CognosSetup\cognos-configure-update.bat
```

```
-was.local.admin.password=itsoadmin -cognos.admin.password=xxxx  
-cognos.db.password=xxxx -metrics.db.password=xxxx
```

For UNIX platform, the command is **cognos-configure-update.sh**.

18. The following success message is displayed.

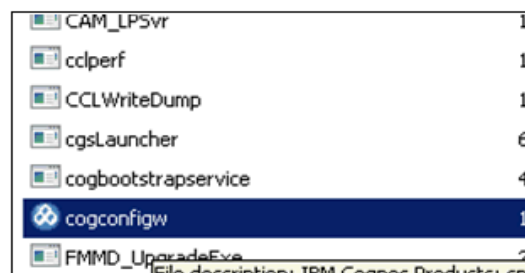


```
Administrator: Command Prompt  
SUCCESS: The scheduled task "MetricsCubeDailyRefresh" was successfully deleted.  
SUCCESS: The scheduled task "MetricsCubeDailyRefresh" has successfully been cre  
ated.  
SUCCESS: The scheduled task "MetricsCubeWeeklyRebuild" was successfully deleted.  
SUCCESS: The scheduled task "MetricsCubeWeeklyRebuild" has successfully been cre  
ated.  
Finished Cube refresh scheduler  
... configuring Cognos Transformer completed  
  
Removing passwords from C:\IBM\CognosSetup\cognos-setup.properties ...  
"C:\IBM\WebSphere\AppServer\java\bin\java.exe" -classpath "C:\IBM\CognosSetup\li  
b\ScrubPwd.jar" com.ibm.connections.install.ScrubPasswords "C:\IBM\CognosSetup\c  
ognos-setup.properties" "C:\IBM\CognosSetup\cognos-setup.properties_clean"  
DEL "C:\IBM\CognosSetup\cognos-setup.properties"  
MOVE /Y "C:\IBM\CognosSetup\cognos-setup.properties_clean" "C:\IBM\CognosSetup\c  
ognos-setup.properties"  
1 file(s) moved.  
... removing passwords from C:\IBM\CognosSetup\cognos-setup.properties completed  
  
C:\IBM\CognosSetup>  
C:\IBM\CognosSetup>  
C:\IBM\CognosSetup>
```

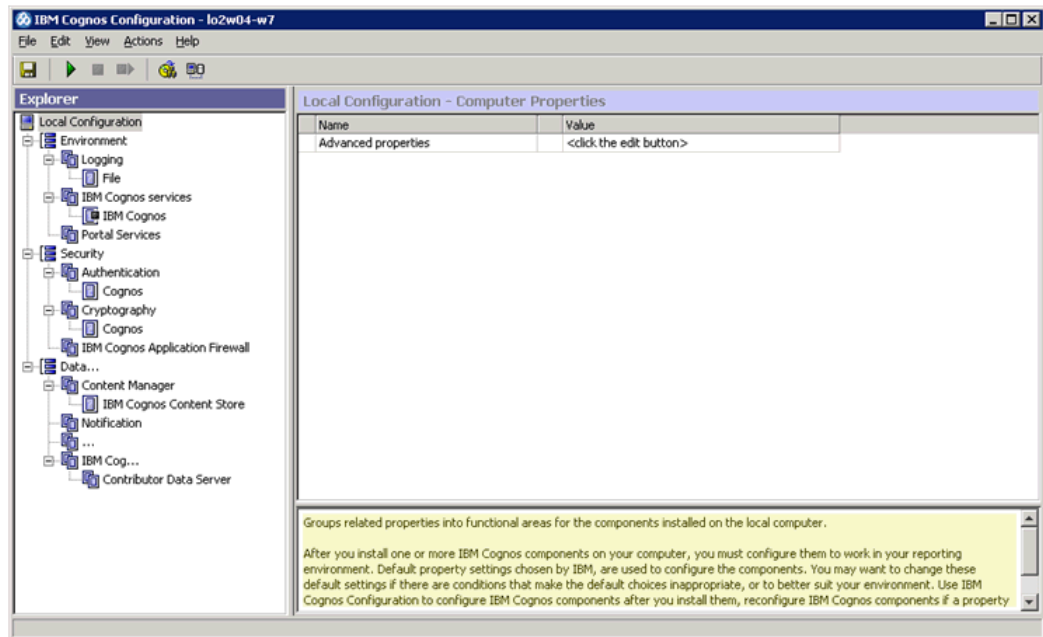
## Configuring LDAP for Cognos BI Server

Perform the following steps to configure Domino LDAP server as user repository.

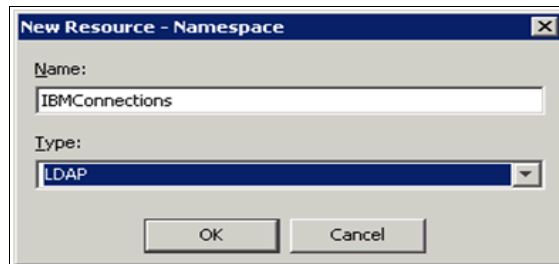
1. Run cogconfigw.exe from the C:\IBM\Cognos64\bin64 directory to start the Cognos BI configuration tool.



2. Launch the wizard.



3. Select **Security** → **Authentication**.
4. Right click **New resource** → **Namespace** and create a namespace called **IBMConnections**.

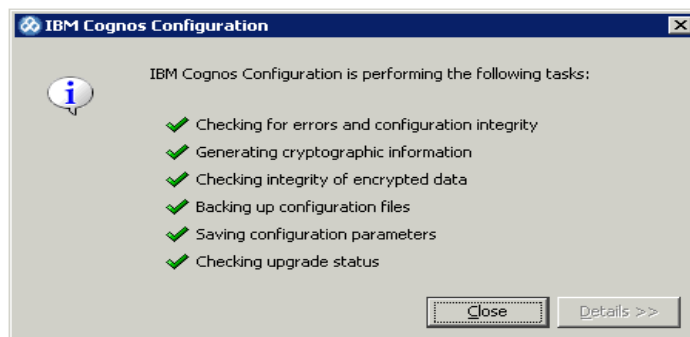


5. Enter the following values for the IBMConnections namespace.

| Name  | Value example                        |
|---|--------------------------------------|
| <b>Namespace ID</b>                           | IBMConnections                       |
| <b>Host and Port</b>                          | dom-ldap.itso.ibm.com:389            |
| <b>Base Distinguished Name</b>                | o=itso                               |
| <b>User Lookup</b>                            | (uid=\${Userid})                     |
| <b>Use External Identity</b>                  | true                                 |
| <b>External Identity Mapping</b>              | (uid=\${environment("REMOTE_USER")}) |
| <b>Bind User DN and password</b>              | domadmin and your password           |
| <b>Object Class( Folder Mapping)</b>          | dominoOrganization                   |
| <b>Object Class(Group Mapping)</b>            | dominoGroup                          |
| <b>Member(Group Mapping)</b>                  | member                               |
| <b>Account Object Class (Account Mapping)</b> | dominoPerson                         |
| <b>Name (Account Mapping)</b>                 | uid                                  |

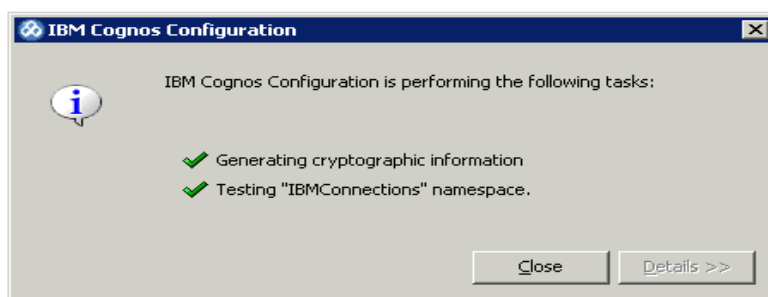
| IBMConnections - Namespace - Resource Properties |                                      |
|--|--------------------------------------|
| Name   | Value                                |
| Type   | LDAP                                 |
| * Namespace ID                                   | IBMConnections                       |
| * Host and port                                  | ldap-dom.itso.ibm.com:389            |
| * Base Distinguished Name                        | o=itso                               |
| User lookup                                      | (uid=\${userID})                     |
| Use external identity?                           | True                                 |
| External identity mapping                        | (uid=\${environment("REMOTE_USER")}) |
| Bind user DN and password                        | *****                                |
| Size limit                                       | -1                                   |
| Time out in seconds                              | -1                                   |
| Use bind credentials for search?                 | False                                |
| Allow empty password?                            | False                                |
| Unique identifier                                | dn                                   |
| Data encoding                                    | UTF-8                                |
| SSL certificate database                         |                                      |
| Advanced properties                              | <click the edit button>              |
| <b>Folder mappings (Advanced)</b>                |                                      |
| Object class                                     | dominoOrganization                   |
| Description                                      | description                          |
| Name   | ou                                   |
| <b>Group mappings (Advanced)</b>                 |                                      |
| Object class                                     | dominoGroup                          |
| Description                                      | description                          |
| Member   | member                               |
| Name   | cn                                   |
| <b>Account mappings (Advanced)</b>               |                                      |
| Account object class                             | dominoPerson                         |
| Business phone                                   | telephonenumber                      |
| Content locale                                   | preferredlanguage                    |
| Description                                      | description                          |
| Email  | mail                                 |
| Fax/Phone  | facsimiletelephonenumber             |
| Given name                                       | givenname                            |
| Home phone                                       | homephone                            |
| Mobile phone                                     | mobile                               |
| Name   | uid                                  |

- Expand **Local Configuration** → **Security** → **Authentication** → **Cognos** and set Allow Anonymous Access to **False**.
- Click **File** → **Save**.

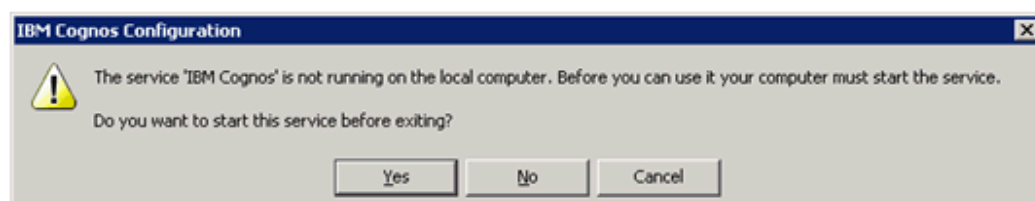




8. Right click the namespace **IBMConnections** and click **Test** to validate the LDAP settings.



9. Click **File** → **Exit**. Select No to start the Cognos service.



10. Login to the Deployment Manager console with the user ID domadmin.
11. Stop the cognos\_server and wait for *one* minute to ensure that the Cognos server is stopped.
12. Validate the Java processes cgsLauncher.exe and CAM\_LPSvr do not exist on the Cognos BI server.
13. Start the cognos\_server.

## Granting access to the global-metrics role and the community-metrics role

By default, all the roles are not mapped to any of the users. To change the Cognos BI server configuration, the Cognos administrator ID must be mapped to metrics-report role and community-metrics role. Use the following steps to map roles and users:

1. Log in to Deployment Manager Admin Console, for example:  
<https://con-dmgr.itso.ibm.com:9043/ibm/console>
2. Go to **Applications** → **WebSphere Enterprise Applications** → **Metrics** → **Security role to User/Group Mapping**.
3. Add Cognos Administrator user ID, domadmin to the following roles.
  - metrics-report-run
  - community-metrics-run

| Map Users... Map Groups... Map Special Subjects |                        |  |              |               |
|---|------------------------|--|--------------|---------------|
| Select  | Role                   | Special subjects                         | Mapped users | Mapped groups |
| <input type="checkbox"/>                        | everyone               | Everyone                                 |              |               |
| <input type="checkbox"/>                        | person                 | All Authenticated in Application's Realm |              |               |
| <input type="checkbox"/>                        | reader                 | Everyone                                 |              |               |
| <input type="checkbox"/>                        | everyone-authenticated | All Authenticated in Application's Realm |              |               |
| <input type="checkbox"/>                        | community-metrics-run  | All Authenticated in Application's Realm | domadmin     |               |
| <input type="checkbox"/>                        | admin                  | None                                     |              |               |
| <input type="checkbox"/>                        | metrics-report-run     | None                                     | domadmin     |               |

**Note:** Failing to add Cognos Administrator domadmin into metrics-report role, you can not configure IBMConnectionsMetricsAdmin role and the request will throw an error message, "Access is restricted"

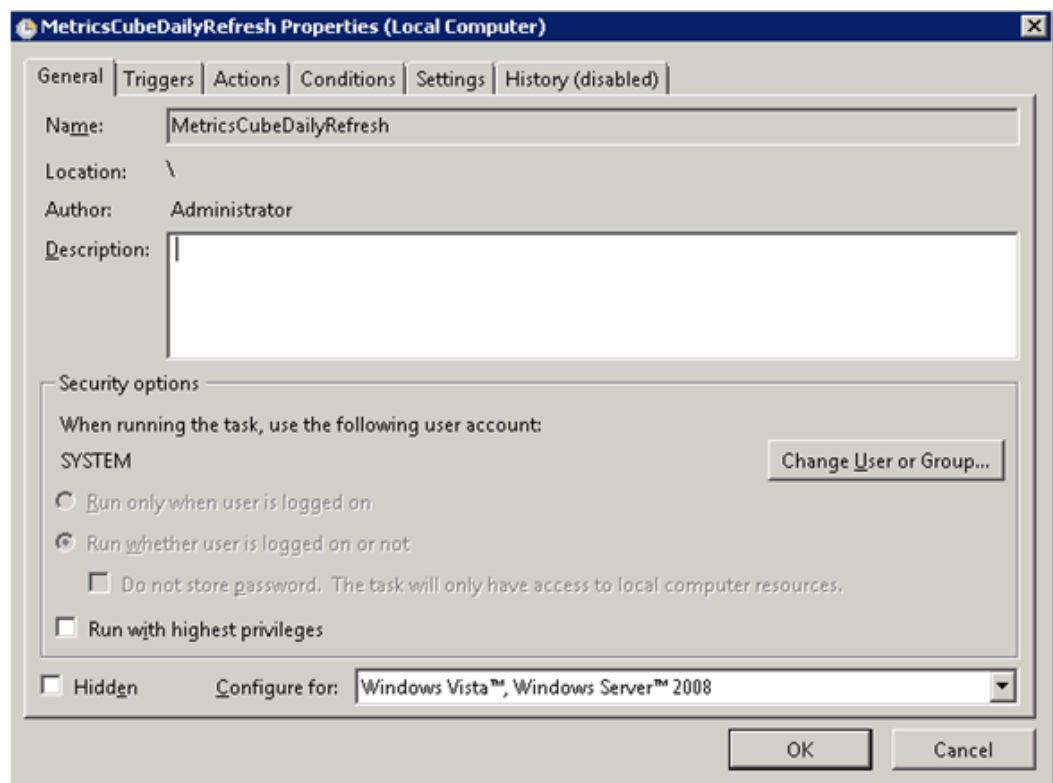
4. Save and synchronize the nodes.
5. Go to **System Administration** → **Node Agents** and restart node agents for the IBM Connection servers.

### Configuring job scheduler for Cognos BI Transformer on Windows

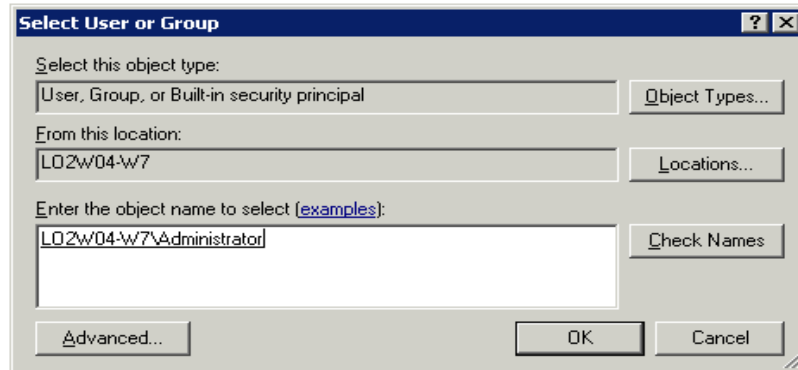
IBM Cognos BI Transformer refreshes the power cube data incrementally once in a day and replaces the power cube's month data once in a week. It is advisable to run the daily tasks at early morning and weekly task at midnight so that other tasks are not impacted.

Complete these steps to configure job scheduler for Cognos BI Transformer on Windows:

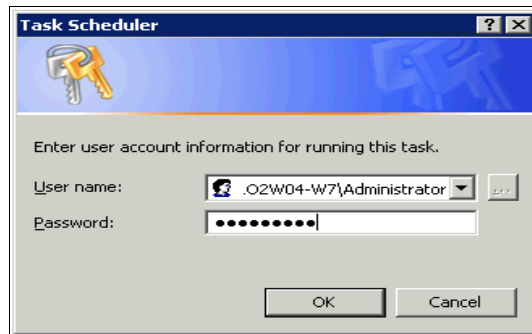
1. Click **Start** → **Control Panel** → **System and Security** → **Administrative Tools**.
2. Click **Task scheduler**.
3. In the Task scheduler, select **MetricsCubeDailyRefresh** to view its properties.



4. Go to **General** tab and select **Change User or Group**.
5. Type **Administrator** in the "Enter the object name to select" and select **Check Names**.



6. Click **OK** to save the settings.
7. Task scheduler prompts password for the Administrator user ID. Enter your password and click **OK**.

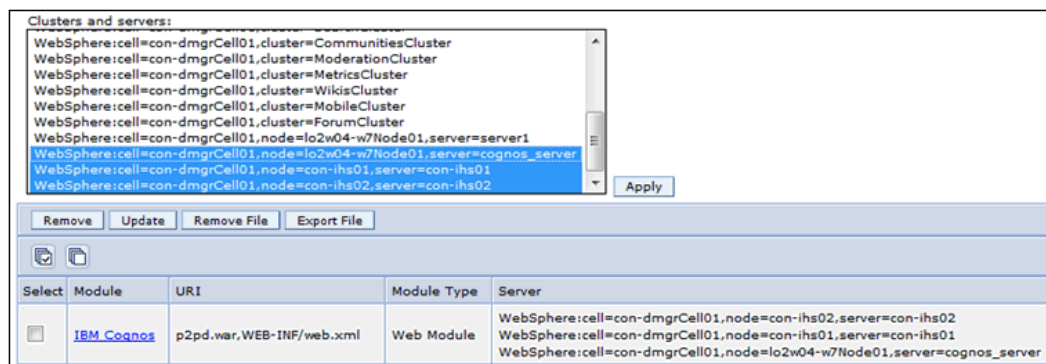


8. Close the Task scheduler.

## Configuring IBM HTTP Server for Cognos applications

IBM Cognos BI server and IBM Cognos BI Transformer are configured with IBM HTTP server so that the request is routed through web servers instead of accessing the servers directly. Use the following steps to configure IBM HTTP server for Cognos applications:

1. Login to Deployment Manager using the following URL with user ID domadmin.  
<https://con-dmgr.itso.ibm.com:9043/ibm/console/>
2. Go to **Applications** → **WebSphere Enterprise Applications** → **Cognos**
3. Select **Manage Modules**.
4. Select the applications and map it to IBM HTTP Server and cognos\_server.



5. Save the configuration.
6. Restart the cognos\_server application server.
7. Go to **Servers** → **Server Types** → **Web Servers**.
8. Select all the web servers and click **Generate Plug-in**.
9. Propagate the plug-in to the web servers and restart the web servers.
10. Validate the Cognos application using IBM HTTP Server.

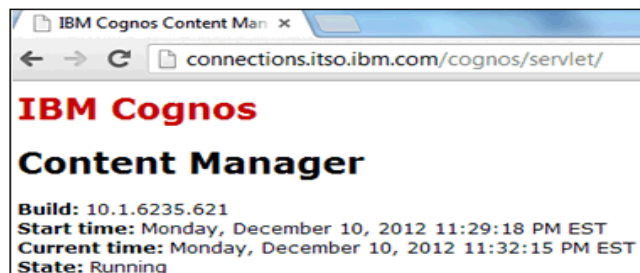
con-ihs01:



con-ihs02:



Using Load Balancer:



11. Run the tool C:\IBM\Cognos64\bin64\cogconfigw.exe to launch the Cognos BI Server configuration tool to operate with IBM HTTP Server.
12. Go to **Local Configuration** → **Environment** and edit the following properties.
  - Dispatch URIs for Gateway
  - Dispatcher URI for external applications
13. Save the configuration and exit the configuration tool. Select **NO** for starting the cognos service while closing the tool.
14. Restart the Cognos server. Make sure that after stopping the cognos\_server application server, the following Java process does not exist prior to starting them back.
  - cgsLauncher.exe

– CAM\_LPSvr processes

15. Enter the following URL to validate the Cognos server:

<https://connections.itso.ibm.com/cognos/servlet>



16. Run the tool C:\IBM\Cognos\bin\cogconfigw.exe to launch the Cognos BI Transformer configuration tool to operate with IBM HTTP Server.

17. Go to **Local Configuration** → **Environment** and edit the following properties to change the value.

Gateway Settings

Other URI Settings

| Environment - Group Properties           |   |
|--|---|
| Name                                     | Value   |
| Data files location                      | ../data   |
| Temporary files location                 | ../temp   |
| Encrypt temporary files?                 | False   |
| Sort buffer size in MB                   | 4   |
| IP Version for Host Name Resolution      | Use IPv4 addresses  |
| <b>Gateway Settings</b>                  |   |
| Gateway URI                              | <a href="https://connections.itso.ibm.com:443/cognos/servlet/dispatch">https://connections.itso.ibm.com:443/cognos/servlet/dispatch</a> |
| <b>Other URI Settings</b>                |   |
| Dispatcher URI for external applications | <a href="https://connections.itso.ibm.com:443/cognos/servlet/dispatch">https://connections.itso.ibm.com:443/cognos/servlet/dispatch</a> |

18. Click **File** → **Save**.
19. Accept the security warnings and click **YES** to proceed.
20. Exit the configuration tool to complete the configuration.

**Note:** We configured load balancer for IBM HTTP Server. Hence we used the load balancer host name instead of direct IBM HTTP Server host name.

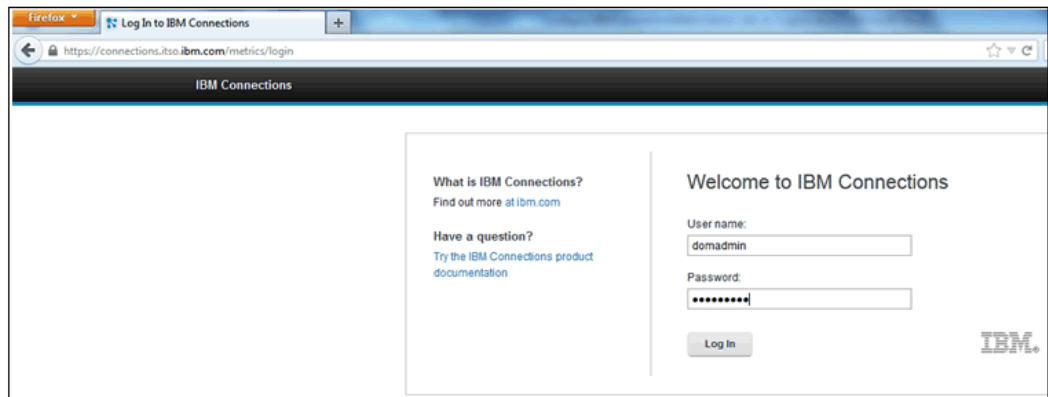
## Configuring the IBMConnectionsMetricAdmin role on Cognos

The IBMConnectionsMetricAdmin role helps Metrics application administrators to access IBM Cognos BI server features and reports. To configure this role, user should login with IBM Cognos administrator user ID and that user ID is present in LDAP server if LDAP authentication is enabled for IBM Cognos BI server. This role must have IBM Cognos administrator and IBM Connections administrator authority, and users belong to metrics-report role.

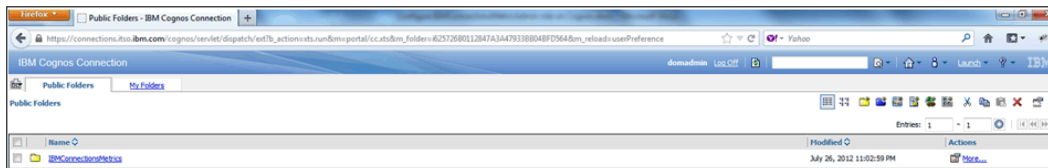
Use the following steps to configure the IBMConnectionsMetricAdmin role on Cognos:

1. Open a browser and enter the following URL.
- <https://connections.itso.ibm.com/cognos/servlet/dispatch/ext>

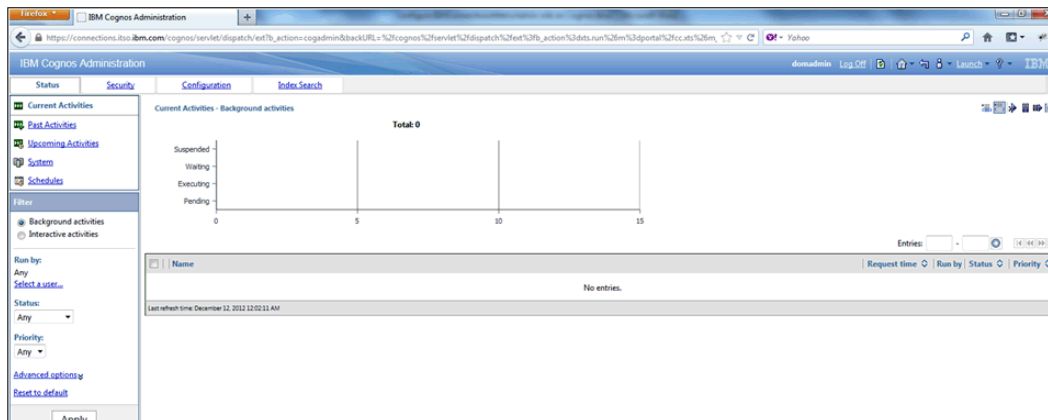
2. Request is route to IBM Connections login page. Enter the user ID as domadmin.



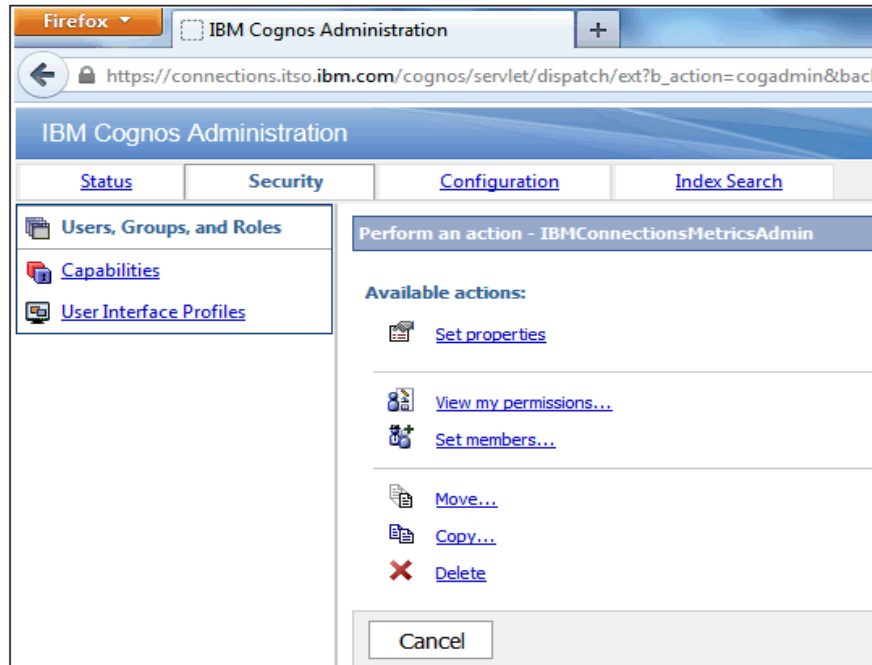
3. After logging in, the request is redirected to Cognos BI Dispatcher page.



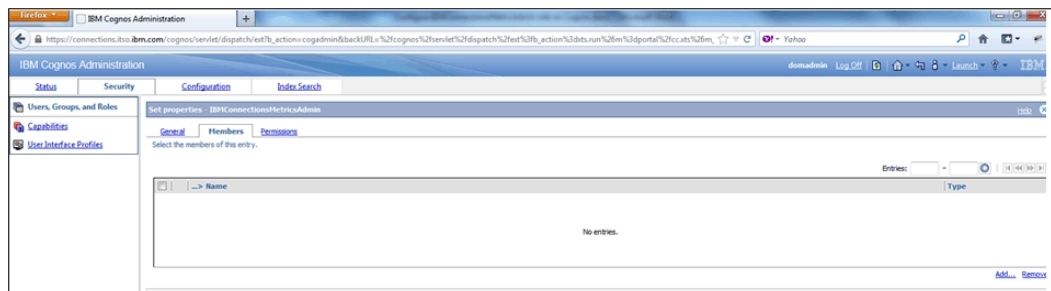
4. Click **Launch** → **IBM Cognos Administration**.



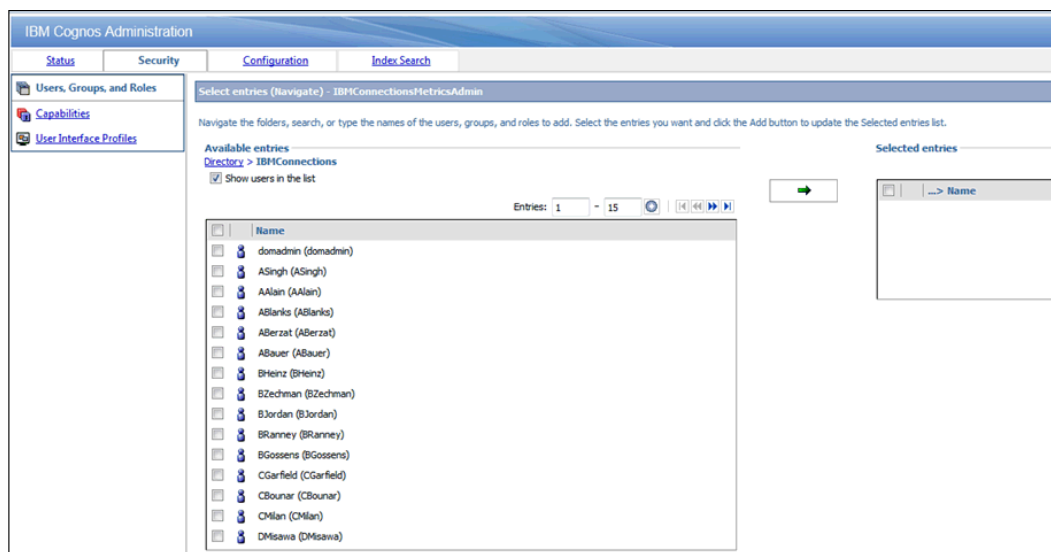
5. Select the **Security** tab
6. On the Directory page, select **Cognos** from the list
7. Select **IBMConnectionsMetricAdmin** role and click **More**.



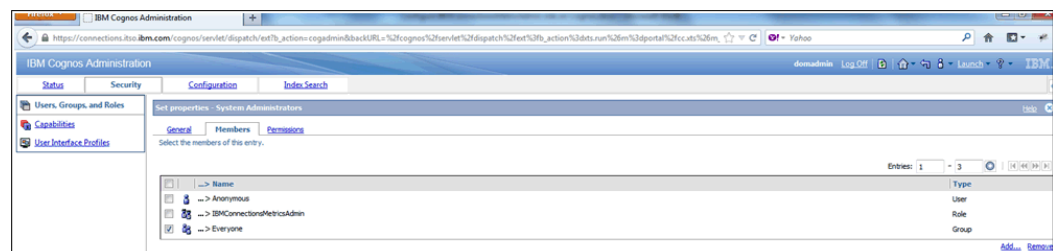
8. Select **Set Members**.
9. Go to **Members** and click **Add**.



10. Select **Show Users in the list** and click **IBMConnections** from the list.



11. Add **domadmin** user to the list. At least, the following users must be added to the list. The domadmin user ID is part of all the roles mentioned below.
  - The Cognos administrator
  - IBM Connection administrators
  - All users assigned to metrics-report-run role
12. Click **OK** to save the changes.
13. Go to **Security** → **Directory** → **Cognos**.
14. Search for the **System Administrators** role and select **More**.
15. Select the **Set Properties** icon
16. Select the **Members** tab.
17. Remove **Everyone** from the Members tab.



18. Click **OK** to save the changes.

## 6.11 Post installation IBM Connections configuration

After installation, you can configure IBM Connection to add the following features:

- ▶ Additional languages
- ▶ Media components
- ▶ Configuring and creating search indexes
- ▶ Setting up RSS feeds
- ▶ File size quotas
- ▶ Status update retention
- ▶ Trash file retention
- ▶ Application security roles
- ▶ Configuring moderation for connection applications

In this section, we describe how to configure IBM Connections to add additional languages, media components and creating search indexes.

### 6.11.1 Additional languages

IBM Connections server supports the following languages by default. The browser's language settings are

- ▶ Arabic
- ▶ Catalan
- ▶ Chinese - simplified and traditional
- ▶ Czech
- ▶ Danish
- ▶ Dutch



- ▶ Finnish
- ▶ French
- ▶ German
- ▶ Greek
- ▶ Hebrew
- ▶ Hungarian
- ▶ Italian
- ▶ Japanese
- ▶ Kazakh
- ▶ Korean
- ▶ Norwegian
- ▶ Polish
- ▶ Portuguese -- Brazilian and traditional
- ▶ Russian
- ▶ Slovenian
- ▶ Spanish
- ▶ Swedish
- ▶ Thai
- ▶ Turkish

To enable additional language, perform the following steps:

1. Create a temporary directory, for example “/opt/IBM/work” on the Deployment Manager.
2. Go to /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin and run the following command `/wsadmin.sh -lang jython -username domadmin -password itsoadmin`
3. Run the following command to initialize the IBM Connections server configuration file:  
`execfile("connectionsConfig.py")`

```
wsadmin>execfile("connectionsConfig.py")
Connections Administration initialized
```

4. Run the following command to check out the IBM Connections server configuration file:  
`LCConfigService.checkOutConfig("/opt/IBM/work","con-dmgrCell01")`

```
wsadmin>LCConfigService.checkOutConfig("/opt/IBM/work","con-dmgrCell01")
Connections configuration file successfully checked out
```

5. Go to **/opt/IBM/work** directory and modify the LotusConnections-Config.xml file as follows. Here we are adding English and French language and making the English language as default.

```
<languageSelector cookieDomain=".itso.ibm.com" cookieName="" defaultLanguage="en"
enabled="true" usePermanentCookie="false">
  <language lang="en">English</language>                                <!--English-->
  <language lang="fr">Fran\u00e7ais</language>                        <!--French-->
</languageSelector>
```

6. Save the changes to LotusConnections-Config.xml.
7. Run the following command to checkin the LotusConnections-Config.xml:  
`LCConfigService.checkInConfig("/opt/IBM/work","con-dmgrCell01")`

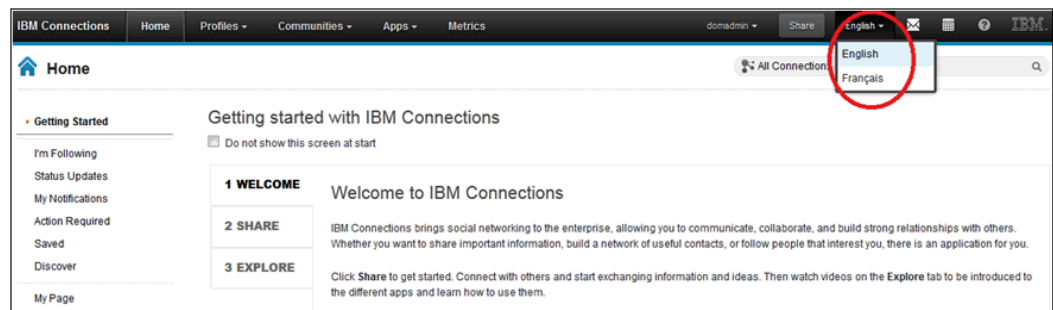
```
wsadmin>LCConfigService.checkInConfig("/opt/IBM/work","con-dmgrCell01")
Loading schema file for validation: /opt/IBM/work/LotusConnections-config.xsd
Loading schema file for validation: /opt/IBM/work/service-location.xsd
/opt/IBM/work/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
```

8. Run the following command to synchronize the nodes:

```
wsadmin>synchAllNodes()
Nodes synchronized
```

9. Restart the IBM Connections server.

10. Login to IBM Connections server homepage. A window similar to the following figure is displayed. Additional language is displayed in the dropdown.



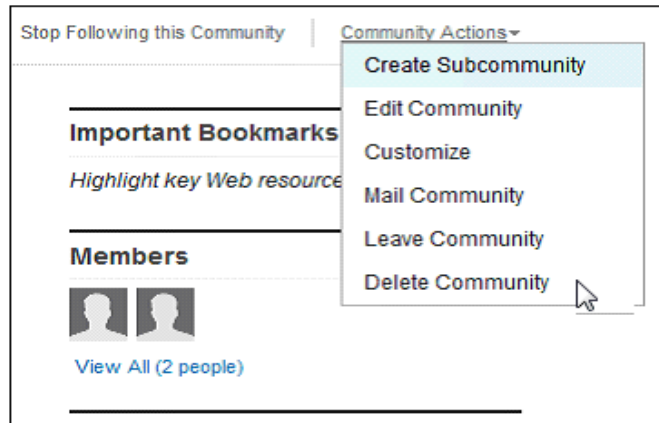
## 6.11.2 Media components

Media Galleries are community widgets that are used to store photos and videos. Administrator configures the widgets and community owners add the widgets into their community page. The following options are available to customize the media gallery widgets:

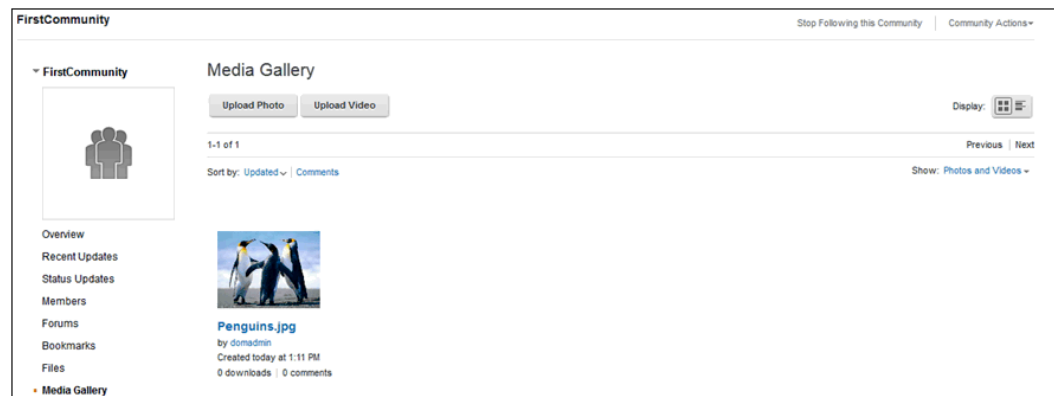
- ▶ Creating custom photo and video types
- ▶ Adding terms and conditions to the uploaded or downloaded photos and videos
- ▶ Changing the thumbnail preview image size
- ▶ Adding third party media player to play the photos and videos
- ▶ Setting the file extension for photos and videos
- ▶ Specifying the numbers seconds wait before upload fails

To add media gallery widget into the community, perform these steps:

1. Login to IBM Connections server.
2. Go to Community applications.
3. Select a community, for example "FirstCommunity".
4. Select **Community Actions** and click **Customize**.



5. Add Media Gallery widgets to the community.
6. Select Media Gallery widget and add photos or videos. A window similar to the following figure is displayed.



### 6.11.3 Configuring and creating search indexes

Search indexes are automatically created during the product installation. However, the indexes can be rebuilt if the index is corrupted or context root for the connections applications was changed.

Perform the following steps to create a search index:

1. Launch the WebSphere Application Server administrative console.
2. Go to **Environment** → **WebSphere Variables** and search for the variable "SEARCH\_INDEX\_DIR".
3. Select **SEARCH\_INDEX\_DIR** to find out the location of search index folder. On Linux, the location of search index folder is `/opt/IBM/Connections/data/local/search/index`.

**WebSphere Variables > SEARCH\_INDEX\_DIR**

Use this page to define substitution variables. Variables have a scope level, which is either server, conflicting scope values, the more granular scope value override cluster variables, which override cell variables.

Configuration

---

**General Properties**

\* Name  
SEARCH\_INDEX\_DIR

Value  
/opt/IBM/Connections/data/local/search

Description  
Search Index Files Directory

Apply OK Reset Cancel

4. Shutdown the search cluster.
5. Delete the index folder from each node. On Linux, the location of index folder is `/opt/IBM/Connections/data/local/search/index`.
6. Start all the nodes in search cluster.
7. Login to the deployment manager and launch the wsadmin client as follows.  
**./wsadmin.sh -lang jython -username domadmin -password itsoadmin**
8. Initialize the search configuration file by running the following command  
**execfile ("searchAdmin.py")**
9. Select the first node of search cluster.

```
wsadmin>execfile("searchAdmin.py")
1: WebSphere:cell=con-dmgrCell01,name=SearchService,type=LotusConnections,node=con-app01Node01,process=SearchCluster_server1
2: WebSphere:cell=con-dmgrCell01,name=SearchService,type=LotusConnections,node=con-app02Node01,process=SearchCluster_server2
Which service do you want to connect to?
1
Connecting to WebSphere:name=SearchAdminService,type=LotusConnections,cell=con-dmgrCell01,node=con-app01Node01,process=SearchCluster_server1
Search Administration initialized
wsadmin>
```

10. Run the following command to build the search index for IBM Connections applications.  
**SearchService.indexNowWithOptimization("activities,blogs,calendar,communities,dogear,files,forums,profiles,status\_updates,wikis")**
11. Go to `/opt/IBM/Connections/data/local/search/index` directory of first search cluster node. The presence of file `INDEX_READY` and `CRAWLING_VERSION` confirms that index is created successfully.



# High availability and disaster recovery

A system with high availability uses detection mechanisms, recovery, and fault masking to maintain the function of services for as long as possible, even during scheduled maintenance. This system should be designed, implemented, and deployed with a sufficient number of components (hardware, software, and procedures) to fulfill the high availability functionality. Redundancy is usually required to withstand failures in one or more of its components. A system with high availability service involves the following features:

- ▶ Redundancy structure
- ▶ Monitoring software layer
- ▶ Mechanism of synchronization

In this chapter, we discuss the high availability and disaster recovery implementation at the application server tier of an IBM Connections environment, including the following topics:

- ▶ 7.1, “Database management systems” on page 165
- ▶ 7.2, “Multiple LDAP servers” on page 166
- ▶ 7.3, “Edge Components Caching Proxy Server” on page 167
- ▶ 7.4, “Role of load balancers” on page 189

## 7.1 Database management systems

IBM Connections supports various relational database system including IBM DB2, Oracle, and Microsoft SQL Server. The database system is used to store all the application (Wiki, Blogs, and so on) data and holds other information for administration and maintenance. These data are vital business information and should be made available based on the business requirements that is usually 24x7 in today's business environment.

To support the high availability data, each vendor has its own high availability and disaster recovery features that you can implement in your IBM Connections environment. IBM DB2 High Availability and Disaster Recovery (HADR), automatic client reroute, Q-replication,

clustering support, and online backup are features that provides the capability of 24x7 data availability.

The IBM Connections data should be backed up regularly with database utility or by exporting data and back them up.

In this wiki, we use IBM DB2 as the repository for the IBM Connections data. For more information about the DB2 high availability and disaster recovery options, see

High Availability and Disaster Recovery Options for DB2 for Linux, UNIX, and Windows <http://www.redbooks.ibm.com/abstracts/sg247363.html>, SG24-7363.

## 7.2 Multiple LDAP servers

Lightweight Directory Access Protocol (LDAP) is a standard Internet protocol for searching and managing objects in a directory. The directory contains many types of entries, such as entries for users, groups, encryption certificates and other services on a network. LDAP server is a server that has a collection of information in some organized and hierarchical way and implements LDAP protocol to communicate with clients.

Besides the possibility to manage all this information, another function of LDAP is to provide authentication of a user. By sharing the authentication information it is possible to provide "single sign on" where one password for a user is shared between many services. This makes LDAP server a critical resource. Having multiple LDAP servers to ensure that the organization can access user data at the corporate directory at any time is one of the high availability common practice for a large IBM Connections deployment. The benefits of multiple LDAP servers setup include:

- ▶ High availability

If the LDAP server failed, the authentication mechanism of the IBM Connections systems cannot be performed. When multiple LDAP servers are set up in a cluster, you can provide the continue service by failed the failed LDAP server to one of the healthy one.

- ▶ Separating users

You can use multiple LDAP servers to fulfill the requirement of maintaining different sets of users, for example, users in corporate level and department level or application level information.

- ▶ Different schema

Another common usage of multiple LDAP servers is for adding users from a newly acquired company before the infrastructure is integrated. A separate LDAP server can be used for the users from the acquired company. In this case, you have to support authentication against different schemas.

You can configure IBM Connections to work with multiple LDAP servers and multiple contexts through the IBM WebSphere Application Server. When using multiple LDAP servers, note the following:

- ▶ LDAP servers store user's information, and users must only exist in one LDAP server (not multiple).
- ▶ The distinguished name (DN) of the base entry must be unique (the subtree name is unique) among the multiple LDAP servers.

## 7.3 Edge Components Caching Proxy Server

A reverse proxy allows static content to be stored locally in proxy server, reducing the workload on the application server. The Edge Components Caching Proxy Server intercepts http requests from a browser. It retrieves the requested information from the content-hosting systems. The retrieved content is stored in a local cache for subsequent requests. Delivering content directly from local cache improves the performance. Although reverse proxy is optional in an IBM Connections environment, a reverse proxy can improve the performance of the IBM Connections systems.

We can configure the reverse proxy to cache parts of the IBM Connections user interface which don't change regularly, such as the navigation bar, footers and so on. In this way the Application server is asked only for the dynamic parts, served ultimately from the database and presented as a web page. This reduction in the requests eases the load on the WebSphere Application Servers and thus increases the performance of the solution.

In our lab environment, we configure Edge Components Caching Proxy Server on two servers for high availability (HA) purpose. In this section, we show the installation and configuration process in the following sections:

- ▶ 7.3.1, “Installing Edge Components Caching Proxy Server” on page 167: Procedure to install Edge Components Caching Proxy Server
- ▶ 7.3.2, “Configuring Edge Components Caching Proxy Server” on page 171: Procedure to set up Edge Components Caching Proxy Server
- ▶ 7.3.3, “Configuring SSL support on Edge Components Caching Proxy Server” on page 177: Procedure to secure the connection between the client browsers and Edge Components Caching Proxy Server using SSL
- ▶ 7.3.4, “Configuring disk cache on Edge Components Caching Proxy server” on page 187: Procedure to configure Edge Components Caching Proxy Server to use disk cache

### 7.3.1 Installing Edge Components Caching Proxy Server

You can install IBM Edge Component Caching Proxy of WebSphere Application Server Network Deployment by using either the graphical installation wizard or the operating system software installation commands.

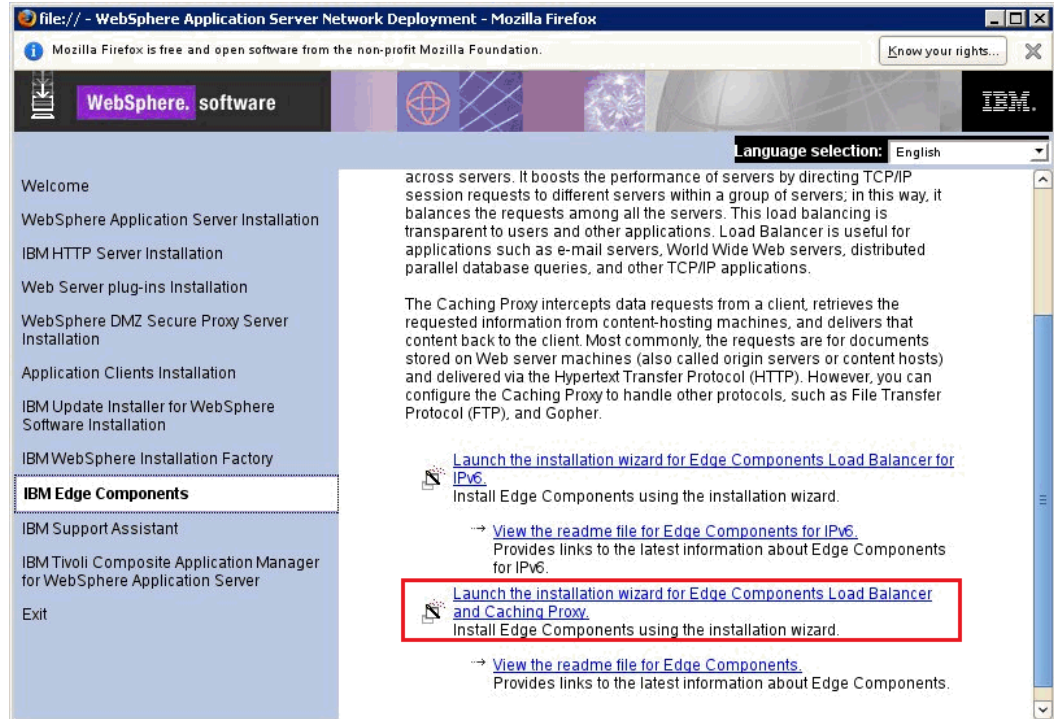
The IBM Edge Component Caching Proxy allows you to cache IBM Connections content. In our lab environment, we set up two proxy server to provide failover and workload balancing to HTTP clients (Internet browsers) when they access Edge cache servers. The installation and configuration process must be applied to each proxy server.

#### Installing Edge Caching Proxy using the installation wizard

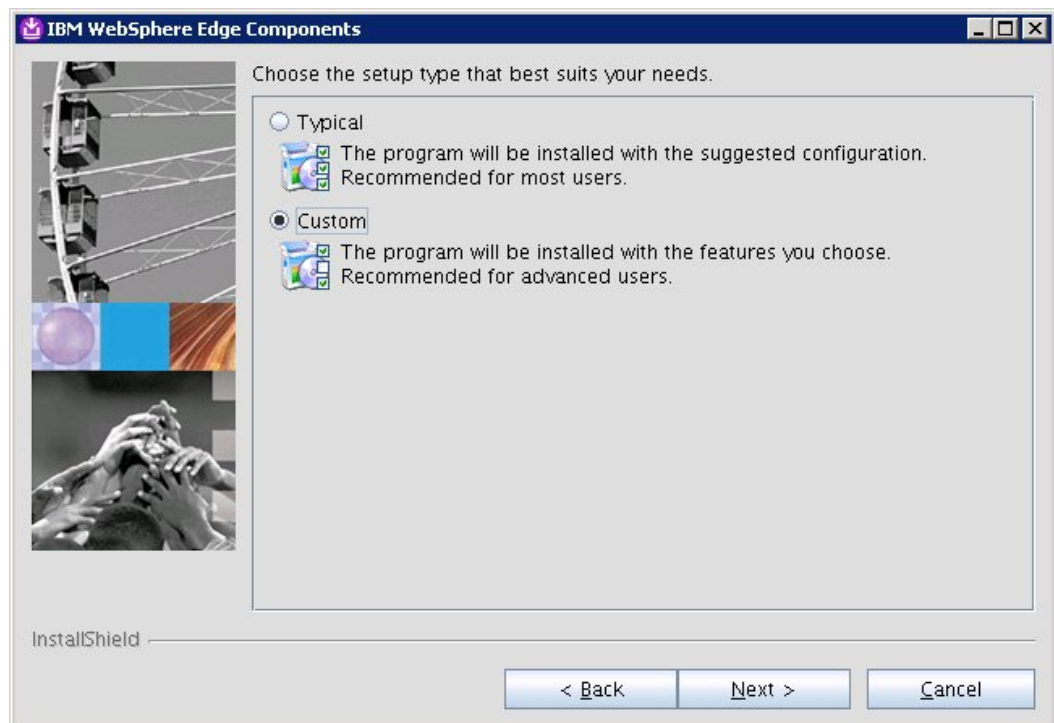
Follow these steps to install the Edge Component Caching Proxy component:

1. Unzip the WebSphere Edge Components into a temporary directory (for example, /tmp or c:\temp), and run the installation wizard as follow:
  - Linux:  
`# 1launchpad.sh`
  - Microsoft Windows:  
`> 1launchpad.bat`
2. In the Welcome window, **choose Launch the installation wizard for Edge Components Load Balancer and Cache Proxy:**

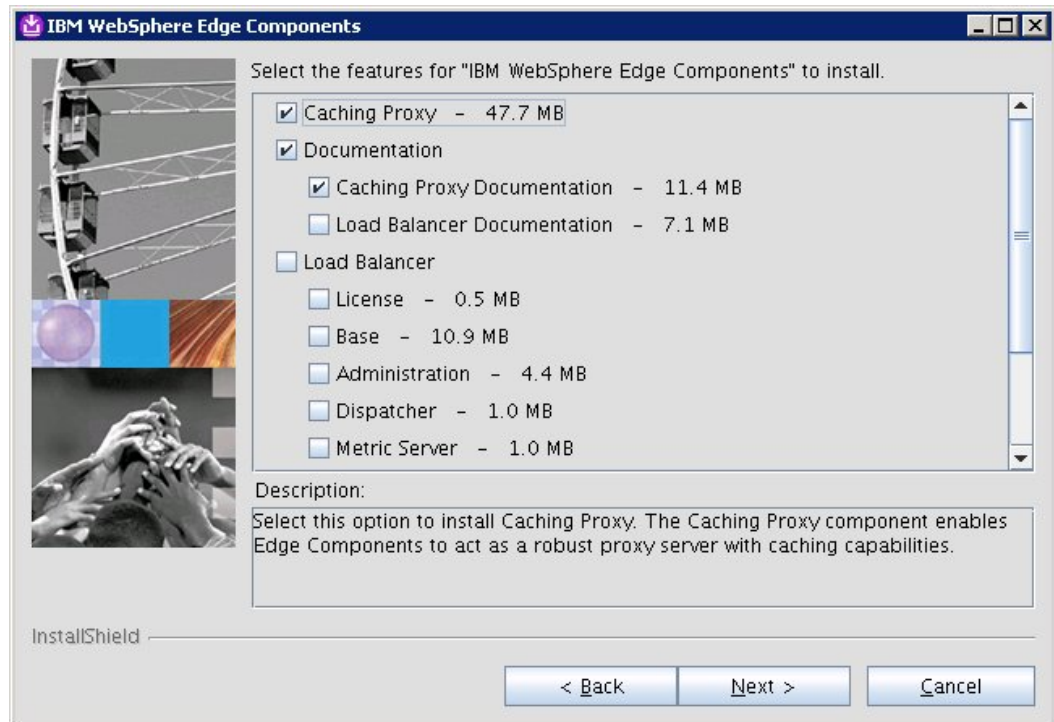




3. Accept the license agreement.
4. English is the default supported language. You can choose another language if you wish.
5. For setup type, select **Custom** to choose the components to be installed.



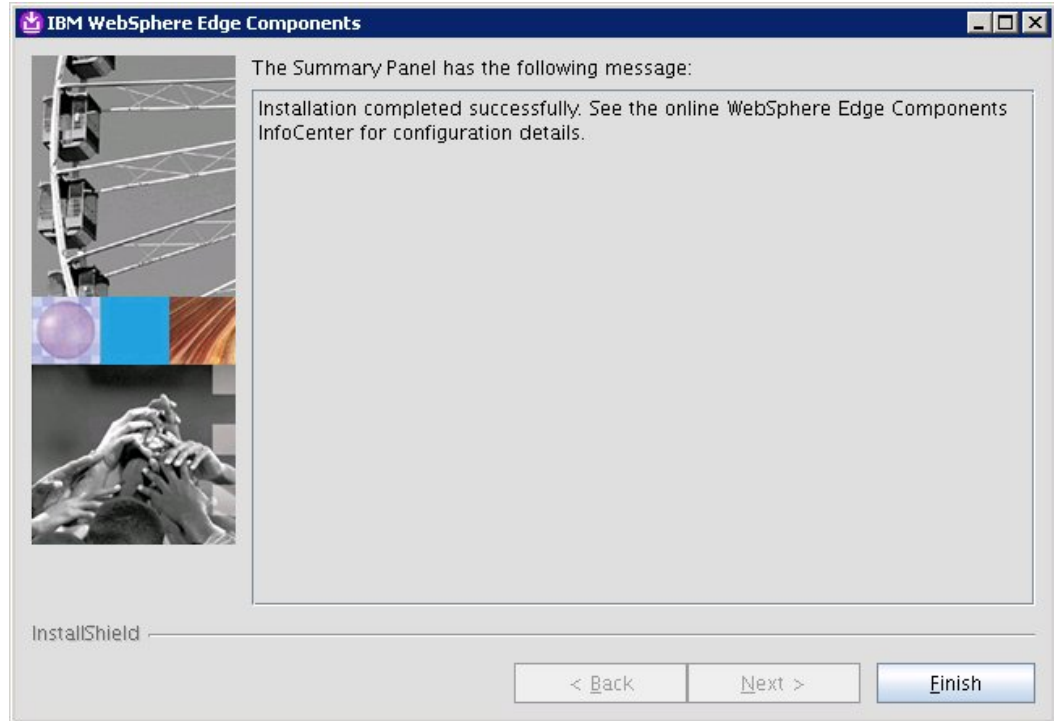
6. Select **Caching Proxy and Caching Proxy Documentation** to install.



7. Validate if all features defined are correct, and click **Next** to continue the installation.



8. The installation wizard shows that Edge Components were installed successfully. Click **Finish**.



## Installing Edge Component Caching Proxy using command

In a Linux environment, if you do not have a graphical environment for installation, you can use the operating system installation commands to Edge Components.

The following are installation procedure with the **rpm** commands:

1. Unzip the WebSphere Edge Components into a temporary directory (for example, /root/temp)
 

```
# mkdir temp
# cd temp
# tar -xvzf ../C1I7NML.tar.gz
```
2. Go to the software directory:
 

```
# cd /root/temp/
```
3. Install Edge Caching Proxy package using the following command (**pay attention for the line break**)
 

```
# rpm -ivh cp/admin/WSES_Admin_Runtime-7.0.0-0.i686.rpm
cp/icu/WSES_ICU_Runtime-7.0.0-0.i686.rpm
cp/cp/WSES_CachingProxy-7.0.0-0.i686.rpm
cp/cp/WSES_CachingProxy_msg_en_US-7.0.0-0.i686.rpm
GSKit/gsk7bas-7.0-4.17.i386.rpm
```
4. The following figure shows the output of the **rpm** command.

```

Preparing... ##### [100%]
1:WSES_ICU_Runtime ##### [ 20%]
2:WSES_CachingProxy_msg_e##### [ 40%]
3:gsk7bas ##### [ 60%]
4:WSES_Admin_Runtime ##### [ 80%]
5:WSES_CachingProxy ##### [100%]
The proxy has been started and is functional.

```

### 7.3.2 Configuring Edge Components Caching Proxy Server

To use the Edge Component Caching Proxy Server in an IBM Connections environments, you must create certain rules to enable a user to connect successfully to IBM Connections through the proxy server. There are two types of rules:

- ▶ **Global rules:** The global rules define the behavior of the Edge Component Caching Proxy server such as only proxy, proxy caching more, and expiration time.
- ▶ **Specific rules:** These rules adjust the Edge Component Caching Proxy server to communicate with the services that stand behind proxy machines in your environment.

These rules are enabled by modify the configuration file *ibmproxy.conf*. After made rule changes, you must restart Edge Component Caching Proxy to apply the required changes.

Ensure that you have installed IBM® WebSphere® Edge Components V6.1, which is supplied with IBM Connections 4.

**Note:** For more information, see WebSphere Edge Components Information Center <http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.edge.doc/edge/concepts.htm>.

Complete the following steps to configure the Edge Component Caching Proxy server:

1. Stop the Edge Component Caching Proxy server:
  - Linux: Run the following command
 

```
# /etc/init.d/ibmproxy stop
```
  - Windows:
 

Click **Start** → **Administrative Tools** → **Services**.

In the Services window, highlight **Caching Proxy** and click **Stop** to initiate the Caching Proxy service.
2. Go to Edge components configuration directory
  - Linux: Run the following command:
 

```
# cd /opt/ibm/edge/cp/etc/en_US
```
  - Windows:
 

```
cd C:\Program Files\IBM\edge\cp\etc\
```
3. Edit the *ibmproxy.conf* configuration file for the Edge Components using a text editor and add or change the following variables:

---

```

CompressionFilterEnable /opt/ibm/edge/cp/lib/mod_z.so
CompressionFilterAddContentType text/plain
CompressionFilterAddContentType text/html
CompressionFilterAddContentType text/xml

```

```
CompressionFilterAddContentType text/xml
CompressionFilterAddContentType text/css
CompressionFilterAddContentType text/javascript
CompressionFilterAddContentType application/x-javascript
CompressionFilterAddContentType application/javascript
CompressionFilterAddContentType application/xml
CompressionFilterAddContentType application/xhtml+xml
CompressionFilterAddContentType application/atom+xml
CompressionFilterAddContentType application/octet-stream
```

```
MaxActiveThreads 700
ServerConnPool on
ServerConnTimeout 5 seconds
ServerConnGCRun 1 minutes
```

```
CacheTimeMargin 0 seconds
SendRevProxyName yes
```

```
PureProxy off
CacheTimeMargin 0 minutes
KeepExpired On
Enable CONNECT
Enable PUT
Enable DELETE
CacheQueries PUBLIC
LimitRequestBody 100 M
```

---

4. Continue to edit the *ibmproxy.conf* configuration file using a text editor, and change according to your environment:

- Define the amount of memory to associate with the cache memory.

This is done by specifying CacheMemory amount directive using the following format:

```
CacheMemory amount {B | K | M | G}
```

The amount can be specified in one of the following units: bytes (B), kilobytes (K), megabytes (M), and gigabytes (G).

For example: **CacheMemory 1200 M**

- Define the reverse pass rules:

The ReversePass rule has the following formats:

```
ReversePass http://* http://*
```

```
ReversePass https://* https://
```

where is the host name of the HTTP server. The \* in the URL to indicate that all URLs will be sent to back-end server.

For example:

#### **ReversePass**

```
http://con-lb01.itso.ibm.com/*http://connections.itso.ibm.com/*
```

#### **ReversePass**

```
https://con-lb01.itso.ibm.com/*https://connections.itso.ibm.com/*
```

- Define the proxy rule:

The proxy directive indicates which protocols the caching proxy is to process and map a request to a server. The following are examples used in our lab exercise:

**Proxy** /\*http://con-lb01.itso.ibm.com/\* :80

**Proxy** /\*https://con-lb01.itso.ibm.com/\* :443

- Change the Pass directory to return to IBM Connections default URL and not to the Edge Caching Admin page:

**# Pass** /\* /opt/ibm/edge/cp/server\_root/pub/en\_US/\*

**Pass** /pub/\* /opt/ibm/edge/cp/server\_root/pub/en\_US/\*

5. Instructs the Edge Caching Proxy server to not to attempt to cache non-cacheable requests.

We use *NoCaching* directive to tell the server not to cache files with the URLs that match the specified template.

---

NoCaching http:/\*activities/service/atom/\*

NoCaching http:/\*activities/service/atom2/\*

NoCaching http:/\*activities/service/atom2/forms/\*

NoCaching http:/\*activities/service/download/\*

NoCaching http:/\*activities/service/download/forms/\*

NoCaching http:/\*activities/service/getnonce

NoCaching http:/\*activities/service/getnonce/forms

NoCaching http:/\*blogs/api\*

NoCaching http:/\*blogs/api\_form\*

NoCaching http:/\*blogs/approvedmsg.jsp\*

NoCaching http:/\*blogs/confirmflagged.jsp\*

NoCaching http:/\*blogs/notify.jsp\*

NoCaching http:/\*blogs/notifiedit.jsp\*

NoCaching http:/\*blogs/notifyflagged.jsp\*

NoCaching http:/\*blogs/notifyquarantined.jsp\*

NoCaching http:/\*blogs/ownermsg.jsp\*

NoCaching http:/\*blogs/roller-services/\*

NoCaching http:/\*blogs/roller-ui/admin\*

NoCaching http:/\*blogs/roller-ui/createWebsite.do\*

NoCaching http:/\*blogs/roller-ui/favorites\*

NoCaching http:/\*blogs/roller-ui/homepage\*

NoCaching http:/\*blogs/roller-ui/myupdates\*

NoCaching http:/\*blogs/roller-ui/rendering/api/\*

NoCaching http:/\*blogs/roller-ui/rendering/api\_form/\*

NoCaching http:/\*blogs/roller-ui/scripts/authCheck.jsp\*

NoCaching http:/\*blogs/roller-ui/servermetrics.do\*

NoCaching http:/\*blogs/roller-ui/yourWebsites.do\*

NoCaching http:/\*blogs/services/atom\*

NoCaching http:/\*blogs/services/atom\_form\*

NoCaching http:/\*blogs/services/xmlrpc\*

NoCaching http:/\*bookmarklet/post/\*

NoCaching http:/\*communities/dsx/\*

NoCaching http:/\*communities/forum/service/atom/\*

NoCaching http:/\*communities/service/atom/communities/my\*

NoCaching http:/\*communities/service/atom/community\*

NoCaching http:/\*communities/service/forum/get/nonce

NoCaching http:/\*communities/service/json/communityview\*

NoCaching http:/\*dogear/atom/inbox/\*

NoCaching http:/\*dogear/atom/mybookmarks/\*

NoCaching http://\*/dogear/atom/mynotifications/\*  
NoCaching http://\*/dogear/atom/mysentnotifications/\*  
NoCaching http://\*/dogear/html/inbox/\*  
NoCaching http://\*/dogear/html/mybookmarks/\*  
NoCaching http://\*/dogear/html/mynotifications/\*  
NoCaching http://\*/dogear/html/mysentnotifications/\*  
NoCaching http://\*/dogear/seedlist/\*  
NoCaching http://\*/dogear/templates/\*

NoCaching http://\*/files/form/authenticated

NoCaching http://\*/homepage/web/getuserpref  
NoCaching http://\*/homepage  
NoCaching http://\*/homepage/web/widgets  
NoCaching http://\*/homepage/web/jsp/\*.jsp  
NoCaching http://\*/homepage/web/servermetrics  
NoCaching http://\*/homepage/admin/admin.jsp  
NoCaching http://\*/homepage/atom/search/\*  
NoCaching http://\*/homepage/atom/mysearch/\*

NoCaching http://\*/mobile/activities/\*  
NoCaching http://\*/mobile/blogs/\*  
NoCaching http://\*/mobile/profiles/\*

NoCaching http://\*/profiles/aboutView.do  
NoCaching http://\*/profiles/home.do\*  
NoCaching http://\*/profiles/html/\*.do

NoCaching http://\*/search/atom/mysearch  
NoCaching http://\*/search/serverStats  
NoCaching http://\*/search/web/\*

NoCaching http://\*/wikis/basic/api/\*  
NoCaching http://\*/wikis/dm/atom/\*  
NoCaching http://\*/wikis/form/api/\*  
NoCaching http://\*/wikis/form/authenticated  
NoCaching http://\*/wikis/seedlist/\*  
NoCaching http://\*/wikis/templates/about.jsp\*  
NoCaching http://\*/wikis/templates/demo.jsp\*  
NoCaching http://\*/wikis/templates/faq/en/tour1.jsp\*  
NoCaching http://\*/wikis/templates/statistics.jsp\*  
NoCaching http://\*/wikis/templates/toolbox.jsp\*

We also apply NoCaching directive to https (ssl) communicator:

NoCaching https://\*/activities/service/atom/\*  
NoCaching https://\*/activities/service/atom2/\*  
NoCaching https://\*/activities/service/atom2/forms/\*  
NoCaching https://\*/activities/service/download/\*  
NoCaching https://\*/activities/service/download/forms/\*  
NoCaching https://\*/activities/service/getnonce  
NoCaching https://\*/activities/service/getnonce/forms

NoCaching https://\*/blogs/api\*  
NoCaching https://\*/blogs/api\_form\*  
NoCaching https://\*/blogs/approvedmsg.jsp\*

NoCaching https://\*/blogs/confirmflagged.jsp\*  
 NoCaching https://\*/blogs/notify.jsp\*  
 NoCaching https://\*/blogs/notifiedit.jsp\*  
 NoCaching https://\*/blogs/notifyflagged.jsp\*  
 NoCaching https://\*/blogs/notifyquarantined.jsp\*  
 NoCaching https://\*/blogs/ownermsg.jsp\*  
 NoCaching https://\*/blogs/roller-services/\*  
 NoCaching https://\*/blogs/roller-ui/admin\*  
 NoCaching https://\*/blogs/roller-ui/createWebsite.do\*  
 NoCaching https://\*/blogs/roller-ui/favorites\*  
 NoCaching https://\*/blogs/roller-ui/homepage\*  
 NoCaching https://\*/blogs/roller-ui/myupdates\*  
 NoCaching https://\*/blogs/roller-ui/rendering/api/\*  
 NoCaching https://\*/blogs/roller-ui/rendering/api\_form/\*  
 NoCaching https://\*/blogs/roller-ui/scripts/authCheck.jsp\*  
 NoCaching https://\*/blogs/roller-ui/servermetrics.do\*  
 NoCaching https://\*/blogs/roller-ui/yourWebsites.do\*  
 NoCaching https://\*/blogs/services/atom\*  
 NoCaching https://\*/blogs/services/atom\_form\*  
 NoCaching https://\*/blogs/services/xmlrpc\*  
 NoCaching https://\*/bookmarklet/post/\*

NoCaching https://\*/communities/dsx/\*  
 NoCaching https://\*/communities/forum/service/atom/\*  
 NoCaching https://\*/communities/service/atom/communities/my\*  
 NoCaching https://\*/communities/service/atom/community\*  
 NoCaching https://\*/communities/service/forum/get/nonce  
 NoCaching https://\*/communities/service/json/communityview\*

NoCaching https://\*/dogear/atom/inbox/\*  
 NoCaching https://\*/dogear/atom/mybookmarks/\*  
 NoCaching https://\*/dogear/atom/mynotifications/\*  
 NoCaching https://\*/dogear/atom/mysentnotifications/\*  
 NoCaching https://\*/dogear/html/inbox/\*  
 NoCaching https://\*/dogear/html/mybookmarks/\*  
 NoCaching https://\*/dogear/html/mynotifications/\*  
 NoCaching https://\*/dogear/html/mysentnotifications/\*  
 NoCaching https://\*/dogear/seedlist/\*  
 NoCaching https://\*/dogear/templates/\*

NoCaching https://\*/files/form/authenticated

NoCaching https://\*/homepage/web/getuserpref  
 NoCaching https://\*/homepage  
 NoCaching https://\*/homepage/web/widgets  
 NoCaching https://\*/homepage/web/jsp/\*.jsp  
 NoCaching https://\*/homepage/web/servermetrics  
 NoCaching https://\*/homepage/admin/admin.jsp  
 NoCaching https://\*/homepage/atom/search/\*  
 NoCaching https://\*/homepage/atom/mysearch/\*

NoCaching https://\*/mobile/activities/\*  
 NoCaching https://\*/mobile/blogs/\*  
 NoCaching https://\*/mobile/profiles/\*



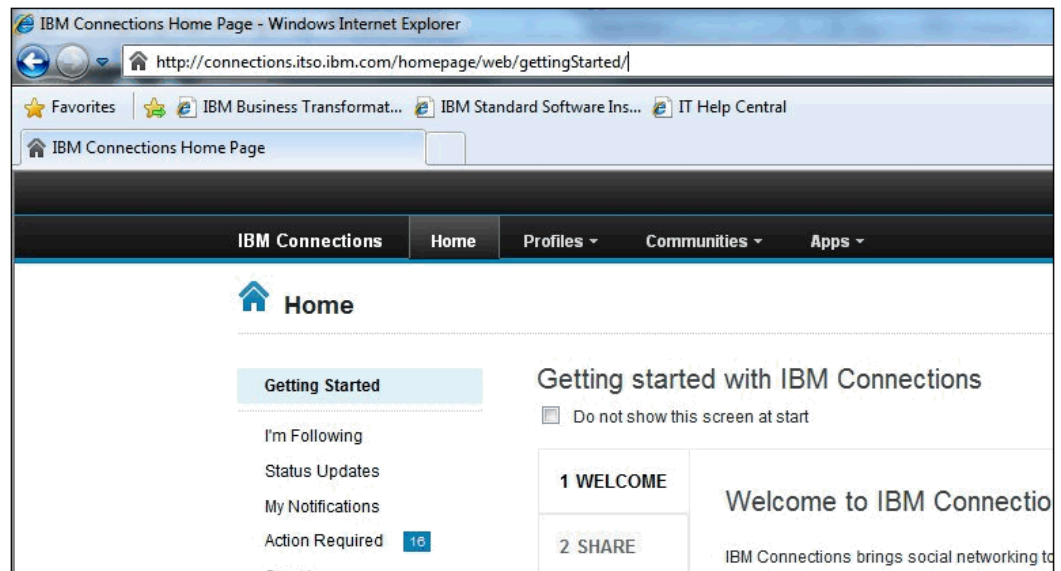
```
NoCaching https://*/profiles/aboutView.do
NoCaching https://*/profiles/home.do*
NoCaching https://*/profiles/html/*.do

NoCaching https://*/search/atom/mysearch
NoCaching https://*/search/serverStats
NoCaching https://*/search/web/*

NoCaching https://*/wikis/basic/api/*
NoCaching https://*/wikis/dm/atom/*
NoCaching https://*/wikis/form/api/*
NoCaching https://*/wikis/form/authenticated
NoCaching https://*/wikis/seedlist/*
NoCaching https://*/wikis/templates/about.jsp*
NoCaching https://*/wikis/templates/demo.jsp*
NoCaching https://*/wikis/templates/faq/en/tour1.jsp*
NoCaching https://*/wikis/templates/statistics.jsp*
NoCaching https://*/wikis/templates/toolbox.jsp*
```

---

6. Save and close the file.
7. Start the Edge Server
  - Linux:  
**# /etc/init.d/ibmproxy start**
  - Windows:  
Click **Start** → Administrative Tools → **Services**.  
In the Services window, highlight **Caching Proxy**.  
Click **Start** to initiate the Caching Proxy service.
8. Access the web server using https from a web browser, in our example,  
<http://connections.itso.ibm.com/>



### 7.3.3 Configuring SSL support on Edge Components Caching Proxy Server

You must complete these steps to secure the connection between the client browsers and Edge Components with Socket Secure Layer (SSL) so all communications are encrypted.

In our example, we use self-sign certificate to enabling SSL. The steps to configure SSL are as follows:

- ▶ “Creating an SSL certificate on Edge Components Caching Proxy server”:  
Using Ikeyman to create a person SSL certificate to be used in the Edge Components Caching Proxy Server
- ▶ “Extracting personal self-signed SSL certificate from IBM HTTP Server” on page 181:  
Using Ikeyman to extract an SSL certificate from IBM HTTP server to be used in Edge Components Caching Proxy Server
- ▶ “Importing an SSL certificate into Edge Components Caching Proxy server” on page 183:  
Importing self-signed certificate from IBM HTTP server into Edge Components Caching Proxy Server to be a trusted certificate
- ▶ “Configuring the SSL certificate on the Edge Components Caching Proxy server” on page 186:  
Configuring the SSL certificate into Edge Components Caching Proxy Server and accessing IBM Connections.

#### Creating an SSL certificate on Edge Components Caching Proxy server

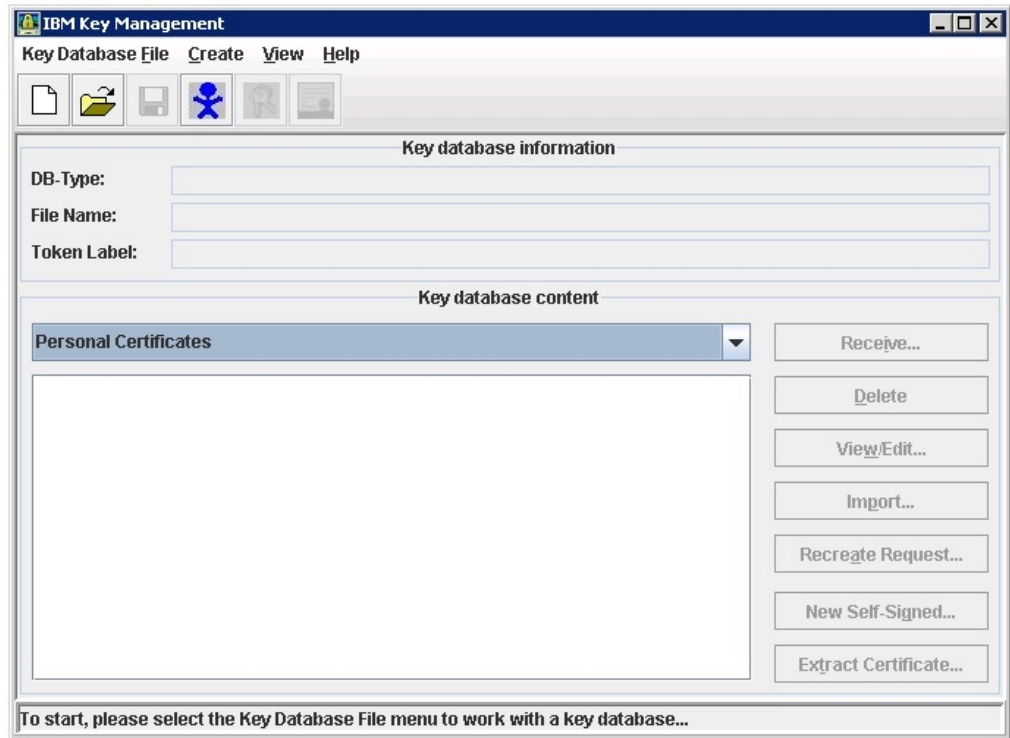
To enable SSL on the IBM Edge Components, you must use the key management utility, *iKeyman*, to create a key for securing your network communications.

This key is defined in the IBM Edge Components configuration file.

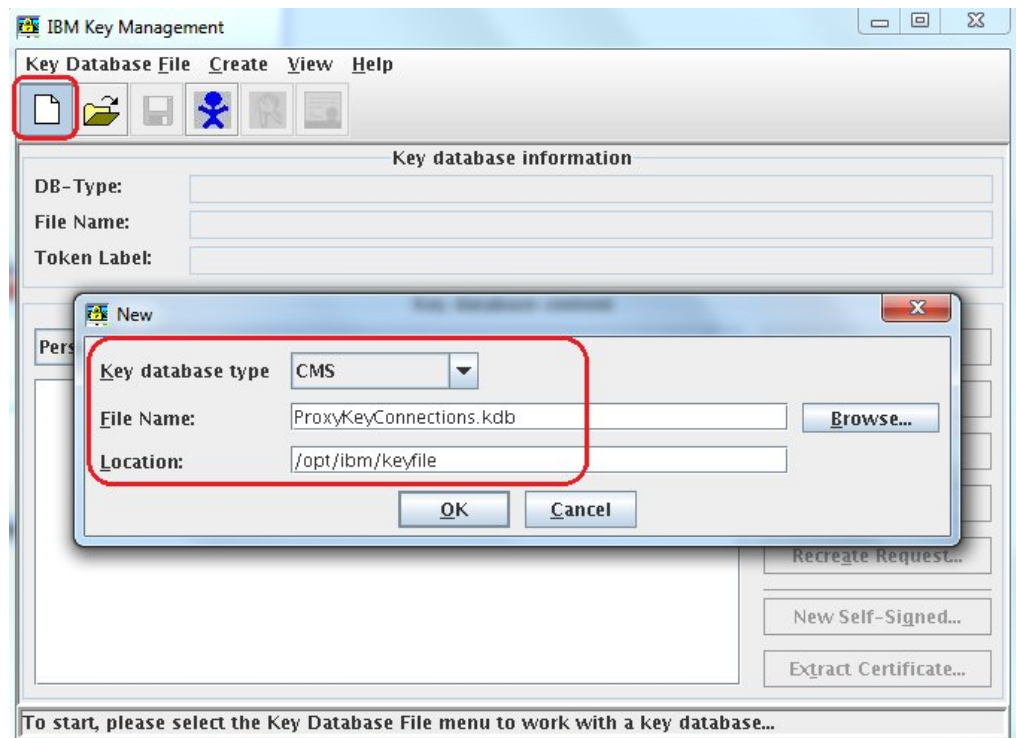
**Note:** For more information about enabling SSL on the IBM Edge Components, see WebSphere Application Server Information Center [http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=%2Fcom.ibm.webspere.ihs.doc%2Finfo%2Fihs%2Fihs%2Fwelc\\_ikeymangui.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v6r1/index.jsp?topic=%2Fcom.ibm.webspere.ihs.doc%2Finfo%2Fihs%2Fihs%2Fwelc_ikeymangui.html) .

The following are the steps to create an SSL key:

1. On the IBM Edge Components installation directory, run **ikeyman** to open the key management utility:
  - AIX/Linux: # **./ikeyman**
  - Microsoft Windows: > **ikeyman**

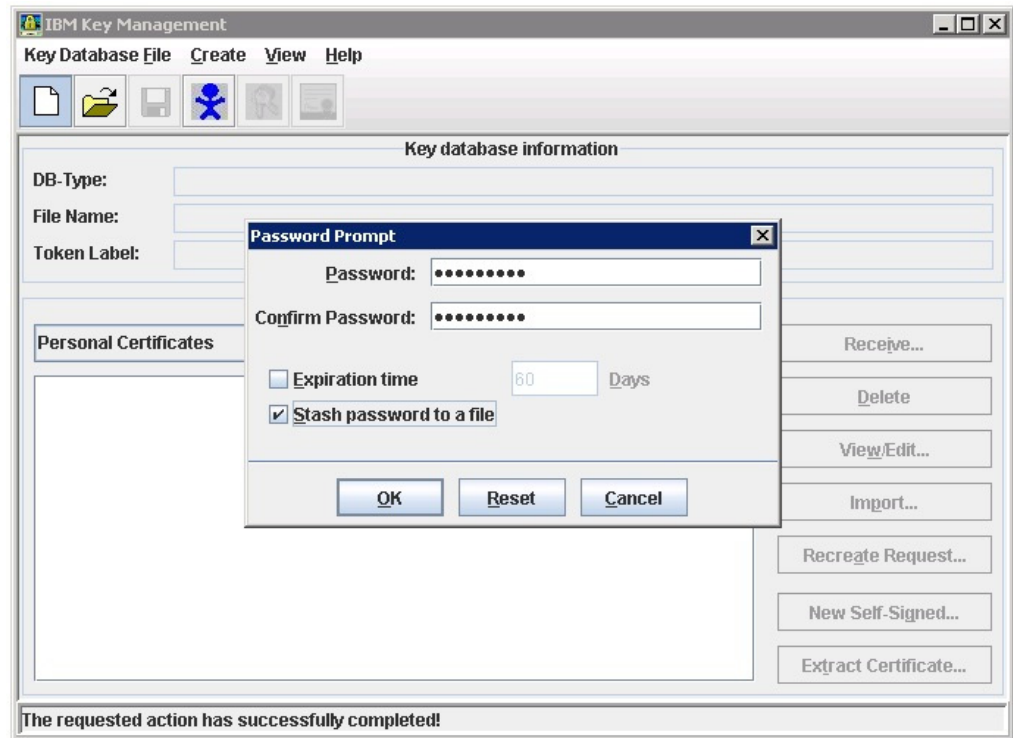


2. From the menu bar, select **Key Database File** → **New** and complete these fields:
  - *Key database type*: Select **CMS**
  - *File Name*: **ProxyKeyConnections.kdb**
  - *Location*: The file location, for example, **/opt/ibm/keyfile**

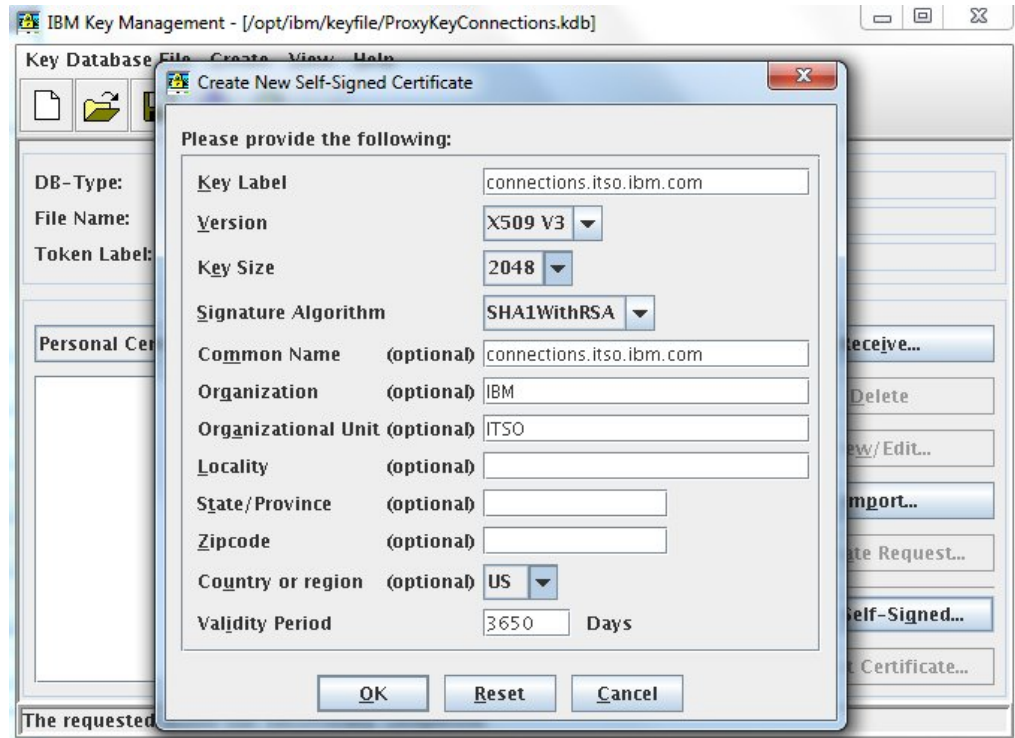


3. On the password prompt, complete the values:

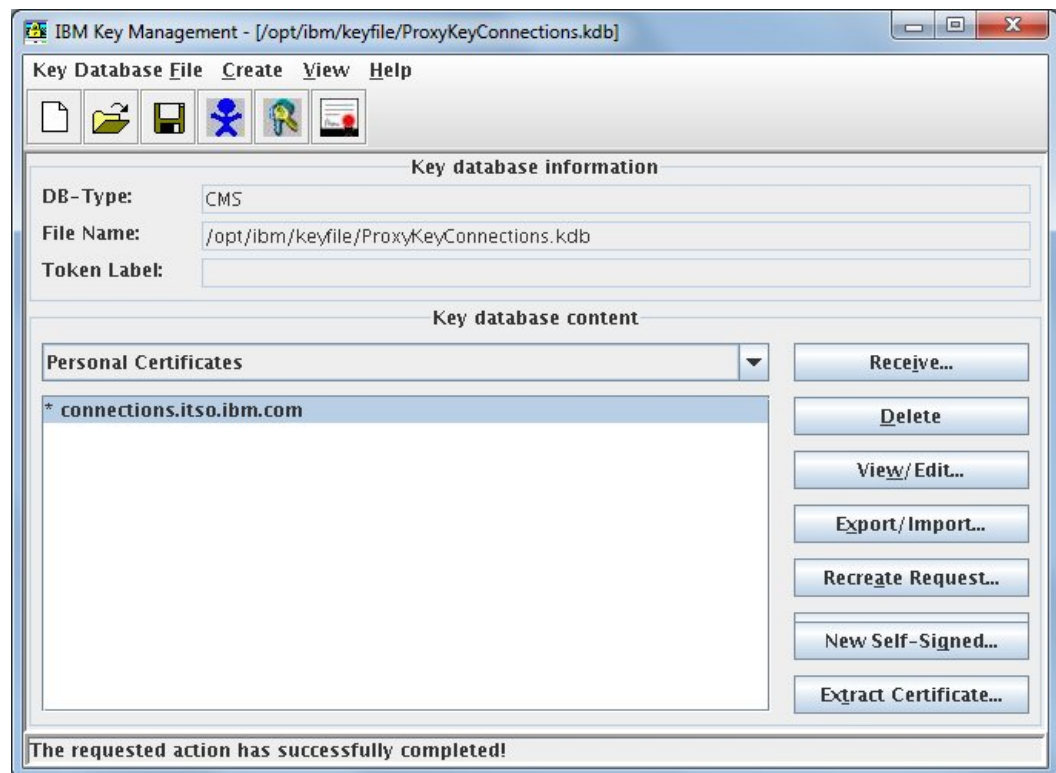
- Define and confirm a password.
- Check **Stash password to a file**



- From menu bar, select **Create** → **New** → **Self-Sign Certificate** and fill the following options:
  - *Key Label*: Define a label to identify your certificate on the key file, for example, **connections.itso.ibm.com**
  - *Version*: Define the SSL version to **X509 V3**
  - *Key Size*: Set the size to **2048**
  - *Signature Algorithm*: Define the signature to **SHA1WithRSA**
  - *Common Name*: Define the full qualified domain name (FQDN) that you choose to access your IBM Connections, for example, **connections.itso.ibm.com**
  - *Organization Name*: Define the organization name, for example, **IBM**
  - *Organization*: Define your unit, for example, **ITSO**
  - *Country or region*: Select your country, for example, **US**
  - *Validity period*: Set the days that the certificate is valid, for example, **3650** days



5. You have finished of creating SSL certificate, see result:



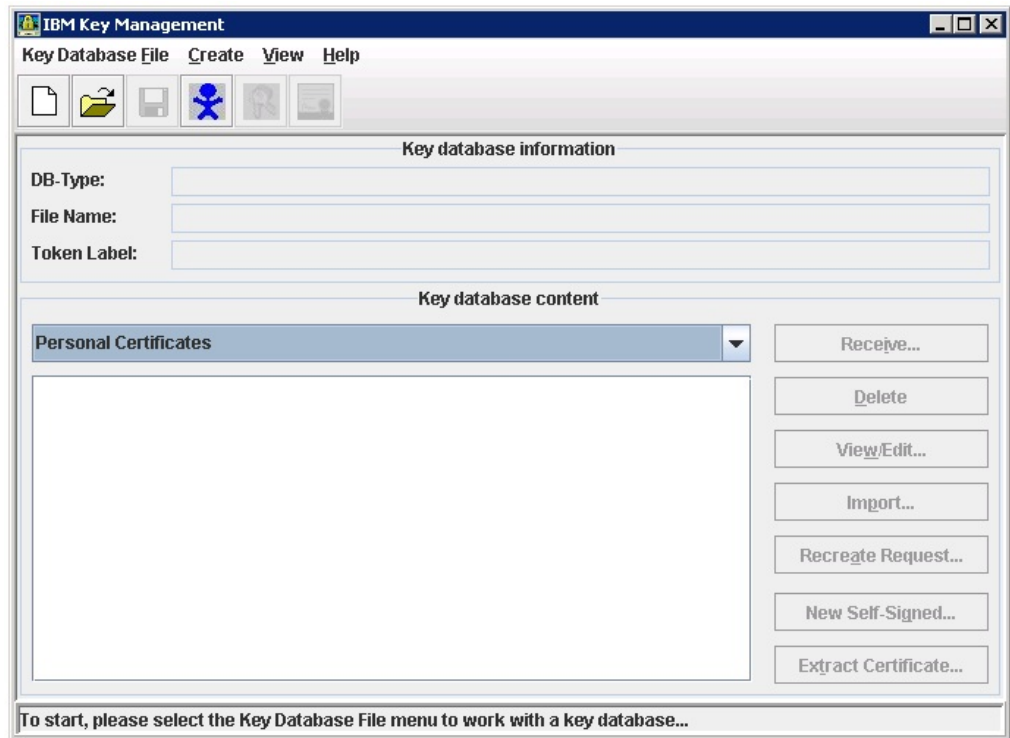
Next step is to extract the an SSL certificate from IBM HTTP server to import into the IBM Edge Components Cache Proxy server.

## Extracting personal self-signed SSL certificate from IBM HTTP Server

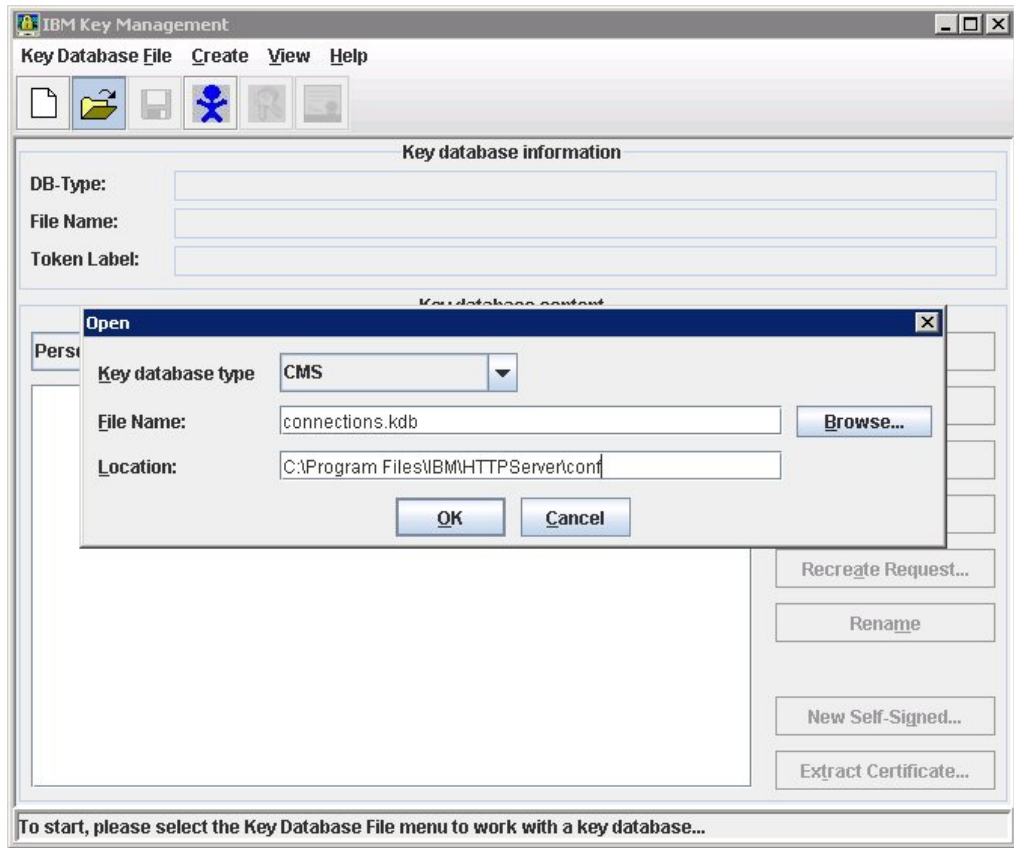
This step is to extract the self-signed SSL certificate from IBM HTTP server to which the IBM Connections connects for importing to Edge Component Caching Proxy server.

Complete the following steps to extract a personal SSL certificate from IBM HTTP Server to be used in the Edge Components Caching Proxy server:

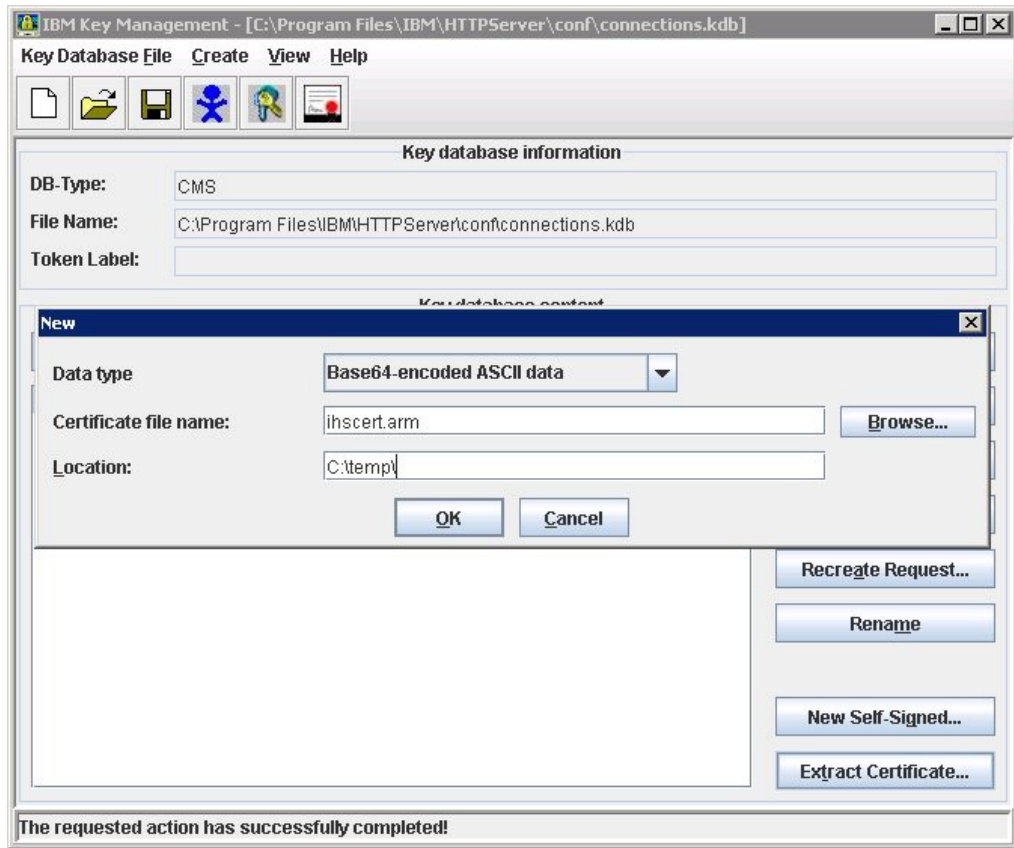
1. On the IBM HTTP Server installation directory, run ikeyman to open the key management utility:
  - Linux: # **./ikeyman**
  - Microsoft Windows: > **.\ikeyman**



2. From the menu bar, select **Key Database File** → **Open**. Complete these fields:
  - *Key database type*: Select **CMS**.
  - *File Name*: **connections.kdb**
  - *Location*: The conf file location of HTTP server such as **c:\Program Files\IBM\HTTPServer\conf**



3. On the password prompt, provide a password and click **OK**.
4. Select **WebSphere Plugin Key**, click **Extract Certificate**, and complete the following fields:
  - *Data type*: Select **Base64-encoded ASCII**
  - *Certificate file name*: **ihscert.arm**
  - *Location*: The directory to place the extracted certificate, for example, **c:\temp\**



Next step is to import this SSL certificate extracted from IBM HTTP server into the Edge Component Caching Proxy server.

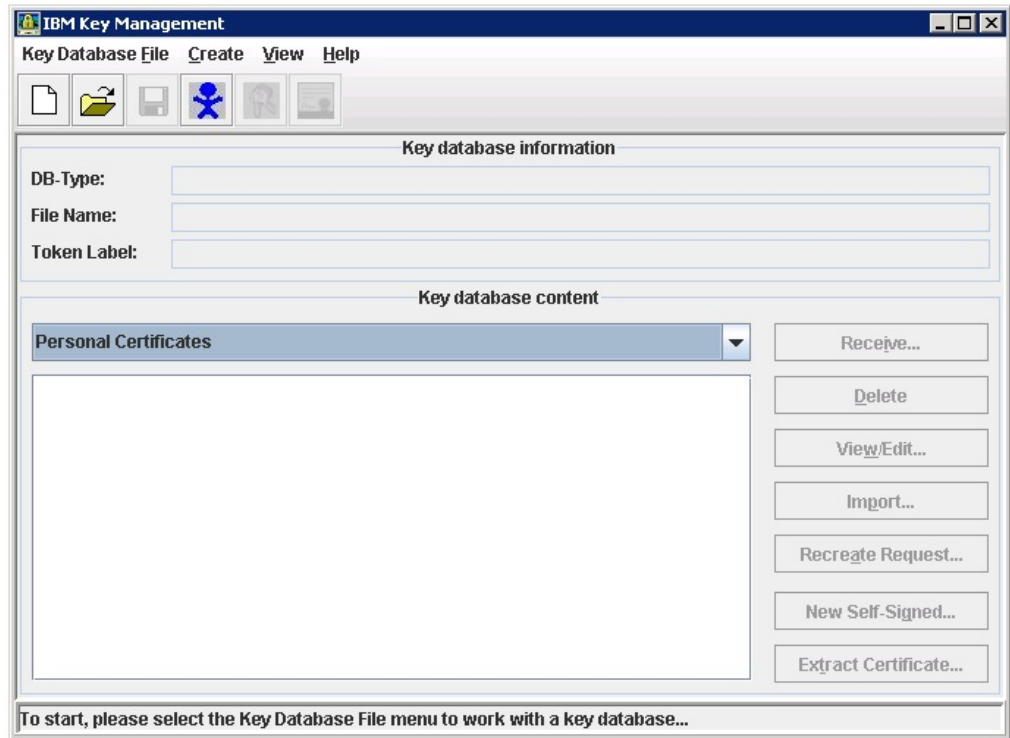
## Importing an SSL certificate into Edge Components Caching Proxy server

When using a self-signed certificate in IBM HTTP server in an IBM Connections environment, you must import this certificate into the key database of Edge Components Caching Proxy server to be a trusted certificate.

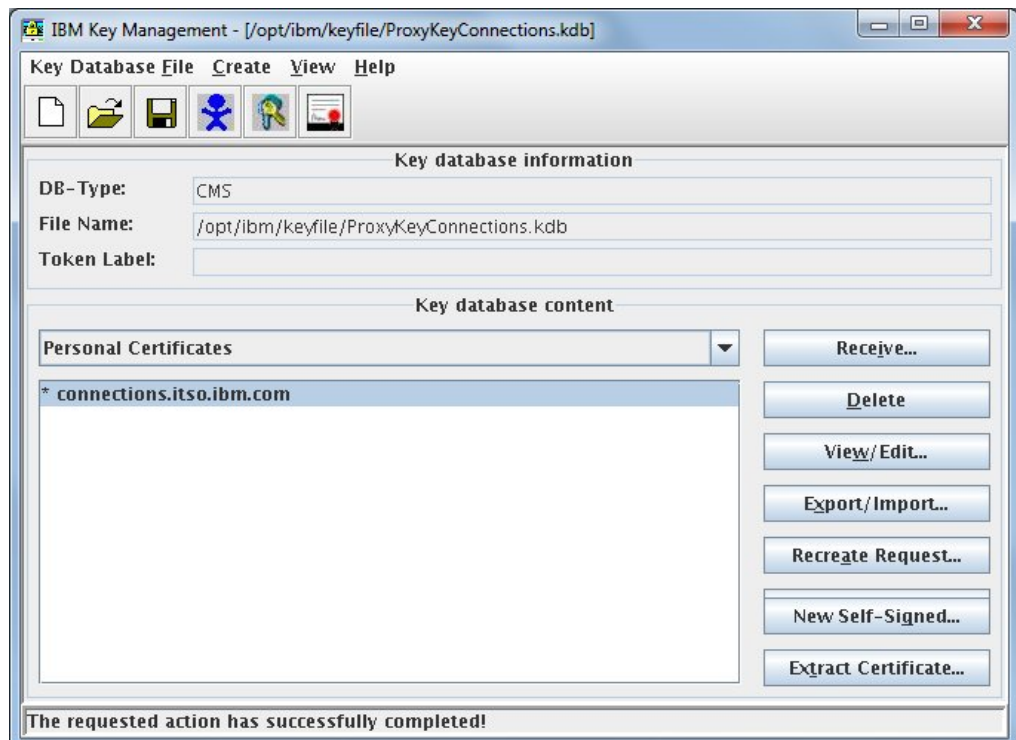
Complete these steps to import the self-signed certificate from IBM HTTP server into the Edge Component Caching Proxy server:

1. On the IBM HTTP Server installation directory, run **ikeyman** to open the key management utility:
  - Linux: # **./ikeyman**
  - Microsoft Windows: > **.\ikeyman**

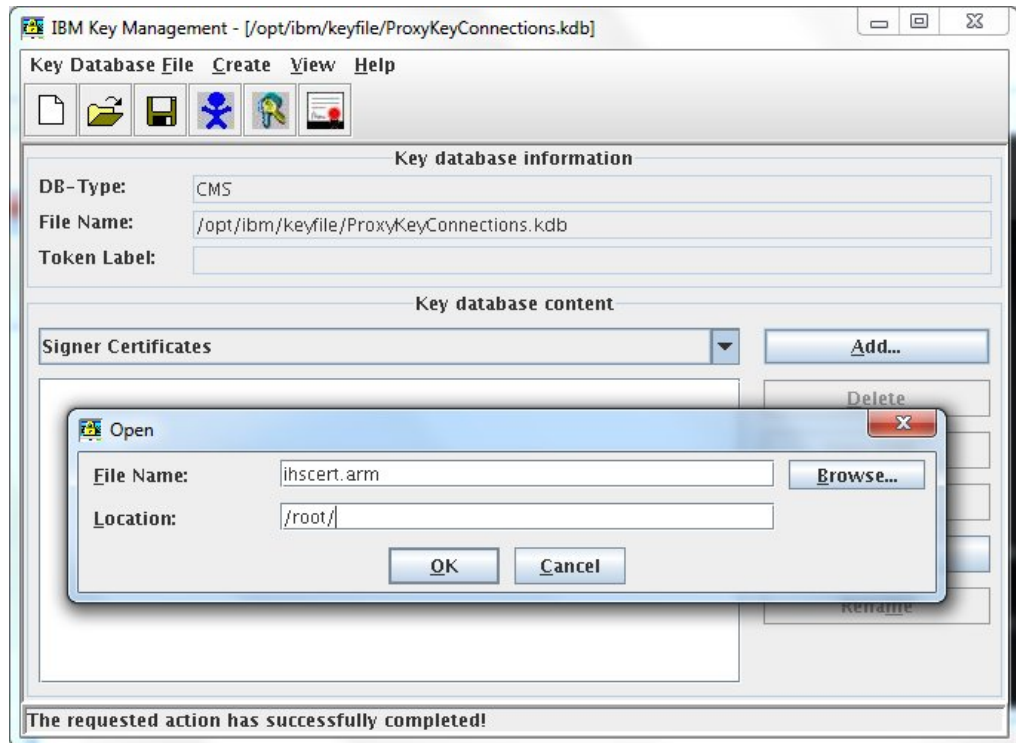




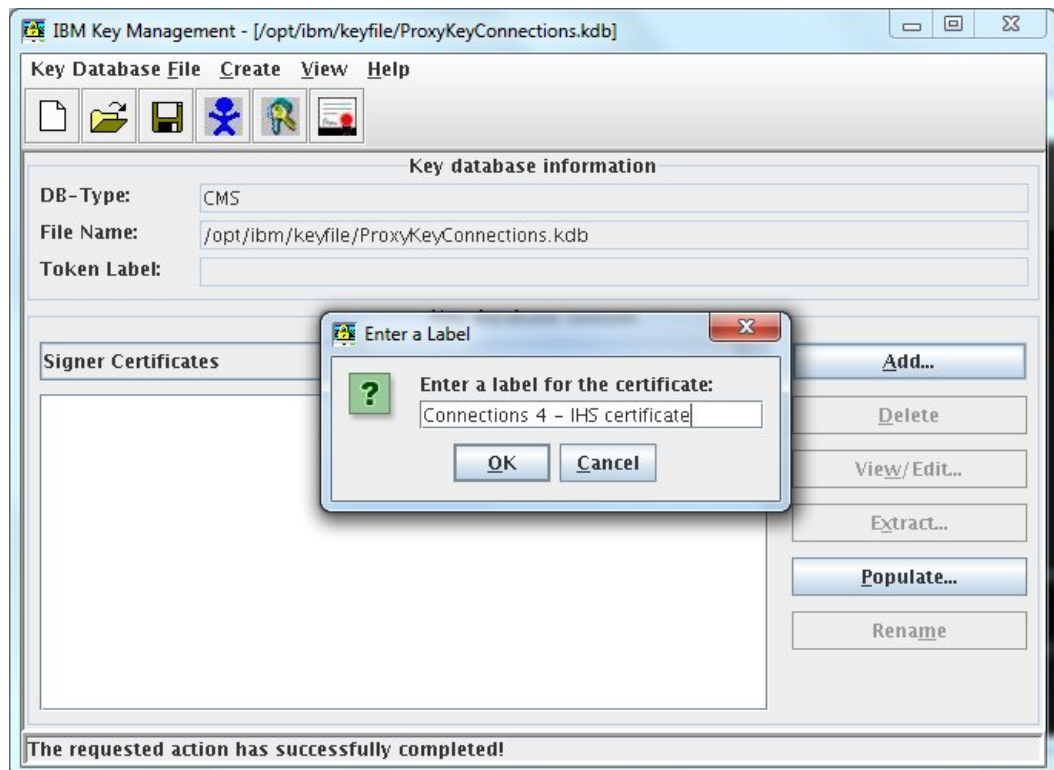
2. From the menu bar, select **Key Database File** → **Open** and complete these fields:
  - *Key database type*: Select **CMS**
  - *File Name*: **ProxyKeyConnections.kdb**
  - *Location*: The file location, for example, **/opt/ibm/keyfil**



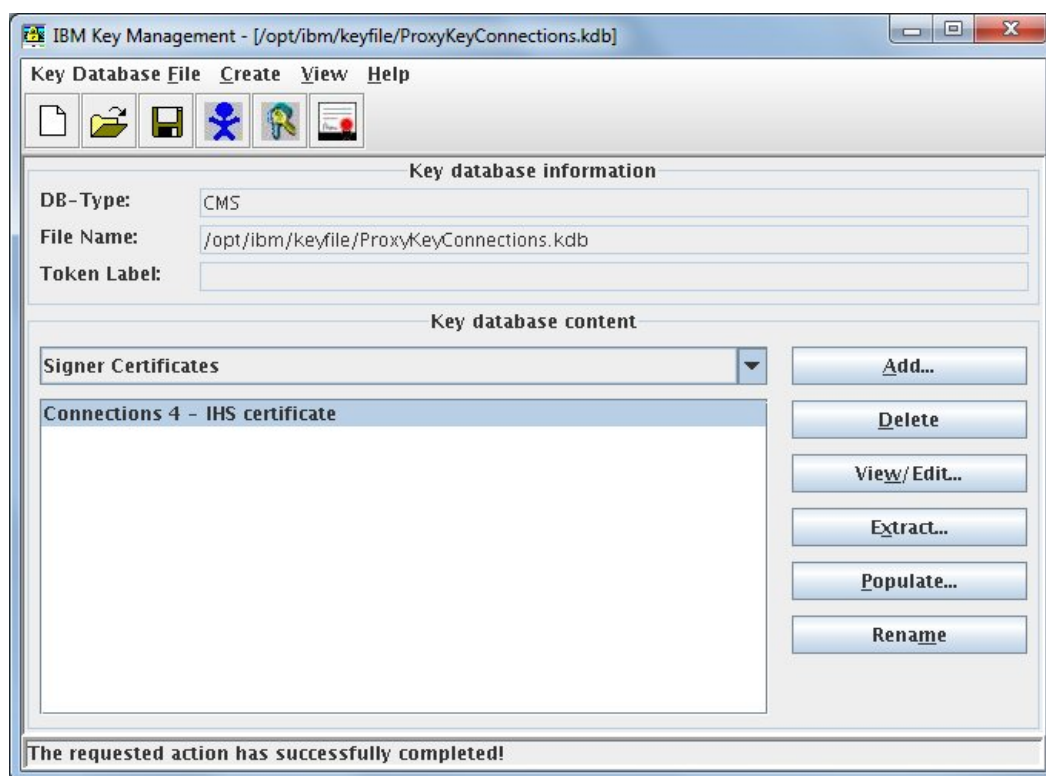
3. Select **Signer Certificates**, click **Add...**, and enter the following data:
  - *File name:* **ihscert.arm**
  - *Location:* **/root/**



4. Provide a label for the certificate and click **OK**.



5. You have finished the import the IBM HTTP SSL certificate.



## Configuring the SSL certificate on the Edge Components Caching Proxy server

Once the IBM HTTP SSL certificate has been imported into the Edge Server the `ibmproxy.conf` file must be modified for it to see these changes. Follow this procedure:

1. Stop the Edge Caching Proxy server using the following command:
  - Linux:
    - `#!/etc/init.d/ibmproxy stop`
  - Microsoft Windows:
    - a. Go to **Start** → **Administrative Tools** → **Services**.
    - b. In the Services window, highlight **Caching Proxy**. Click **Stop**.
2. Go to the Edge Components configuration directory:
  - Linux: `# cd /opt/ibm/edge/cp/etc/en_US`
  - Microsoft Windows: `> cd C:\Program Files\IBM\edge\cp\etc\`
3. Edit the **ibmproxy.conf** configuration file for the Edge Caching Proxy server and add the following variables:
 

In the SSL Directives section, add or enable the following rules:

**SSLEnable On**

**SSLCaching On**

In the Proxy Directives section, add or enable the following rules:

**SSLTunneling on**

In the Keyring Directive section, add or enable the following rules:

**KeyRing /opt/ibm/keyfile/ProxyKeyConnections.kdb**

**KeyRingStash /opt/ibm/keyfile/ProxyKeyConnections.sth**

Save and close the file.

4. Start the Edge Caching Proxy server using the following command:

– Linux:

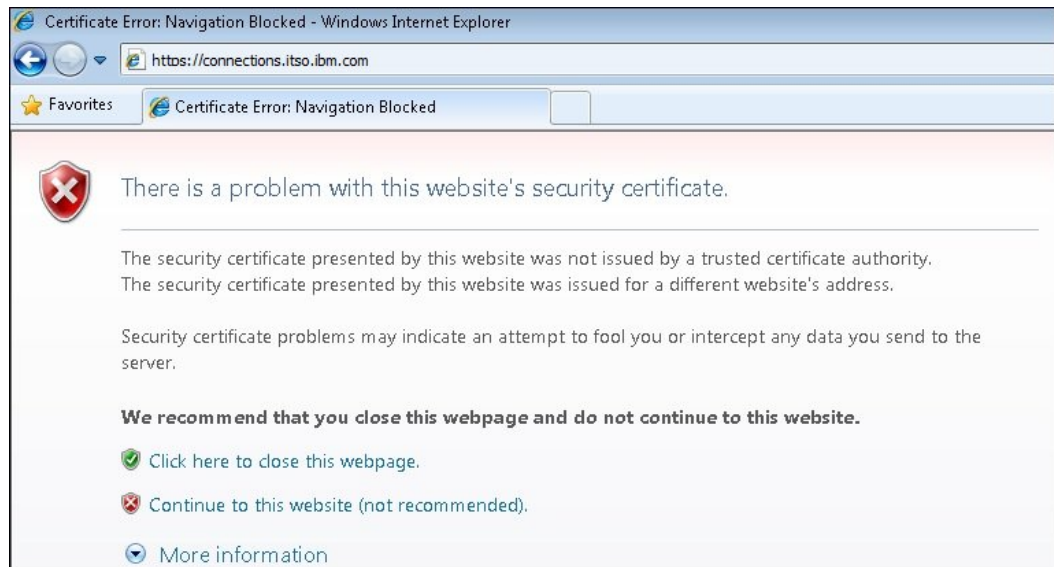
**# /etc/init.d/ibmproxy start**

– Microsoft Windows:

i. Go to **Start → Administrative Tools → Services**.

ii. In the Services window, highlight **Caching Proxy** and click **Start** to initiate the Caching Proxy service.

5. Access the web server using https from a web browser, in our example, <https://connections.itso.ibm.com/> When using a self-signed certificate, a warning is displayed informing you that the certificate is not trusted by a Certificate Authority (CA), click **Continue** to go to your web site.



This concludes the SSL configuration on IBM Edge Component Caching Proxy server. The network connection security between your browser and the web server is enabled.

### 7.3.4 Configuring disk cache on Edge Components Caching Proxy server

Though memory caching provides a faster response time, it is limited by the amount of memory available in the Edge Caching Proxy server. Compared to memory caching, the disk cache allows storing a larger amount of cacheable objects with the trade-off of a less effective response time.

For the disk cache to be efficient, a dedicated partition for disk cache should be allocated. This disk partition stores on other object but the caching objects. In this section, we describe how to create this partition and configure the Edge Components to make use of it:

## Creating a new RAW device

1. On the Edge Caching Proxy server, create a disk partition using the utility or command of the operating system:
  - Linux: **fdisk**
    - i. Check if raw module is loaded in the Kernel using the following command:  
**# modprobe raw**
    - ii. Bind a raw device to a block device using the following command:  
**# raw /dev/raw/raw1 /dev/sdb1**
  - Microsoft Windows: **Disk management tool**
2. Format the partition using the following command:
  - Linux: **# htcformat /dev/raw/raw1 -blocksize 8192**
  - Microsoft Windows: **> htcformat \\.\d:**

## Configuring Edge Caching Proxy server to use disk cache

Complete these steps to configure the Edge Caching Proxy server to use the disk cache:

1. Stop the Edge server:
  - Linux:  
**# /etc/init.d/ibmproxy stop**
  - Microsoft Windows:
    - i. Go to **Start → Administrative Tools → Services**.
    - ii. In the Services window, highlight Caching Proxy, and click **Stop**.
2. Go to Edge components configuration directory:
  - Linux: **# cd /opt/ibm/edge/cp/etc/en\_US**
  - Microsoft Windows: **> cd C:\Program Files\IBM\edge\cp\etc\**
3. Edit the ibmproxy.conf configuration file for the Edge components with a text editor and add the following variables:
  - Linux:  
**CacheDev /dev/raw/raw1**  
**BlockSize 8192**
  - Microsoft Windows:  
**CacheDev \\.\d:**  
**BlockSize 8192**  
Save and close the file.
4. Start the Edge Caching Proxy server:
  - Linux:  
**# /etc/init.d/ibmproxy start**
  - Microsoft Windows:
    - a. Go to **Start → Administrative Tools → Services**.
    - b. In the Services window, highlight **Caching Proxy**, and click **Start**.

## 7.4 Role of load balancers

The function of a load balancer is to distribute the incoming client request among two or more servers to improve the throughput and processing time. A load balancer can be implemented with hardware, software, or a combination of the two. Hypertext Transfer Protocol (HTTP) is commonly used in a company's Internet and Intranets services. A single HTTP server can easily become the network bottleneck and degrade the performance. Load balancing is frequently used as the solution for this issue.

In this section, we show how to configure the Load Balancer of IBM® WebSphere Edge Components, Version 7.0 shipped with WebSphere Application Server Network Deployment of IBM Connections 4. We cover the following topics:

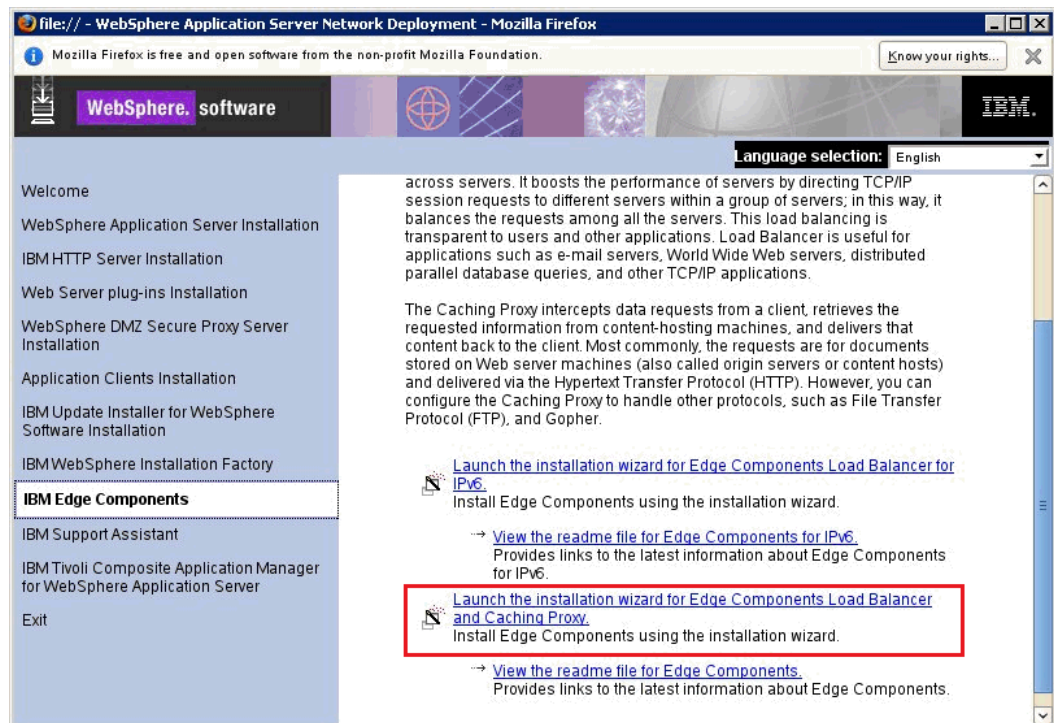
- ▶ 7.4.1, “Installing Load Balancer” on page 189: Procedure to install Edge components, Load Balancer using a graphical Installation wizard
- ▶ 7.4.2, “Configuring Load Balancer” on page 193: Procedure to configure the Edge components, Load Balancer

### 7.4.1 Installing Load Balancer

In this Section, we explain how to install Load Balancer using the graphical Installation wizard.

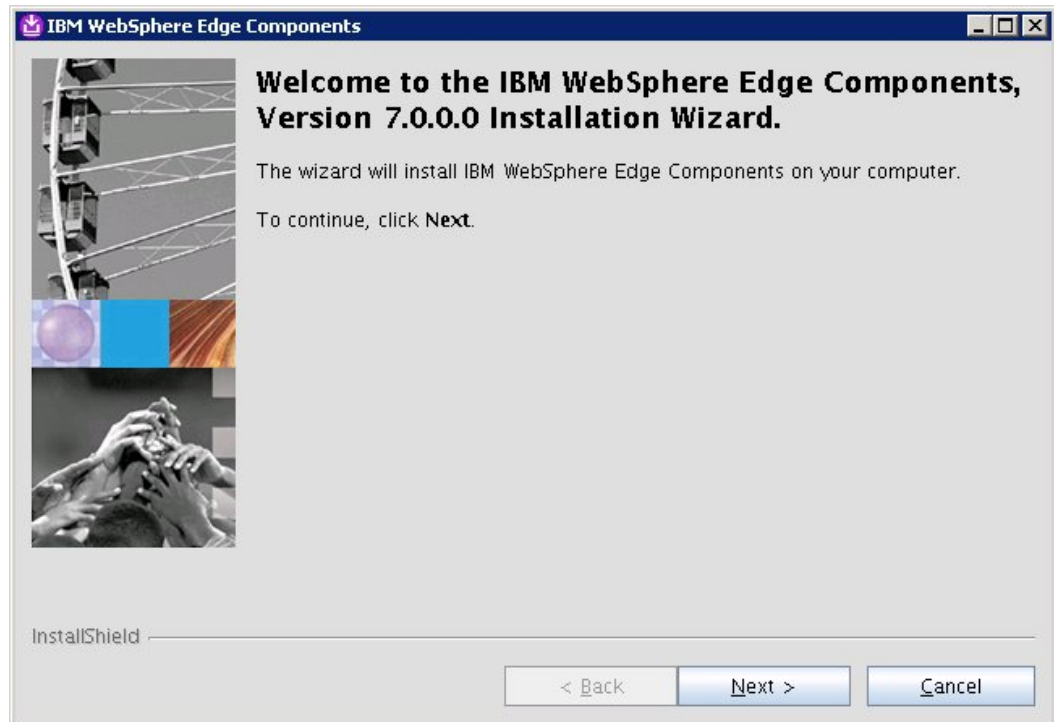
Follow these steps to install IBM Edge Components Load Balancer on a Linux system:

1. Unzip the WebSphere Edge Components into a temporary directory, for example, /tmp or c:\temp.
2. Run `1aunchpad.sh` (`1aunchpad.bat` for Windows) to launch the installation wizard.
3. On the Welcome WebSphere Edge Components window, select **Launch the Installation wizard for Edge Components Load Balancer and Caching Proxy**.



4. In the Welcome window, click **Next**.

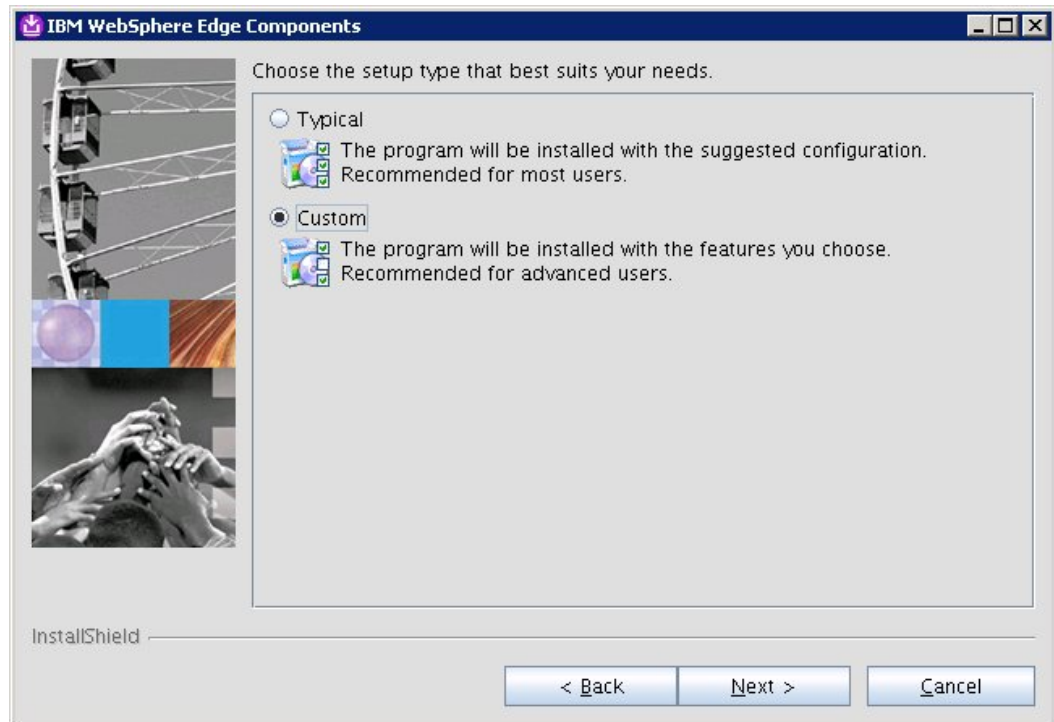




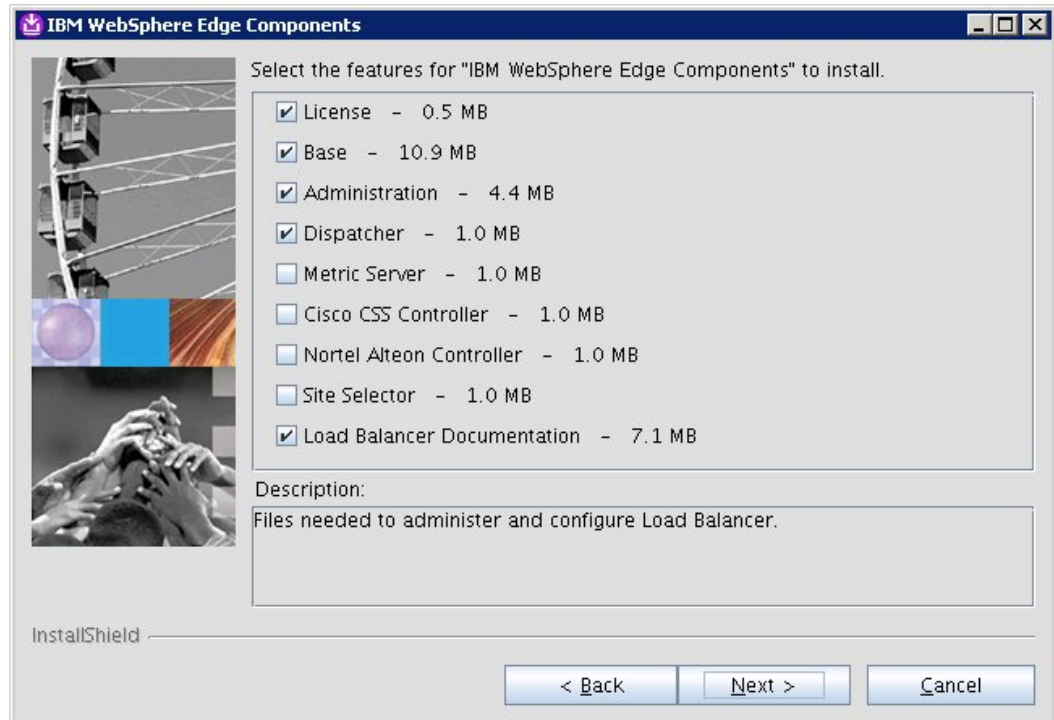
5. Accept the license agreement.
6. English is the default installation Language. You can select other language.



7. For installation type, select **Custom** to specify the components to install.



8. Select **License, Base, Administration, Dispatcher and Load Balancer Documentation** to install.



9. Validate if all features selected are correct, and click **Next** to continue the installation.





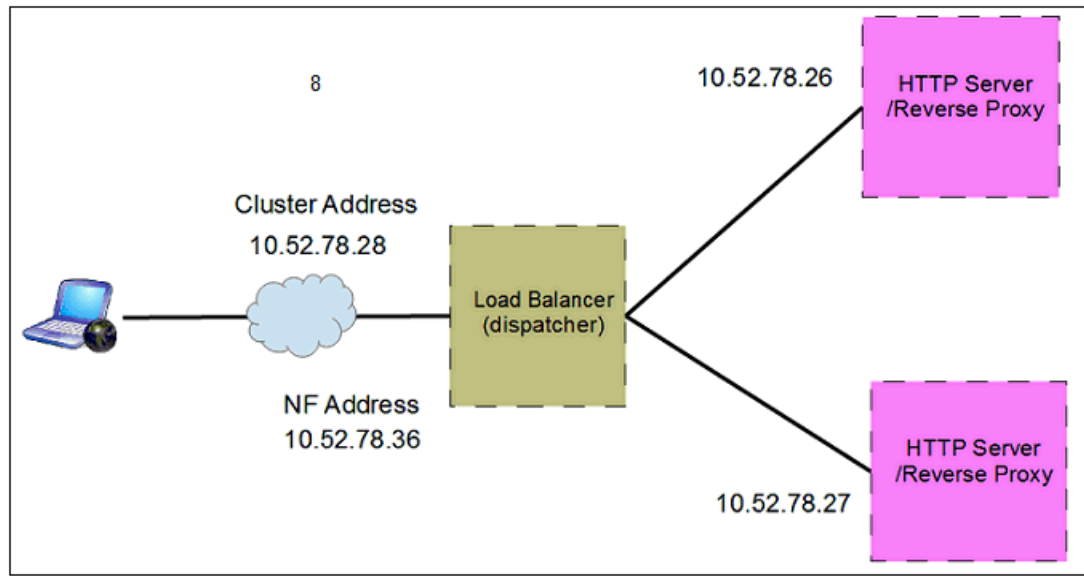
10. The installation wizard shows that **Edge Components** were installed successfully on your server. Click **Finish**.



## 7.4.2 Configuring Load Balancer

This section explains the best way to configure the IBM Edge components Load Balancer (IPv4 & IPv6) to balance the client requests of IBM Connections 4. We explain the configuration steps on a Linux operating system, though Microsoft Windows, AIX, HP-UP, and Solaris systems are supported as well.

The following figure shows the network topology of our lab environment.



In this topology, we include one WebSphere Edge Load Balancer 6.1 component for balancing the incoming HTTP connections for two HTTP servers. We use the same topology for Edge Caching Proxy servers.

In lab scenario, we have installed WebSphere Edge Load Balancer and assigned two static IP addresses are assigned to it. For the Load Balancer system, note the following:

- ▶ The server selected for the Load Balancer installation must reside on the same LAN segment as the nodes to be clustered.
- ▶ Ensure that `/opt/ibm/edge/ulb/bin` is added to the PATH.

### Configuring the WebSphere Edge Load Balancer

Use the following steps to configure the WebSphere Edge Load Balancer:

1. Start the server function by running the following command on a command prompt:

```
dsserver
```

2. Stop the executor function using the following command:

```
dscontrol executor stop
```

3. Change Log level to 1 using the following command:

```
dscontrol set loglevel 1
```

4. Start the executor function using the following command:

```
dscontrol executor start
```

5. Set nfa IP address:

```
dscontrol executor set nfa 10.52.78.36
```

6. Define a cluster and set cluster options:

```
dscontrol cluster add 10.52.78.28
dscontrol cluster set 10.52.78.28 proportions 49 50 1 0
dscontrol executor configure 10.52.78.28M
```

The dispatcher balances the requests from clients to the servers configured behind dispatcher. The cluster is either the symbolic name, the dotted decimal address, or the special address 0.0.0.0 that defines a wildcard cluster. Wildcard clusters can be used to match multiple IP addresses for incoming packets to be load balanced.

7. Define ports and set port options with the adding dscontrol port command, dscontrol port add cluster@port. For example:

```
dscontrol port add 10.52.78.28@80
```

8. Define the load-balanced server machines. To define a load-balanced server machine, run the following command:

```
dscontrol server add 10.52.78.28@80@10.52.78.26
dscontrol server set 10.52.78.28@80@10.52.78.26 weight 14
dscontrol server add 10.52.78.28@80@10.52.78.27
dscontrol server set 10.52.78.28@80@10.52.78.27 weight 14
```

9. Repeat the steps 6 and 7 to setup dispatcher in port 443 used by https protocol.

```
dscontrol port add 10.52.78.28@443
dscontrol server add 10.52.78.28@443@10.52.78.26
dscontrol server set 10.52.78.28@443@10.52.78.26 weight 14
dscontrol server add 10.52.78.28@443@10.52.78.27
dscontrol server set 10.52.78.28@443@10.52.78.27 weight 14
```

10. Start the manager function to improves load balancing. To start the manager, run the following command:

```
dscontrol manager start manager.log 10004
```

11. Start the advisor function. The advisors give the manager more information about the ability of the load-balanced server machines to respond to requests.

```
dscontrol advisor start http 80 http_80.log
dscontrol advisor start https 443 http_443.log
```

## Configuring the HTTP Servers servers

The HTTP Servers servers need configuration changes for the Load balancing to work. The Dispatcher only balances requests across servers that allow the loopback adapter to be configured with an additional IP address, for which the back-end server will never respond to ARP (address resolution protocol) requests.

In Linux to configure a loopback interface you must run the following command:

```
ip -4 addr add 10.52.78.28/32 dev lo
```

Remember to run this command in both HTTP servers.

**Note:** For information about configuring loopback on a Microsoft Windows environment, see Edge Components Info Center  
[http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.edge.doc/lb/welcome\\_edge.html](http://pic.dhe.ibm.com/infocenter/wasinfo/v7r0/topic/com.ibm.websphere.edge.doc/lb/welcome_edge.html).

## **Conclusion**

Your Load Balancer is now configured and ready to use. For information on managing your Load Balancer, a full list of advisors, metric server functions for Dispatcher, and other advanced features, refer to the product documentation that comes with the Load Balancer.



## Working with IBM Connections mobile

IBM Connections is supported on a broad range of mobile devices including Android, iOS, RIM BlackBerry and older Windows Mobile phones. IBM makes the client application for IBM Connections available for these devices through their respective App stores.

The mobile clients provide a richer experience for using IBM Connections on a mobile device than would be the case using simply a web-browser presentation. For example, using the client application, it becomes possible to integrate opening of files from other applications on the device into IBM Connections or uploading a photo from the photo gallery of the device into IBM Connections.

For Apple iOS the current IBM Connections client works on all generations of iPad, iPhone and iPod Touch, provided they are running iOS 5 or higher.

For Android , the base version of the operating system required is version 2.2.

For Blackberry, the base operating system is version 6.0.0 or higher.

Different from version 3 of IBM Connections, version 4 comes ready to support these mobile clients. At the time of writing there is a cumulative fixpack release available from IBM (<http://www-01.ibm.com/support/docview.wss?uid=swg21612692>) which fixes a broad range of issues including mobile access.

Broadly there are two methods for making mobile clients able to access a live IBM Connections environment:

- ▶ Opening a port on the external firewall which directs traffic to the HTTP server of the IBM Connections environment. Authentication is then done directly with the Connections environment as if you were using a regular web browser.
- ▶ Establishing a VPN connection on the device to inside your organization's LAN and then using IBM Connections as if you were on your corporate network.

The best method for your organization must be decided on by you.

## 8.1 Setting up an IBM Connections mobile client

Before starting setting up your mobile client, ensure that there is a valid means of connection for the mobile clients to reach your Connections' HTTP server. For clients that will connect through a VPN connection, generally this means that they will access the IBM Connections environment as if they were on your corporate LAN. For clients connecting from outside the network, you must set up some access through your firewall for clients. In either condition test accessing the server using a regular web browser before attempting to connect.

Complete the following steps to install and configure an IBM Connections mobile client:

1. Obtain the appropriate client software for your mobile devices:
  - For Apple iOS, the current Connections client works on all generations of iPad, iPhone and iPod Touch, provided they are running iOS 5 or higher. See <https://itunes.apple.com/gb/app/ibm-connections/id450533489?mt=8>
  - For Android, the base version of the operating system required is version 2.2. See <https://play.google.com/store/apps/details?id=com.ibm.lotus.connections.mobile&hl=en>
  - For Blackberry, the base operating system is version 6.0.0 or higher. See <http://appworld.blackberry.com/webstore/content/52232/>
2. Install the client according to the instructions provided which are appropriate for the device. Remember that mass distribution of the client to a large number of devices may be possible using the device vendor's management software or a compatible mobile device management solution. Configuring such solutions for the Connections mobile client is outside of the scope of this document.
3. After the client is installed on the device, follow these instructions:
  - a. iOS:
    - i. Tap the IBM Connections application icon from the home screen of the iOS device.
    - ii. Select a login option, usually "My Company's Server".
    - iii. Enter the URL or IP address which is accessible from your device to the IBM Connections server. This might be the internal URL if you connect first with a VPN client or the external DNS name of the IBM Connections server if you do not.
    - iv. Enter your user name and password.
    - v. Tap **Login**.
  - b. For Android devices:
    - i. Tap the IBM Connections application icon from the home screen of the Android device.
    - ii. Select a login option, usually "My Company's Server".
    - iii. Enter the URL or IP address which is accessible from your device to the Connections server. This might be the internal URL if you connect first with a VPN client or the external DNS name of the Connections server if you do not.
    - iv. Enter your user name and password.
    - v. Tap **Login**.
  - c. For BlackBerry devices
  - d. Tap on the Connections application icon from the home screen of the BlackBerry device.
  - e. Select a login option, usually "My Company's Server".

- f. Enter the URL or IP address which is accessible from your device to the IBM Connections server. This might be the internal URL if you connect first with a VPN client or the external DNS name of the Connections server if you do not.
- g. Enter your user name and password.
- h. Tap **Login**.

## 8.2 Troubleshooting

The most common problem with the mobile client is that it is unable to connect to the server. The lack of good diagnostic tools on mobile devices makes troubleshooting this issue quite difficult. Test, therefore, with a regular browser that you can reach the mobile site for your IBM Connections server, for example, <https://greenhouse.lotus.com/mobile>. Compare this with the server name you have provided in the URL field. Note that it is not necessary to specify the /mobile in the URL on the mobile device.

Sometimes in a poorly configured IBM Connections environment it is necessary to log in to the mobile service using your email address and not your "common name". For example, I might log in to IBM Connections on my computer as "Frank Adams" but it might be necessary to log in on the mobile device as "frank.adams@renovations.com". This indicates a poor configuration of the Federated LDAP repositories on the IBM Connections application server.





# IBM Connections metrics

IBM Connections 4.0 suite provides optional IBM Cognos Business Intelligence component to generate reports against IBM Connections application. If the customer has license only for IBM Connections suite, they can use Cognos only for generating reports through Metrics application and they should not either customize or perform any other activities on Cognos Business Intelligence server.

## 9.1 Security for IBM Connections Metrics application

IBM Connections Metrics application generates report for all the IBM Connections applications using IBM Cognos Business Intelligence software. This report helps to analyze how IBM Connections applications are accessed by the end users. By enabling security for this Metrics application, only authorized users can view the report. IBM Connections Metrics application provides the following roles by default.

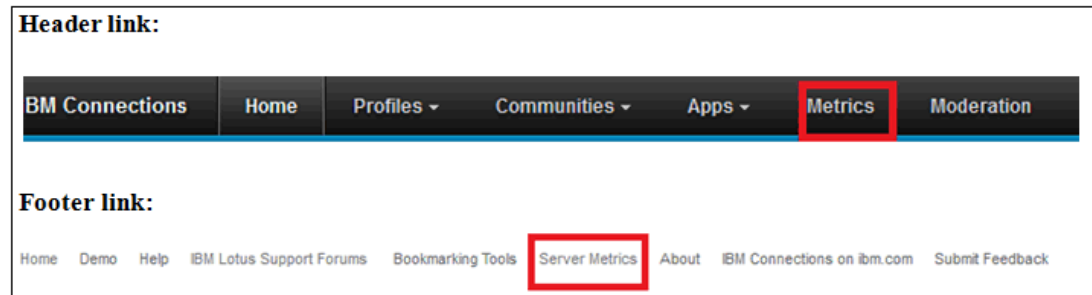
- ▶ admin
- ▶ metrics-report-run
- ▶ community-metrics-run
- ▶ reader

### 9.1.1 Admin role

*Admin* role is the super-user role presents in all IBM Connections applications. By default, it is not mapped to any users. It is recommended to map only IBM Connections administrators for this role.

If a user is mapped to admin role only in Metrics applications, then only that user can access Metrics application using URL such as <https://connections.itso.ibm.com/metrics> but not through header and footer link. If a user is mapped to admin role only in Common application, then the user is able to see the header and footer link, but do not have access to the application. If a user is mapped to admin role for Metrics and Common application, then the user is able to access the Metrics application through URL such as

<https://connections.itso.ibm.com/metrics> and able to see the header and footer link. A similar window is shown to the user.



The user mapped to admin role can access the Metrics link for all communities even though user is not a member for a specific community.

### 9.1.2 Metrics-report-run role

This role authorizes who can have access for Metrics applications to generate reports. This role presents only in Metrics and Common applications. If a user is mapped to only in Metrics application, then user can access Metrics application only through URL such as <https://connections.itso.ibm.com/metrics>. If a user is mapped to the Metrics-report-run role in Common application only, the user can see the link for Metrics application in Header and footer, but cannot perform any activity. If a user is mapped to the Metrics-report-run role in both Metrics and Common applications, then the user is able to access the Metrics application through URL such as <https://connections.itso.ibm.com/metrics> and the header and footer link.

### 9.1.3 Community-metrics-run role

This role presents only in Metrics and Community applications and by default it is mapped to “All Authenticated in Application Realm”. This means that the Community owner can see the link for Metrics reports. If there is any particular user mapped to this role, then, only that user can see the Metrics link to access static reports, no one else can see the Metrics link.

### 9.1.4 Reader-role

The reader-role is present for the following applications:

- ▶ Activities
- ▶ Blogs
- ▶ Bookmarks
- ▶ Wikis
- ▶ Files
- ▶ Forums
- ▶ Profiles

By default, this role is mapped to everyone. If a user is mapped to any specific application, user can access reports for that application only using the global Metrics URL such as <https://connections.itso.ibm.com/metrics>.

## 9.2 Using IBM Connection Metrics

IBM Connections Metrics application provides report for IBM Connections server and it is classified into three categories:

- ▶ People
- ▶ Content
- ▶ Participation

User can view a report for an application based on one of these categories.

### 9.2.1 People

In this category, IBM Connections Metrics application provides report about how many people logged into the IBM Connections server. This report can be generated based on the time frame and group by options. The following figure is an example of the report that shows how many people logged into the IBM Connections server.



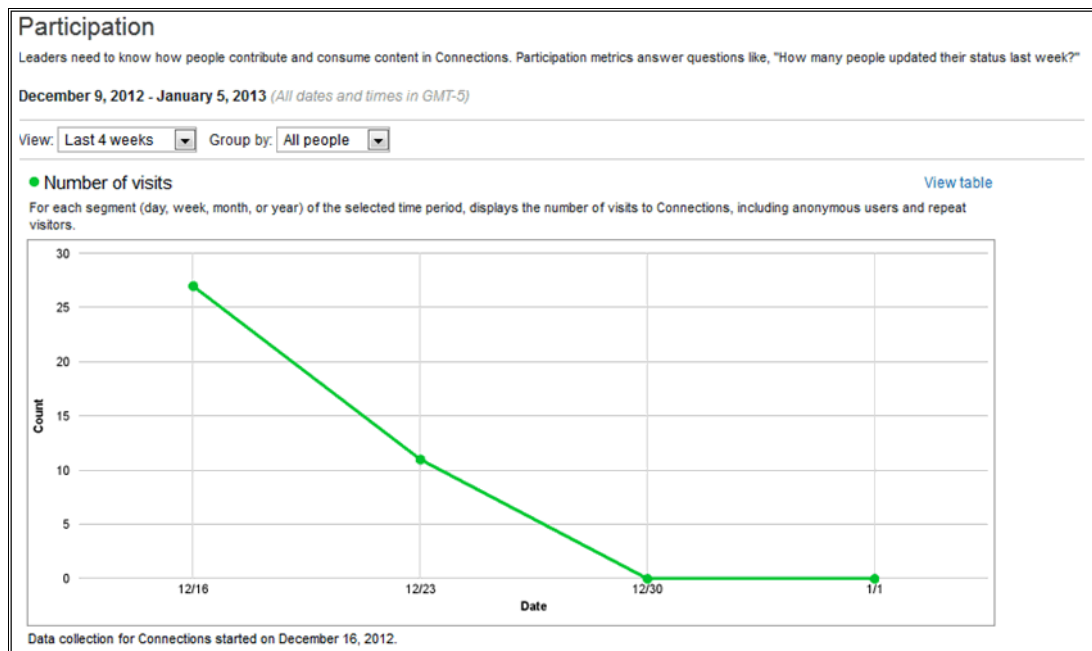
### 9.2.2 Content

In this category, Metrics report gives details for most active content in IBM Connections server so that leaders can take decision to update or modify the content to utilize the IBM Connections server effectively. The following report example shows the most active content in communities and forums.



## 9.2.3 Participation

In this category, metrics report gives details for how many people contributed to the IBM Connections server. The following report example shows the number of users contributed to the IBM Connections Server.



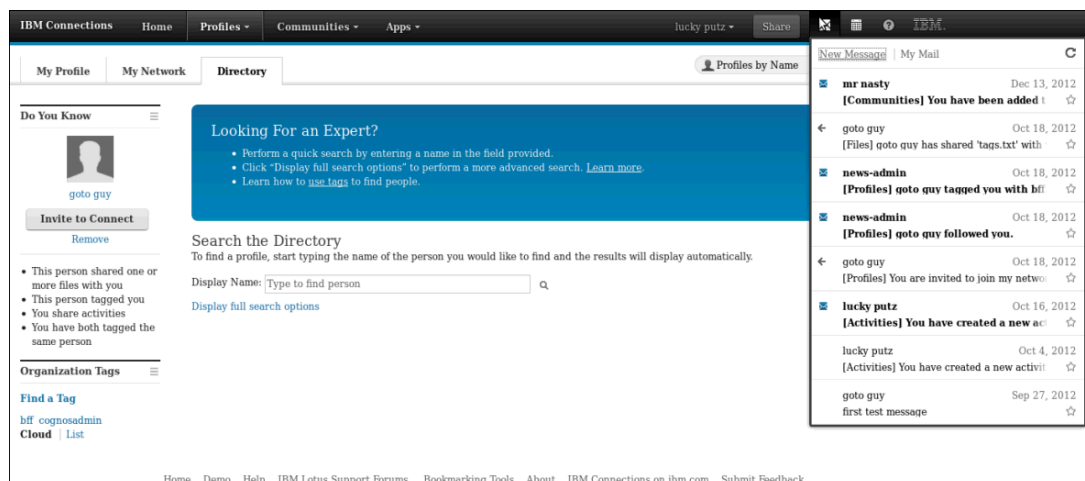
# IBM Connections mail

Starting in version 4 of IBM Connections, a feature is available that allows you to access your IBM Notes or Microsoft Outlook email and calendar from within the IBM Connections product. This feature provides the User with icons for email and calendar that they can simply hover a cursor over to perform essential tasks.

There no longer is a need to have multiple web browsers (or tabs) open when a user is working with IBM Connections their email or calendar. The ability to read messages and compose new ones along with checking calendar entries is now available within the same user interface.

## 10.1 Features of IBM Connections mail

IBM Connections Mail consists of email and calendar functions that can be accessed within the IBM Connections product. These integrated functions allows users to accept network Invitations right from their Inbox or comment on a notification sent by an IBM Connections Application.



## 10.1.1 Email

The following table lists the functions available with the Email feature:

| What do you want to do?  | How you do it   |
|--|---|
| Check for new messages   | Hover-over the email icon and click <b>Refresh</b> .  |
| Read a message   | Hover-over the email icon and click <b>Message</b> .  |
| Move a message to a folder in your email   | Read the message then click <b>Move To Folder</b> and select the folder.                        |
| Save an attachment to either your workstation or the IBM Connections Files Application | Read the message, then click either <b>Download</b> or <b>Share</b> beside the attachment icon. |
| List more messages from your Inbox   | Go to the bottom of your Inbox and click <b>Load More Messages</b> .                            |
| Mark a message as important  | Hover-over the email icon and click the star icon.  |
| Reply to a message   | Hover-over the email icon then the Message and click <b>Reply/Reply-To-All</b> .                |
| Forward a message  | Hover-over the email icon and then the Message and click <b>Forward</b> .                       |
| Delete a message   | Hover-over the email icon and then the Message and click <b>Delete</b> .                        |

When composing a new message within IBM Connections Mail, type-ahead look up is available which checks your existing contacts (in IBM Connections and IBM Notes or Microsoft Outlook) for matches with the characters that you are typing. A Check Names button is also provided so that you can verify that the email addresses specified in the To/Cc/Bcc fields do match what you have in your Contacts. In addition, you can add attachments to the message that exist either on your Workstation or in the IBM Connections Files Application.

Here are other exciting features of IBM Connections Mail:

- ▶ Preview image files
- ▶ Open someone's profile page
- ▶ Re-share a file if you have access
- ▶ Follow or stop following a person or file
- ▶ Accept or reject a request to join your network
- ▶ See, like, and comment on files, status updates, and wall posts
- ▶ Sort, add, edit, or delete comments on a file or wall post that you own

**Note:** Some are available only with IBM Domino Servers.

## 10.1.2 Calendar

The Calendar function provided with the IBM Connections Mail feature is essentially read-only, where you can view your schedule from a previous day, the current day, or a specific date. A handy ability in the Calendar function are the identification of conflicting

entries within your Calendar. Conflicting entries within a Calendar displayed in IBM Connections have an orange-bar to clearly indicate a possible scheduling problem.

## 10.2 Configuring Mail for IBM Connections

Installing the IBM Connections Mail feature comprises of four major steps, whether using IBM Domino or Microsoft Exchange as your email server:

1. Install IBM Connections Mail.
2. Set up Access to IBM Connections Mail.
3. Set up Discovery Service for IBM Connections Mail.
4. Set up Help for IBM Connections Mail.

Before you begin, you must prepare your IBM Connections 4 environment to deploy IBM Connections Mail. Aside from ensuring that your environment is working properly, you must set a single sign-on (SSO) solution. If you use a Microsoft Exchange Server, you must configure your IBM Connections environment to use SPNEGO. The IBM Connections Mail feature supports SSO with IBM Domino Servers through SPNEGO or LTPA. The user email addresses must:

- ▶ Be valid email addresses.
- ▶ Be visible in IBM Connections.
- ▶ Their records of email addresses on the Mail Server must match what is stored in IBM Connections.

Refer to product documentation Preparing to install IBM Connections Mail

([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+Mail+1.0+documentation#action=openDocument&res\\_title=Preparing\\_to\\_install\\_IBM\\_Connections\\_Mail\\_icml&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+Mail+1.0+documentation#action=openDocument&res_title=Preparing_to_install_IBM_Connections_Mail_icml&content=pdcontent)) for more details about preparation that you must take before proceeding to deploy the IBM Connections Mail feature.

Fix Pack 1 (FP1) for IBM Connections Mail V1.0 is a prerequisite of Component Refresh #2 for IBM Connections 4.0 deployments that use the IBM Connections Mail V1.0 feature. Plan to install this FP1. More details on IBM Connections Mail V1.0 FP1 and its prerequisites, see IBM Greenhouse - IBM Connections Mail 1.0 FP1

<https://greenhouse.lotus.com/plugins/plugincatalog.nsf/assetDetails.xsp?action=editDocument&documentId=31651AAAE1F4913685257A5F00548896>.

### 10.2.1 Installing IBM Connections Mail

Complete the following steps to install IBM Connections Mail:

1. Review the software and hardware requirements for the systems that host IBM Connections Mail.

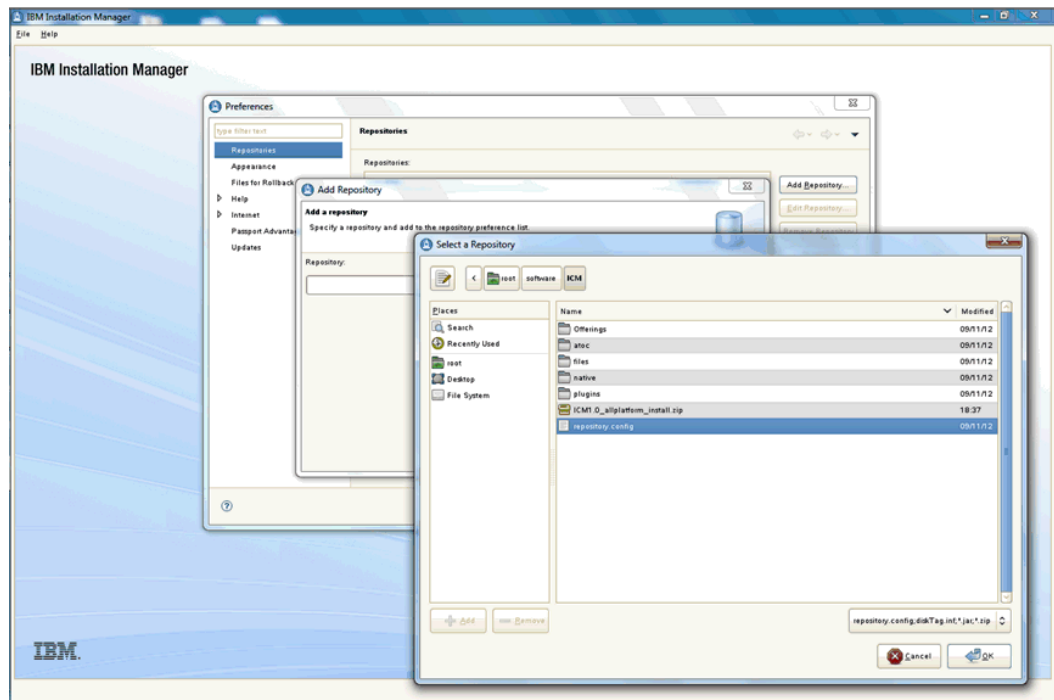
**Note:** For more information, see IBM Connections Mail system requirements: Detailed system requirements for IBM Connections Mail  
(<http://www.ibm.com/support/docview.wss?uid=swg27036069>)

2. Configure single sign-on between Connections and your mail servers. If you are using Microsoft Exchange servers or IBM Domino servers with self-signed certificates, import SSL certificates. Then verify that your settings are correct. For more information, see Preparing to install IBM Connections Mail:

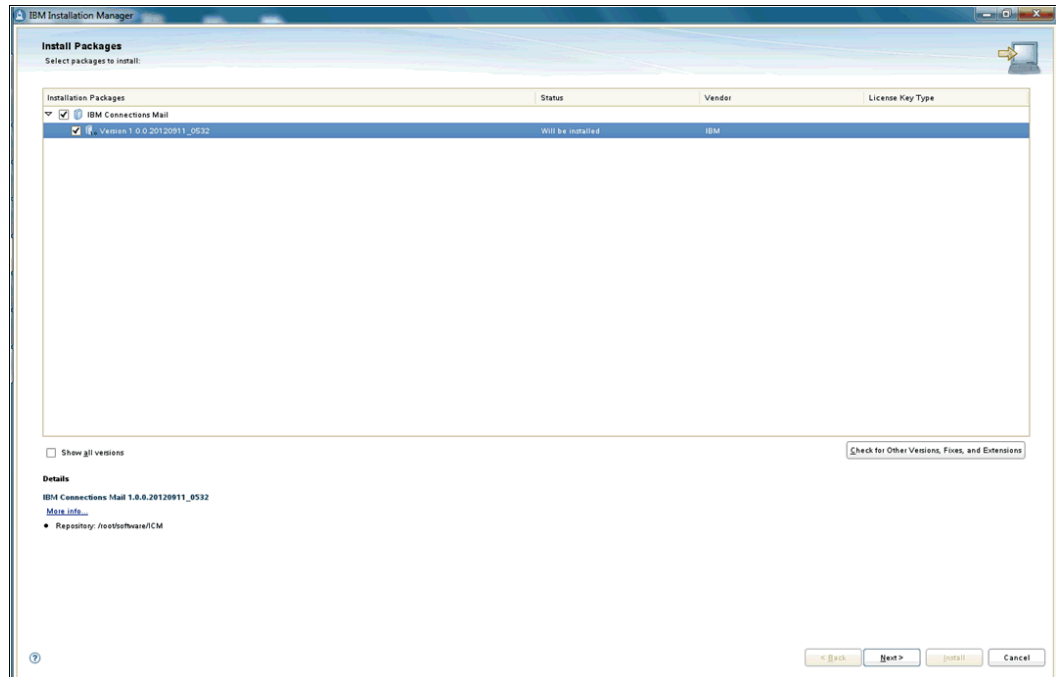


Product Documentation > IBM Connections Mail 1.0 documentation > Deploying IBM Connections Mail > Preparing to install IBM Connections Mail  
([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+Mail+1.0+documentation#action=openDocument&res\\_title=Preparing\\_to\\_install\\_IBM\\_Connections\\_Mail\\_icml&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+Mail+1.0+documentation#action=openDocument&res_title=Preparing_to_install_IBM_Connections_Mail_icml&content=pdcontent))

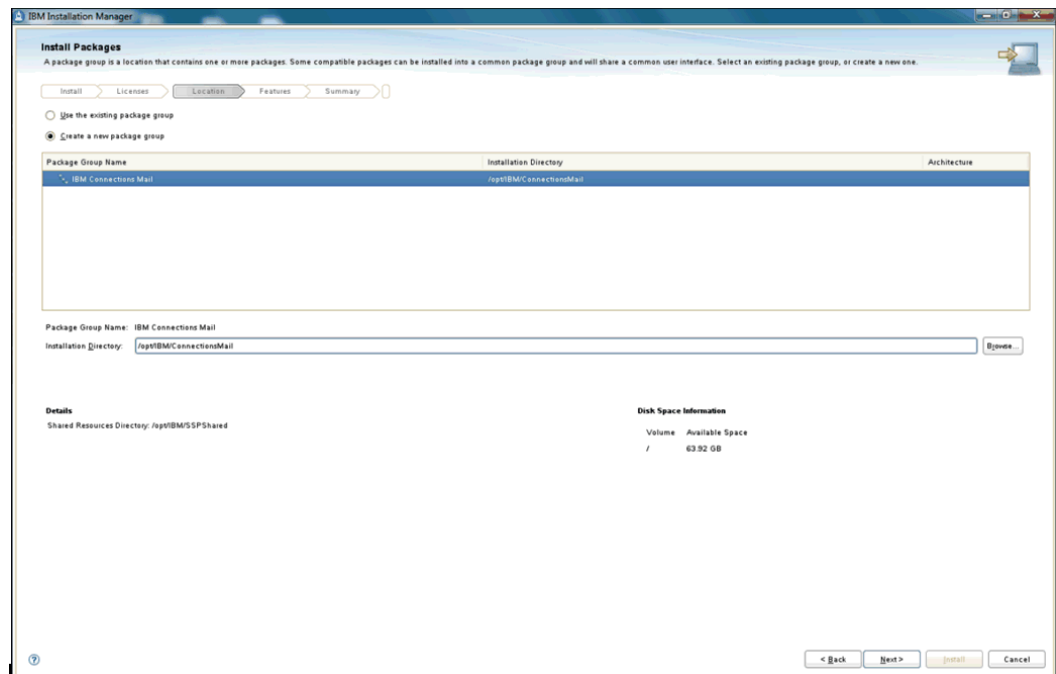
- Restart all Connections servers.
- Download and extract the IBM Connections Mail installation file.
- Open IBM Installation Manager from the server on which you are installing Connections Mail. This server must be running the WebSphere Application Server Deployment Manager.
- Select **File** → **Preferences**, and then select **Repositories**:



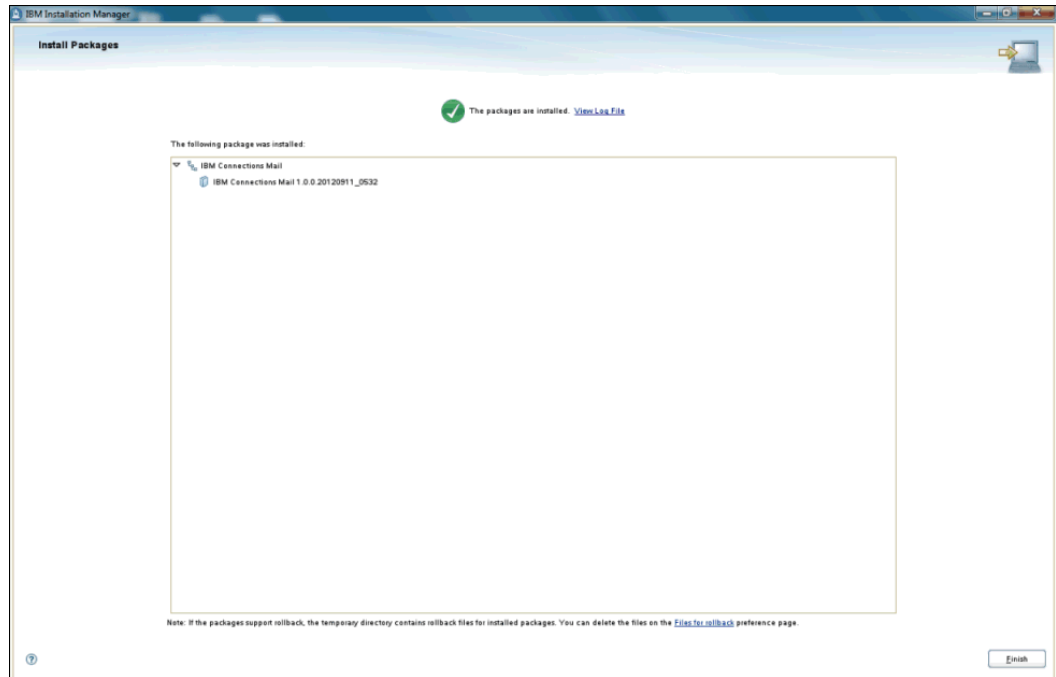
- From the Repositories panel, select **Add Repository**, navigate to the directory to which you saved the IBM Connections Mail files, and select the **repository.config** file.
- Click **OK** until you are returned to the Installation Manager main panel. Click **Install**.
- Select **IBM Connections Mail**, and click **Next**.



10. Read and accept the license agreement, and select **Next**.
11. Select **Create a new package group**. Accept the default value for the Installation Directory field or specify the path to another directory, and click **Next**. You must remember this file path for Enabling the discovery service for IBM Connections Mail.

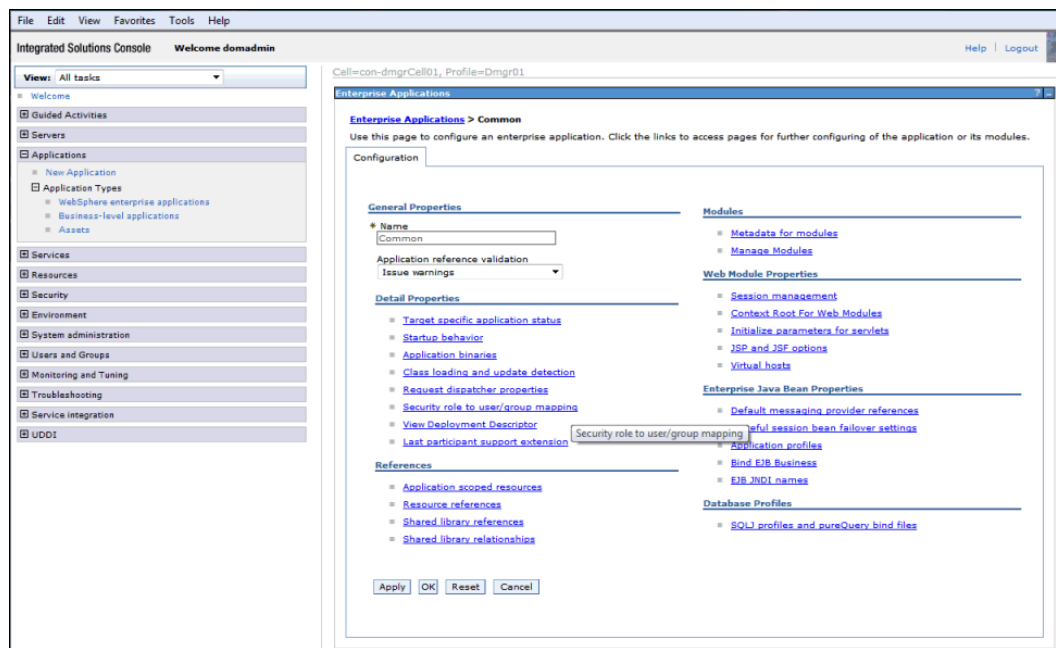


12. Click **Next**, click **Install**, and click **Finish**.



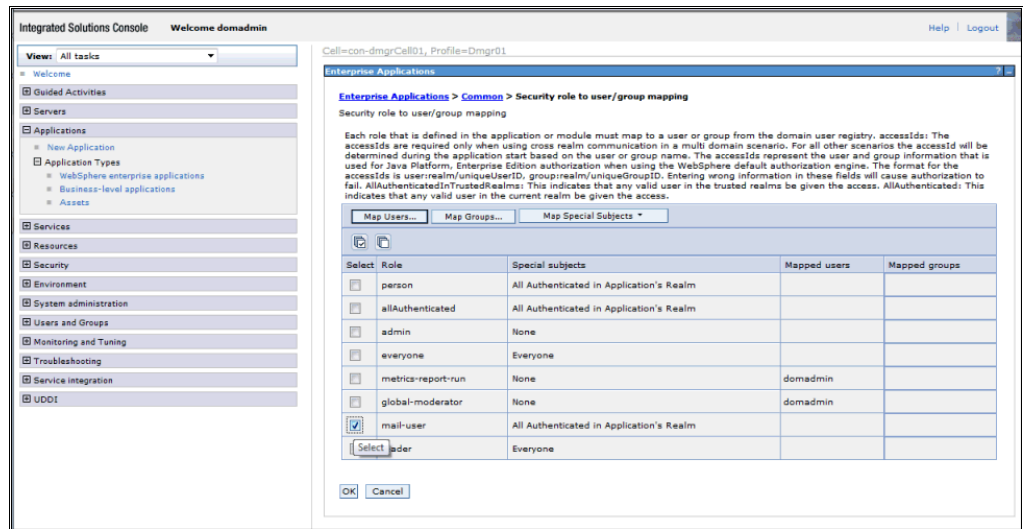
## 10.2.2 Configuring access to IBM Connections Mail

1. From the WebSphere® Application Server administrator console, click **Applications** → **Application Types** → **WebSphere enterprise applications** → **Common**.
2. Click the **Configuration** tab.
3. In the Detail properties section, select **Security role to user/group mapping**.



4. In the Security role to user/group mapping table, select the check box next to the mail-user role with Special subjects set to **None**.

5. From the Map special subjects field, select an option:
  - To enable for all users, select **All Authenticated in Application's Realm**.
  - To enable for specific users, select those users. The users must be listed in this role.



6. Click **OK** twice, and then click **Save**.

### 10.2.3 Setting up Discovery service for IBM Connections Mail

Have this information on-hand before executing this procedure:

- ▶ Administrator user IDs and passwords for your LDAP servers
- ▶ Names of LDAP servers and domains used by Microsoft Exchange servers
- ▶ (Exchange only:) User ID and password that can authenticate with the Microsoft Exchange Auto-discovery servers

Complete the following steps to set up the Discovery service for IBM Connections Mail:

1. If you use IBM Domino mail servers only, skip to step 3.
2. If you use Exchange mail servers, create a keystore certificate file. Complete the following tasks on each Exchange Auto-discovery server in your Active Directory:
  - a. Place copies of the certificates from your Exchange Auto-discovery servers onto the File-system of your Deployment Manager.
  - b. Open a command prompt and go to the directory of your Deployment Manager.
  - c. Run the following command:
 

```
keytool -import -file certificatefile.cer -alias servername -keystore keystore.filename
```
  - d. Define a six-character password and take note of it. You will need it for the configuration of Exchange servers in the socialmail-discovery-config.xml file.
  - e. Trust the certificate.
  - f. Append each IP address of your Exchange Auto-discovery servers to the hosts file of the WebSphere Application Server running IBM Connections Mail & your Deployment Manager.

3. Copy these files into the *WAS-root/AppServer/profiles/Dmgr01/config/cells/cell-name/LotusConnections-config* directory:

| File name                                | From                       | To   |
|--|----------------------------|--|
| socialmail-discovery-config-template.xml | C:\IBM\Connections Mail\   | C:\WAS-root\AppServer\profiles\Dmgr01\config\cells\cell-name\LotusConnections-config\socialmail-discovery-config.xml |
| socialmail-discovery-config-template.xml | /opt/IBM/Connections Mail/ | /WAS-root/AppServer/profiles/Dmgr01/config/cells/cell-name/LotusConnections-config/socialmail-discovery-config.xml   |
| socialmail-discovery-config.xsd          | C:\IBM\Connections Mail\   | C:\WAS-root\AppServer\profiles\Dmgr01\config\cells\cell-name\LotusConnections-config\socialmail-discovery-config.xsd |
| socialmail-discovery-config.xsd          | /opt/IBM/Connections Mail/ | /WAS-root/AppServer/profiles/Dmgr01/config/cells/cell-name/LotusConnections-config/socialmail-discovery-config.xsd   |

4. Rename the copied socialmail-discovery-config-template.xml file to *socialmail-discovery-config.xml*.
5. In the socialmail-discovery-config.xml file, replace the example information with your information. For each Mail-server configuration in your environment, you must have a ServerConfig tag with a unique name attribute. For example,
6. Within each ServerConfig tag, insert the following tags for the type of mail server that you use in your environment. There are three types of mail servers to choose from:
  - IBM Domino Servers only:
    - Insert the tags listed in the table:

| Property  | Value  |
|-----------|--|
|           | Enter DOMINO   |
|           | Enter the IP address or fully qualified host name of the Domino LDAP server that is used to determine the validity of email addresses and to return users' mail setup data.<br><br>Example: 9.119.6.07 or serverName.company.com |
| Optional: | To specify a port for the URL specified in the DirectoryServer tag, enter the port number.<br><br>The protocol for this port must match the protocol used to access Connections.   |
|           | Enter the name of an IBM Domino user that has full read access to the LDAP service.<br><br><b>Note:</b> Enter only the username. For example, do not include "cn=" or "domain/".   |
|           | Enter the password for the IBM Domino user specified in the DirectoryUser tag.   |

| Property  | Value   |
|-----------|---|
| Optional: | <p>To specify a mail server that might not be the user's primary server, enter the IP address or fully qualified host name, for example: 9.119.6.08 or https://serverName.company.com</p> <p>If this server includes a non-default port, the protocol must match the protocol used to access Connections, for example, 9.119.6.08 or https://serverName.company.com:843</p> |
|           | <p>For each domain of email addresses that use this server configuration, enter a &lt;MailPattern type=" " /&gt; containing the domain. The domain is the portion of the email address that follows the @ symbol.</p> <p>Example: &lt;MailPattern type="example.com"/&gt;</p>   |

- Insert the tags listed in the table. Example:

---

```
<ServerConfig name="domino1">
  <ConfigType>DOMINO</ConfigType>
  <DirectoryServer>domino1.example.com</DirectoryServer>
  <DirectoryUser>username</DirectoryUser>
  <DirectoryPW>adminpw</DirectoryPW>
  <MailPattern type="example.com" />
  <MailPattern type="example2.com" />
</ServerConfig>
```

---

- IBM Domino Mail Servers using iNotes redirector:

- Insert the tags listed in the table:

| Property | Value   |
|----------|---|
|          | Enter REDIRECT  |
|          | <p>Enter the URL to an IBM iNotes® redirection application.</p> <p>Example: http://domino2.example.com/dwaredir.nsf or http://domino2.example.com</p> <p>If this URL includes a non-default port, the protocol must match the protocol used to access Connections.</p> <p>Example: http://domino2.example.com:843</p> |
|          | <p>For each domain of email addresses that use this server configuration, enter a containing the domain.</p> <p>You can add multiple in the ServerConfig tag.</p> <p>Example: &lt;MailPattern type="domino2.example.com"/&gt;</p>   |

- Insert the tags listed in the table. Example:

---

```
<ServerConfig name="domino2-redirect">
  <ConfigType>REDIRECT</ConfigType>
  <RedirectURL>http://domino2.example.com</RedirectURL>
  <MailPattern type="example.com" />
```

---

```
<MailPattern type="example2.com" />
</ServerConfig>
```

---

– Microsoft Exchange Mail Servers:

- Insert these tags for Microsoft Exchange mail servers:

| Property | Value   |
|----------|---|
|          | Enter EXCHANGE.   |
|          | Enter the IP address or fully qualified host name of the Active Directory LDAP server that is used to determine the validity of email addresses and to return users' mail setup data.<br><br>Example: 9.119.6.77 or servername.example.com      |
|          | Enter the domain for access to the Active Directory Server.   |
|          | Enter the name of an Exchange user that has read access to the Active Directory.<br><br><b>Note:</b> Enter only the username. For example, do not include "cn=" or "domain/".   |
|          | Enter the password for the Exchange user specified in the DirectoryUser tag.  |
|          | Enter the file path and file name to the keystore file that was created in step 2.  |
|          | Enter the six-character password that was created in step 2.  |
|          | Enter the domain qualifier and user name used to authenticate to the Autodiscovery servers.<br><br>Example: SMDEV2010\Administrator   |
|          | Enter the password used to authenticate to the Autodiscovery servers.   |
|          | For each domain of email addresses that use this server configuration, enter a<br>type=" " /> containing the domain. The domain is the portion of the email address that follows the @ symbol.<br><br>Example:<MailPattern type="example.com"/> |

– Example:

```
EXCHANGE
exchange1.example.com
username
adminExpw
exchange1.example.com
c:\example\exchangecertificate
exampleCellManager01/certificateFileAuth
```

7. (Optional / Recommended): To encrypt user names and passwords in the socialmail-discovery-config.xml file, follow these steps:

- a. Using the Integrated Solutions Console, create aliases for each user name and password pair that you want to encrypt, by following these steps: Creating the J2C authentication data entry

([http://publib.boulder.ibm.com/infocenter/mpadoc/v7r0m0/index.jsp?topic=%2Fcom.ibm.websphere.wemp.doc%2Fconfiguring%2Fcreate\\_j2c\\_auth\\_de\\_t\\_mssql.html](http://publib.boulder.ibm.com/infocenter/mpadoc/v7r0m0/index.jsp?topic=%2Fcom.ibm.websphere.wemp.doc%2Fconfiguring%2Fcreate_j2c_auth_de_t_mssql.html)).

- b. In the socialmail-discovery-config.xml file, replace the following tags with the new tags indicated. In the new tags, enter the alias that corresponds to one that you created in WebSphere Application Server.

| Original tags                              | Replace with             |
|--|--------------------------|
| DirectoryUser and DirectoryPW              | DirectoryAuthAlias       |
| Exchange only: ADDomainUser and ADDomainPW | ADDomainAuthAlias        |
| Exchange only: CertificateFilePW           | CertificateFileAuthAlias |

Example:

```
<ServerConfig name="EncrytpedExchange2">
  <ConfigType>EXCHANGE</ConfigType>
  <DirectoryServer>exchange2.example.com</DirectoryServer>
  <DirectoryServerDomain>exchange2.example.com</DirectoryServerDomain>
  <DirectoryAuthAlias>exchangeLdapAuth</DirectoryAuthAlias>
  <CertificateFile>c:\example\exchangecertificate</CertificateFile>
  <CertificateFileAuthAlias>exampleCellManager01/certificateFileAuth</CertificateFileAuthAlias>
  <ADDomainAuthAlias>shimcon81CellManager01/addDomainAuth</ADDomainAuthAlias>
  <MailPattern type="exchange2.example.com"/>
</ServerConfig>
```

8. Delete examples from the xml file that do not apply to your environment.
9. Save and close the socialmail-discovery-config.xml file.
10. Synchronize the changes from the deployment manager to the nodes.

## 10.2.4 Enabling help for IBM Connections Mail

Complete the following steps to enable help for IBM Connections Mail:

1. Using the Administrator ID of your WebSphere Deployment Manager, open a command prompt.
2. Change directory to the WebSphere Deployment Manager's bin directory:

Examples:

Windows: C:\app\_server\_root\profiles\dmgr01\bin

Linux/AIX: app\_server\_root/profiles/Dmr01/bin

3. Then launch the wsadmin client:

Examples:

Windows: wsadmin.bat -lang jython -username *username* -password *password* -port 8879

Linux/AIX: sh wsadmin.sh -lang jython -username *username* -password *password* -port 8879

**Note:** See the following URL for more information on starting the wsadmin client:

Starting the wsadmin client

([http://www-10.lotus.com/ldd/1cwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Starting\\_the\\_wsadmin\\_client\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/1cwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Starting_the_wsadmin_client_ic40&content=pdcontent))

4. Next execute this command to work with the configuration of IBM Connections:



```
execfile("connectionsConfig.py")
```

5. If you are running AIX or Linux, create a temporary directory that allows writing:

```
mkdir /temp/dir
```

```
chmod +w /temp/dir
```

6. And then use this command to indicate the applications that you want to provide help information for. Note, application(s) not mentioned will not be included in the IBM Connections Help:

```
LCConfigHelp.setHelp("C:/temp","activities","blogs","bookmarks","communities","files","forums",homepage,"profiles","wikis","icemail")
```

7. Then open a web-browser and access the WebSphere Integrated Console.
8. Goto Applications → WebSphere Enterprise Applications.
9. Put a check beside the Help Application & click Stop.
10. Delete the directory that you specified in Step 6. Note, this directory will be recreated as the application starts.
11. Restart all Connections servers.
12. Open a web browser & login to Connections.
13. Enter the following URL into your browser, where test-user-email is a user's email address:

```
http://domino1.example.com/resources/discovery/DiscoveryServlet?email=test-user-email
```

The following information will be displayed in your web browser if IBM Connections Mail is configured correctly:

```
DOMINO domino1.example.com mail/user-email.nsf  
http://domino1.example.com/mail/testuser.nsf
```

# Customizing IBM Connections user experience

Customizing IBM Connections is one of the main steps in deploying the product beyond the initial installation. Many social business projects want to stamp the organizations branding, naming, look and feel, and so forth on the system. In some situations, it is necessary to blend the IBM Connections user interface into the UI of a corporate portal or other systems so that the whole experience is uniform.

In this section, we explore how to customize the user interface of IBM Connections. IBM provides extensive documentation on this in the IBM Connections 4 product documentation ([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_ic40&content=pdcontent))

## 11.1 Branding

One of the first targets for any customization is the basic branding of the IBM Connections user interface. For the most part the white sections should be left alone and the basic layout of the system should not be customized to ensure future functionality and upgrades work. However, the top banner and the links it displays is a common candidate for customization.

To change the color scheme and the navigation options in the top banner bar, you change the header.jsp file, according to the instructions below:

1. Enable customization debugging - see [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_and\\_disabling\\_customization\\_debugging\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_and_disabling_customization_debugging_ic40&content=pdcontent).
2. Follow the instructions at [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_the\\_navigation\\_bar\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_the_navigation_bar_ic40&content=pdcontent) to modify the header.jsp file which contains the navigation bar.

3. Re-disable customization debugging - see

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_and\\_disabling\\_customization\\_debugging\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_and_disabling_customization_debugging_ic40&content=pdcontent).

You might also want to add your organization's logo to replace the IBM logo at the top left. Again, follow these instructions:

1. Enable customization debugging - see

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_and\\_disabling\\_customization\\_debugging\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_and_disabling_customization_debugging_ic40&content=pdcontent).

2. Follow the instructions at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Changing\\_the\\_IBM\\_Connections\\_logo\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Changing_the_IBM_Connections_logo_ic40&content=pdcontent) to customize the logo.

3. Re-disable customization debugging.

A variety of the standard user interface objects, such as the header, the login page, and the footer can be customized to reflect your organization's requirements. This might include links to your helpdesk or other systems, certain terminology or other disclaimers you need to present. Follow these instructions:

1. Enable customization debugging.

2. Follow the instructions at the link below to customize the user interface

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_the\\_user\\_interface\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_the_user_interface_ic40&content=pdcontent).

Specific instructions for the login screen can be found at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_the\\_login\\_page\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_the_login_page_ic40&content=pdcontent).

3. Re-disable customization debugging.

Because the first impressions are very important, especially in a system such as this, some organizations choose to brand the Getting Started page to have organization-specific information. Some systems include an IFRAME to a new section held on another system which might show corporate news, or a feed from somewhere else. Importantly, the structure of the Getting Started page is intended to allow customization to suit your requirements.

Detailed instructions can be found at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_the\\_Getting\\_Started\\_view\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_the_Getting_Started_view_ic40&content=pdcontent).

More advanced branding can be achieved by modifying the style sheets

([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Adding\\_styles\\_to\\_the\\_IBM\\_Connections\\_stylesheet\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Adding_styles_to_the_IBM_Connections_stylesheet_ic40&content=pdcontent)) associated with IBM Connections (see this link too [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Making\\_extensive\\_color\\_and\\_style\\_changes\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Making_extensive_color_and_style_changes_ic40&content=pdcontent)) This should be attempted by a skilled web designer. In addition to this, you may also wish to include your own custom Java script which might offer further context sensitive help. IBM has documented ways that you can achieve this at [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Adding\\_custom\\_Java\\_script\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Adding_custom_Java_script_ic40&content=pdcontent).

[4.0+documentation#action=openDocument&res\\_title=Overriding\\_and\\_extending\\_JavaScript\\_in\\_IBM\\_Connections\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Overriding_and_extending_JavaScript_in_IBM_Connections_ic40&content=pdcontent).

Lastly, your organization may wish to change the terminology used in Connections. Some organizations prefer to call Activities Projects, others want to call wikis Knowledge Bases, and so on. IBM has documented how to do this at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_product\\_strings\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_product_strings_ic40&content=pdcontent).

## 11.2 Multiple language support

IBM Connections 4 supports many languages. In some situations, this might not be ideal such as a native Spanish speaker using an American English browser, or a Swiss Italian user on a Swiss German browser. The user's browser identification string is used by IBM Connections to determine which language to display the user interface in.

Some configuration changes are necessary to allow the user to override the default language choice imposed by IBM Connections. Full instructions on doing this can be found in the IBM Connections 4 documentation wiki at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_users\\_to\\_set\\_a\\_language\\_preference\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_users_to_set_a_language_preference_ic40&content=pdcontent).

## 11.3 Profile types

One of the intentions of the Profiles component of IBM Connections is to provide a comprehensive corporate directory for the people in the organization. Presenting much of the difficult-to-find person information, such as skills, background, employee numbers, and the likes is one of the first steps to socializing an organization.

The data model and user interface for Profiles can be customized heavily and common extensions made by organizations include people's LinkedIn profiles, Twitter handles, personal blogs, and so on. Another common extension in Profiles is to provide a Google Maps lookup of the users location.

The IBM Connections documentation describes the customization of the Profiles data model and user interface extensively is at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_Profiles\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_Profiles_ic40&content=pdcontent).

You should also consider how you might automate the integration of other systems in to the Profile information. For example a person's working hours might be a useful thing to publish in the Profile so that others wanting to contact that person can know when they will be at their desk. It is impractical to manually provide this information but it could well be information that you hold in your human resource (HR) system.

Using customized Assembly Lines in the Tivoli Directory Integrator product, which is provided as part of the Connections installation, you can pull this kind of information in from your HR system and, by customizing the data model and user interface of the Profile can display the additional information you need from the other system.

**Note:** For further information on this topic, please see [http://infolib.lotus.com/resources/connections/4.0/doc/en\\_us/ic4\\_p3.html#c\\_admin\\_profiles\\_develop\\_custom\\_tdi\\_scripts](http://infolib.lotus.com/resources/connections/4.0/doc/en_us/ic4_p3.html#c_admin_profiles_develop_custom_tdi_scripts).

## 11.4 Notification

When installing Connections, an important post-installation configuration step is to ensure that the email address that is used as the sender address of email notifications complies with your corporate guidelines. If you do not customize the sender address you will typically receive emails from **news-admin@example.com** and other such standardized addresses.

To customize the “administrator” email addresses used (like news-admin@example.com), use

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Defining\\_valid\\_administrator\\_email\\_addresses\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Defining_valid_administrator_email_addresses_ic40&content=pdcontent).

To customize which notifications end users receive, review

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_users\\_to\\_specify\\_email\\_notification\\_preferences\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_users_to_specify_email_notification_preferences_ic40&content=pdcontent).

The content of the email notifications themselves can also be customized. Doing so is quite a lengthy process and involves the use of a specialist markup language called Freemarker (<http://freemarker.sourceforge.net/>).

- ▶ To customize the email digests (sent out at scheduled intervals), review [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_email\\_digests\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_email_digests_ic40&content=pdcontent).
- ▶ To customize the individual email notifications (sent when users choose to notify others when they create something), review [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_standard\\_notifications\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_standard_notifications_ic40&content=pdcontent).

## 11.5 Renaming Applications

Before attempting to rename the applications in IBM Connections you should read the guidance on Best Practices for Customizing Connections

([http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_the\\_user\\_interface\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_the_user_interface_ic40&content=pdcontent)).

Renaming individual applications can be achieved by changing the product strings.

**Note:** For more information, see [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_product\\_strings\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_product_strings_ic40&content=pdcontent).

## 11.6 Hiding Applications

When installing IBM Connections, you can choose which applications you wish to install. In many cases, this is all of the components of the solution. In others, because of your standard entitlements, it might only be Profiles and Files. If you want to restrict access to certain applications within the IBM Connections product suite, such as Wikis, Activities, or Blogging, it is possible to temporarily (or permanently) disable that application and then hide it from the user interface.

Full instructions on doing this can be found at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Disabling\\_an\\_application\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Disabling_an_application_ic40&content=pdcontent).



# Integrating with other software

IBM Connections' open platform provides capabilities to deliver the most comprehensive integrated social environment. You can Integrate your IBM solutions and 3rd party solutions to extend your enterprise social software platform.

## 12.1 WebSphere Portal

IBM WebSphere Portal provides core portal services that aggregate applications and content and delivers them as role-based applications. IBM Connections applications can be deployed as portlets, so that portal users can access the IBM Connections applications directly along with the portlet application. These portlets communicate with IBM Connections applications services and retrieve the data for each applications This helps user can participate in social networking activities for example writing blogs or posting any topic to forums. IBM Connections server and WebSphere Portal server should be deployed in same network and Lightweight Third Party Authentication (LTPA) token should be exchanged between these two servers to participate in Single Sign On (SSO).

### 12.1.1 IBM Connections application portlets

The following IBM Connections applications are available as portlets:

- ▶ Profiles Summary
- ▶ Profiles
- ▶ Forums Summary
- ▶ Forums
- ▶ Community Overview
- ▶ Bookmarks Summary
- ▶ Bookmarks
- ▶ Blogs Summary
- ▶ Blogs



- ▶ Activities
- ▶ Wikis

Portlets are available only for IBM Connections V 3.0.1.1 only and these portlets work on IBM Connections 4.0 server also. These portlets can be downloaded from Greenhouse solutions catalog and there is no support from IBM. The URL for downloading the portlet is <http://greenhouse.lotus.com>

### 12.1.2 Installing and Configuring IBM Connections portlets

Complete the following steps to install and configure an IBM Connections portlet into a WebSphere Portal environment:

1. Download the application from greenhouse solution catalog, <http://greenhouse.lotus.com>
2. Extract the application to a temporary directory.
3. Install a portlet using WebSphere Portal Administration Interface.
4. Copy the following files to /shared/app.
  - /POCResolver/com.ibm.lconn.lcaccelerator.poc.jar
  - /REP/com.ibm.lconn.lcaccelerator.rep.jar
5. Create a page and add portlets to that page.
6. Add IBM Connection server URLs to WebSphere Resource Environment provider.
7. Configure DynaCache for IBM Connections portlets.
8. Setup an authentication alias to manage VMM services.
9. Configure application specific AJAX-proxy settings for Connection portlets.
10. Import SSL certificates from Connection Server to Portal Server to establish secured connection.
11. Export the LTPA token from IBM Connection server to WebSphere Portal server to enable Single Sign On (SSO).

### 12.1.3 Test integration with WebSphere Portal

You can use the following steps to test the installation and configuration of the portlet:

1. Login to WebSphere portal with a valid user ID.
2. Navigate to a page where IBM Connection portlets are deployed.
3. User is logged into the specific application automatically.
4. If there are any issues found, check out the SystemOut and System Error log files found at directory[WJC2] to troubleshoot the issue.

## 12.2 Sametime

If you have an IBM Sametime proxy server configured in your organization and have the Profiles application deployed, you can enable presence awareness and simple chats in IBM Connections.

When you enable presence awareness using the Sametime Proxy server, a person's online status is indicated by a set of icons and an associated status message that is available from the person's profile and business card. Presence awareness can tell you whether the person is available to chat, busy in a meeting, or away from their computer. In addition to seeing a person's availability, you can also chat with that person even when no Sametime client is installed.

## 12.2.1 System requirement

You must have the following software enabled to be able to add presence awareness to IBM Connections:

- ▶ Domino Server 8.5 or later
- ▶ IBM Sametime 8.5.2 Interim Feature Release 1 or later, with the Sametime System Console, Sametime Community Server, and Sametime Proxy Server components.

## 12.2.2 Pre-requisite

Before you start setting up Sametime function, enable single sign-on between the Domino environment and the IBM Connections server.

## 12.2.3 Procedure

1. Start the wsadmin client from the following directory of the system on which you installed the deployment manager:

```
app_server_root\profiles\dm_profile_root\bin
```

2. Use the wsadmin client to access and check out the IBM Connections extension configuration files.
3. Enter the following command to access configuration file

---

```
execfile("connectionsConfig.py")
```

---

4. Enter the following command to check-out the LotusConnections-config.xml file

---

```
LCConfigService.checkOutConfig("working_directory","cell_name")
```

---

5. From the directory you specified as the working directory in the previous step, open the *LotusConnections-config.xml* file in a text editor, and then find the sametimeProxy service section.
6. Specify the attributes as per the example below:

---

```
<sloc:serviceReference enabled="true" isConnectClient="true"
serviceName="sametimeProxy"
ssl_enabled="true"><sloc:href><sloc:hrefPathPrefix/>
<sloc:static href="http://sametimeproxyserver.enterprise.example.com/"
ssl_href="https://sametimeproxyserver.enterprise.example.com:9444"/>
<sloc:interService
href="https://sametimeproxyserver.enterprise.example.com:9444/>
</sloc:href>
</sloc:serviceReference>
```

---

7. Save and close the *LotusConnections-config.xml* file.

8. Run the following command to check-in the changes

---

```
LCCConfigService.checkInConfig(working_directory,cell_name)
```

---

9. Run the following command to sync the nodes

---

```
synchAllNodes()
```

---

10. Exit the wsadmin prompt by typing **exit**.

11. Stop and restart all IBM Connections application servers.

## 12.3 Quickr

Using the IBM Connections Connector for Quickr you can integrate the Communities within IBM Connections with the Team Space and Files within a Quickr implementation. To find out more, read

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Customizing\\_product\\_strings\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Customizing_product_strings_ic40&content=pdcontent).

You can also integrate file storage within Activities to publish files into Quickr instead of holding the file in the Activity itself. The result is that the file is published to a Quickr place and a link placed into the Activity to the file in Quickr, rather than the file residing in two places. For information on implementing this feature, review

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Integrating\\_Activities\\_with\\_IBM\\_Lotus\\_Quickr\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Integrating_Activities_with_IBM_Lotus_Quickr_ic40&content=pdcontent)

For optimum results, you should enable Single Sign-On between the IBM Connections environment and the Quickr environment. If your Quickr environment is based in IBM Domino, you must import an LTPA token from the IBM WebSphere Application server running IBM Connections into the Domino server running Quickr. Full instructions on exporting the LTPA keys from WebSphere and importing them into Domino can be found at

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Enabling\\_single\\_signon\\_for\\_Domino\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_single_signon_for_Domino_ic40&content=pdcontent)

## 12.4 FileNet

IBM FileNet P8 is a reliable, scalable, and highly available enterprise platform that enables you to capture, store, manage, secure, and process information to increase operational efficiency and lower total cost of ownership. IBM Connections can be integrated with IBM FileNet Content Manager using linked library widgets so that documents can be stored in content repository.

FileNet Services for IBM Quickr is an adaptable web service component that integrates IBM Connections server and IBM FileNet Content Manager. A Linked Library is a custom IBM Quickr widget installed on the IBM Connections server and by default it is not enabled.

## 12.4.1 Configuring FileNet

FileNet P8 Content Engine and FileNet services for IBM Quickr need to be installed and configured prior to integrating with IBM Connections server. A library object is created in the FileNet P8 Enterprise Content Manager (ECM) to manage all the documents and folders.

1. Install and Configure FileNet P8 server on an appropriate platform. For detailed steps, see FileNet documentation at <http://www-01.ibm.com/support/docview.wss?rs=86&uid=swg27021508>
2. If FileNet is installed on a Linux platform, install FileNet Enterprise Manager (FEM) on a Windows platform so that the FileNet Content Engine can be managed from FEM.
3. Install and configure FileNet Services for Quickr on an appropriate platform.
4. Install FileNet Services for Quickr add-ons to FileNet Object Store.
5. When the above steps are completed, you will see QuickrRoot under RootFolder in FileNet Enterprise Manager.
6. Create a library and apply the necessary access settings.
7. Enter the following URL to validate the library:

*http: < fully qualified Quickr services hostname>:/dm/atom/libraries/feed*

8. To validate FileNet Services for Quickr services, enter the following URL. This service status would be either running or stopped.

*http: < fully qualified quickr services hostname >:/dm*

## 12.4.2 Configuring IBM Connections

To use FileNet with IBM Connections server Linked library widget need to be enabled. To enable Linked library widgets, the configuration file need to be checked out to a temporary location and make a necessary changes and check-in to the configuration repository.

1. Start the wsadmin client from Deployment Manager Profile Directory where IBM Connection server is installed:  
`/wsadmin.sh(bat) -lang jython -username -password`
2. Run the Jython script interpreter using following command to initialize the Communities configuration file:

`execfile("communitiesAdmin.py")`

Now Communities Admin service is initialized.

3. Run the following command to check out the widget-config.xml:

`CommunitiesConfigService.checkOutWidgetsConfig("working_directory", "cell_name")`

Where

- cell\_name is the name of the WebSphere cell hosting the communities application.
- Working\_directory is the directory where configuration files are copied.

4. Go to working directory and add the following entries at the end of widget-config.xml to enable Linked library widget for IBM Connections communities.

---

```
<widgetDef defId="<Library Name>" bundleRefId="lc_clib"
url="{webresourcesSvcRef}/web/quickr.lw/widgetDefs/LibraryWidget_QCS_Connection
s.xml?etag={version}" description="CustomLibrary.description" modes="view edit
fullpage" primaryWidget="false"
```

```

helpLink="{helpSvcRef}/topic/com.ibm.lotus.connections.communities.help/c_com_1
library_frame.html" iconUrl="{contextRoot}/nav/common/images/iconFiles16.png"
uniqueInstance="true" displayLoginRequired="true"> <itemSet><item
name="allowCustomServers" value="false"/><item name="allowedHosts" value="
http://<FileNetQuickrServices Host Name>:<port>"/></itemSet></widgetDef>

```

---

5. Run the following command to check-in the widget-config.xml:

```
CommunitiesConfigService.checkInWidgetsConfig("working_directory","cell_name")
```

6. Run the following command to initialize the general service:

```
execfile("connectionsConfig.py")
```

7. Run the following command to check out the proxy-ecm-config.tpl file:

```
LCConfigService.checkOutProxyEcmConfig("working_directory", "cell name")
```

8. Go to the working directory and modify the proxy-ecm-config.tpl file to allow IBM Connections server to communicate with FileNet Services for Quickr server:

Before:

---

```

<proxy:policy url="http://www.myECMServer.com:8080/*" acf="none"
basic-auth-support="true">

```

---

After:

---

```

<proxy:policy url="http://<FileNet Services for Quickr>:<port>/*" acf="none"
basic-auth-support="true">

```

---

9. Run the following command to check in the proxy-ecm-config.tpl file:

```
LCConfigService.checkInProxyEcmConfig("working_directory","cell name")
```

10. Restart the IBM Connections server.
11. Log into IBM Connection server with administrator user ID.
12. Go to Communities tab and select a Community.
13. Select **Customize**.
14. Add the newly configured linked library widgets to the list.
15. Export the LTPA token from FileNet WebSphere Application server to IBM Connections WebSphere Application Server. The domain name must be same and share the same LDAP to enable Single Sign on (SSO) between IBM Connections and IBM FileNet ECM server.

### 12.4.3 Testing the integration with FileNet

When user adds documents or folders to Linked library in IBM Connections community application, the document is actually stored in the FileNet Content Manager. To validate the scenario, execute the following steps as mentioned below:

1. Login to the IBM Connection server with a valid user ID and password and go to Community where you want to work.
2. If the Community administrator added the linked library to the community, it will be shown to the user along with other widgets.
3. Select the Linked library widget.

4. Login to the FileNet Services for Quickr application with existing credential or new credential
5. Library will be retrieved from the FileNet Content Manager repository.
6. User can add files or folder that will be stored in the FileNet Content Manager repository.
7. Log out from the IBM Connections server after completing the task.

## 12.5 Microsoft

IBM Connections can be integrated into existing SharePoint Document Libraries to provide Communities with access to the file resources in SharePoint. This might be useful for organizations who have initially deployed SharePoint for file sharing and now wish to collaborate better using IBM Connections without abandoning their existing deployment Full details on implementing the SharePoint connector can be found at [http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=IBM\\_Connections\\_Widget\\_for\\_Microsoft\\_SharePoint\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=IBM_Connections_Widget_for_Microsoft_SharePoint_ic40&content=pdcontent).

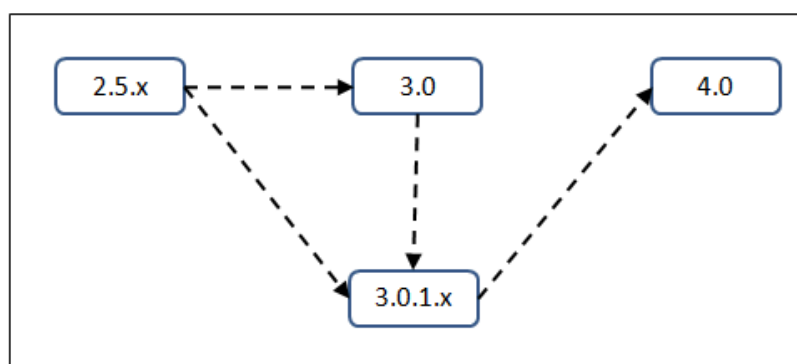
In addition to SharePoint, IBM Connections has a Microsoft Windows Desktop Integration tool which provides drag and drop access to the Files in IBM Connections to the Windows desktop. You can download the desktop enabler from the IBM Greenhouse Product Catalog at <https://greenhouse.lotus.com/plugins/plugincatalog.nsf/assetDetails.xsp?action=editDocument&documentId=8AE593DC335311DE852579C2006D6F66>



# Upgrading from previous versions

You can directly migrate your IBM Connections to version 4 if your current installation is on version 3.0.1.x. For earlier versions, you must do an incremental upgrade.

The following figure shows the incremental upgrade between various IBM Connections versions.



## 13.1 Before you begin

Ensure that your environment meets the hardware and software requirements for IBM Connections 4.0. If you have a version of IBM Connections that is earlier than version 3.0.1.x, you must migrate it to version 3.0.1.x before migrating to version 4.0.

If you plan to install the new Metrics application, it is recommended to deploy IBM Cognos Business Intelligence before installing IBM Connections 4.0. However, you can defer deploying Cognos and still install Metrics.

Plan and choose your migration strategy depending on your requirement.



## 13.2 Migration process

Further sections in this chapter will guide you on how you can migrate your IBM Connections environment to 4.0.

### 13.2.1 Saving existing customization

Before you upgrade your environment, it is very important that you save your customizations from the existing setup. You will have to reapply most of the customizations again manually.

The files that you need to migrate again manually include:

- ▶ User interface (customized CSS, JSP, and HTML; labels and strings)
- ▶ Header and Footer
- ▶ Email notification templates
- ▶ Blog themes
- ▶ Security role mappings
- ▶ service-location.xsd
- ▶ profiles-policy.xml
- ▶ validation.xml
- ▶ JavaScript.
- ▶ IBM Connections Connector for IBM Quickr
- ▶ Server whitelist for publishing file attachments from Activities to IBM Quickr

### 13.2.2 Backing up your IBM Connections environment

It is recommended to back up your databases and applications before starting the upgrade process.

How to take the back up is your choice and you can take a decision depending upon your environment. You can choose between backing up the entire deployment at once or individual applications.

### 13.2.3 In-place upgrades

There are several procedures required to migrate your deployment. Your migration strategy determines which procedures you need to follow. An in-place strategy minimizes costs but causes more downtime. It is similar to the side-by-side strategy except that you do not need to deploy new hardware.

The main advantage of using this strategy is that you need minimal new systems. The disadvantages of this method are the down time is longer and if instructions are not followed and an unclean installation is done then the environment can be corrupted.

Use these steps for in-place migration:

1. Save your customizations.
2. Create a back-up these elements of your current 3.0.1.x environment:
  - IBM Installation Manager data directory
  - IC\_Home, Installation Manager and SSPShared directory
  - WebSphere Application Server profile directory
  - profileRegistry.xml file located under WAS\_HOME/properties

3. Copy the migration tool in the current environment under */migration* directory.
4. Export application data.
  - Perform full synchronization of all the nodes.
  - Rename *migration* directory.
  - Copy the **migration\_4.0.0.0\_date\_time.zip** file from the *IBM\_Connections\_Install/IBMConnections/native* directory of the installation media, where date and time represent the date and time stamps of the file.
  - Extract the file to the IBM Connections 3.0.1.x installation directory. You should get a *migration* directory at the same directory level as the *ConfigEngine* directory.
  - Open a command prompt on the version 3.0.1.x system, change to the migration directory and run the following command depending on your OS:  
`./migration.sh|bat 1c-export.`
  - Back up the migration directory to a location outside your 3.0.1.x deployment.
5. Shut down your 3.0.1.x deployment and uninstall it.
6. Clean up all the nodes.
7. Upgrade database to 4.0.
8. Upgrade Websphere Application Server to 7.0.0.21.
9. Delete local content store and anything related with search in shared content store.
10. Install IBM Connections 4.0.
11. Create a back-up copy of WAS Deployment Manager profile directory.
12. Keep the Deployment Manager running but shut down all the nodes.
13. Copy the exported applications data to the 4.0 environment under */migrations/work*.
14. Import application data using:  
`/migration.sh|bat 1c-import -DDMuserid= -DDMPassword=`
15. Restart Deployment Manager.
16. Start and sync all nodes and start cluster.

### 13.2.4 Side-by-side upgrades

A side-by-side migration strategy minimizes the downtime of your production environment but costs more in terms of hardware resources. The advantage of this upgrade method is that minimum down time is required. The disadvantage is that you will need new systems.

Use these steps for this side-by-side migration:

1. Save your customizations.
2. Copy the migration tool in your 3.0.1.x environment under */migration*.
3. Export application data. Refer to in-place migration section for the procedure.
4. Install and configure a new WAS instance on your new system.
5. Create a new location for 4.0 content store.
6. Install 3.0.1 test database on new instance and transfer the 3.0.1.x database to the test database and update 4.0.
7. Install IBM Connections 4.0 on the new system.
8. Create a back-up copy of the WAS Deployment Manager profile directory.

9. Run the Deployment Manager but shut down all the nodes.
10. Copy the exported applications data to new system under *<IC\_Home>/migration/work*.
11. Import application data using:  

```
/migration.sh|bat 1c-import -DDMuserid= -DDMPassword=.
```
12. Restart Deployment Manager.
13. Start and sync all the nodes and start cluster.
14. Verify your new setup.
15. Shut down 3.0.1.x deployment.
16. Copy 3.0.1.x content store to 4.0 content store.
17. Perform in- place database upgrade.
18. Modify your JDBC and other parameters accordingly.

### 13.2.5 Restoring customization

After updating or migrating IBM Connections, you must manually update any custom fields and customized files that could not be automatically updated or migrated.

1. Migrate any JSP, CSS, and string customizations.
2. Verify that your Blogs themes are present in 4.0. If not, manually update them.
3. Update your customized Community themes.
4. Copy the 3.0.1.x version of the *profiles-policy.xml* file to the 4.0 deployment, overwriting the 4.0 version of the file.
5. Copy the customized XSD elements of the 3.0.1 *service-location.xsd* file to the 4.0 version of the file.
6. Redefine customized Profiles fields in the *validation.xml* file.
7. Migrate your 3.0.1 JavaScript customizations.

# Administering IBM Connections

IBM Connections administration includes configuration and on going support. In this section, we describe some of the on-going support tasks and the tool. This section includes the following topics:

- ▶ 14.1, “Introducing the Integrated Solutions Console” on page 234
- ▶ 14.2, “Working with servers” on page 237
- ▶ 14.3, “Finding and using server logs” on page 240
- ▶ 14.4, “Working with enterprise applications” on page 243
- ▶ 14.5, “Using wsadmin to modify and update application settings” on page 246
- ▶ 14.6, “Where is the IBM Connections data” on page 247
- ▶ 14.7, “Backing up and protecting data” on page 249

## 14.1 Introducing the Integrated Solutions Console

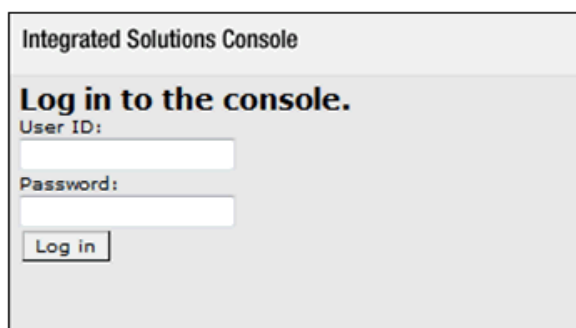
The WebSphere Network Deployment environment for IBM Connections consists of a single cell with multiple deployed servers and clusters within it. The cell therefore has a process called the *deployment manager* whose job is to manage the configuration for every server within the cell that it is responsible for. This is done through a single administrative environment called the Integrated Solutions Console (ISC).

Regardless what WebSphere based product that you are working with, there is always an ISC for you to log into and manage your environment. To work with IBM Connections environment, you must log into the ISC from any browser by typing

**`https://9043/ibm/console`**

The default port the ISC is installed on is 9060 (unsecure) and 9043 (secure). In most cases, it redirects URLs to 9043. Any install of WebSphere Application Server contains an ISC for you to login to and the default ports are always 9060 and 9043.

Here is the login screen for the ISC. The name and password asked for here are the ones that you use when you originally installed WebSphere, usually "wasadmin" as the login name and whatever you chose as the password.

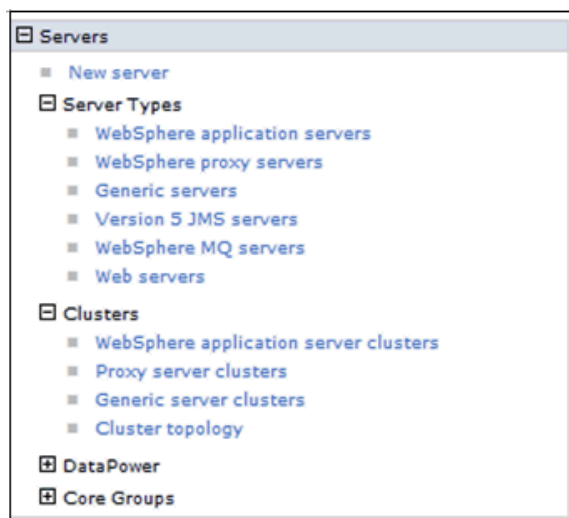


If you can not login here, consider if the login you set up also exists in LDAP, in which case, WebSphere sees it as a duplicate login and it will not work. You must remove the login from LDAP so it is unique as a WebSphere account.

The ISC menu, after you log in, looks identical for any WebSphere 7.x hosted application. Therefore, when you learn where to find things, the same rules apply regardless of what application that you are working with. Here are some key menus within the ISC and what they do.

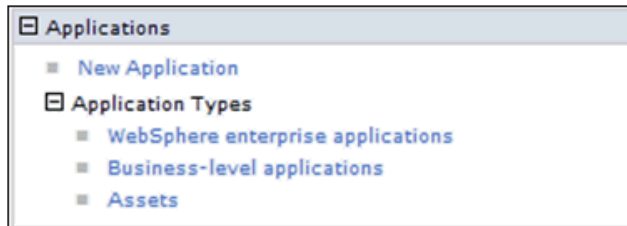
## Servers

The server menu is where you find the Application servers that are installed into this cell and details of any WebSphere proxy servers, web servers, and cluster configurations. Under each menu you can see and manage the running status of the servers.



## Applications

The applications menu is where you find any installed J2EE applications, such as each of the IBM Connections applications that are installed. These menus allow you to review, restart, and update individual applications.



## Security

The Global Security menu is where you define the LDAP servers and application security and configure the single sign-on options.



## Users and Groups

The users and groups menus are where you can search the directories for accounts to confirm LDAP is set up correctly. You can use the "Administrative user roles" and "Administrative group roles" menus to configure access to the ISC itself.

**Note:** These roles do not refer to access to the actual applications such as Blogs, Wikis, and Activities, that access is configured under the Enterprise Application menus.



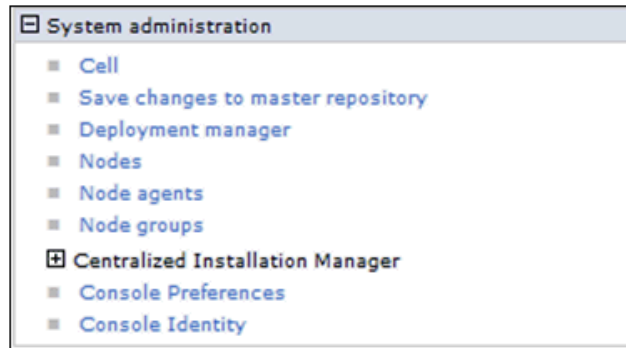
## Troubleshooting

The Logs and trace menus under Troubleshooting are where you can view the log activity for each server and cluster as well as altering the diagnostic logging level. If you are asked by support to increase the logging level for a server in order to gather more data, you do so through the Logs and trace menu.



## System Administration

The system administration menus give you complete control over all the deployed servers and the status of their configurations. Managed by the deployment manager of the cell the menus contain a list of all the network deployed servers, nodes, and node agents. It is through these menus that changes are manually distributed out from the deployment manager to the nodes (by synchronizing the nodes). You can also use this section to instruct the Node agents to restart all their managed servers.



## 14.2 Working with servers

You can work with servers either using a command line directly or through the Integrated Solutions Console (ISC). In general, it is simpler to work with the server through the ISC where you have a single interface and location to work with. Otherwise, starting 10 servers means issuing 10 command lines from 10 different locations. Consider always that a WebSphere Application Server server cannot be started unless its node agent is already started because it is the node agent that is responsible for starting and stopping the servers.

Let us start by looking at the ISC and what it can tell us about the servers. The items highlighted on the servers menu below are those we use most often.

- ▶ *WebSphere application servers* shows you all WebSphere Application Server servers installed in the cell
- ▶ *Web servers* show you any defined web servers such as an IHS server that are being managed from within this cell



## 14.2.1 WebSphere Application Servers

This is where you find all servers being used in your IBM Connections environment and any defined cluster instances. In the figure below, you can see a list of some of the servers in our large scale IBM Connections deployment.

Cell=con-dmgrCell01, Profile=Dmgr01

**Application servers**

Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

Preferences

New Delete Templates... Start Stop Restart ImmediateStop Terminate

| Select                   | Name                                       | Node            | Host Name | Version     | Cluster Name       | Status |
|--------------------------|--|-----------------|-----------|-------------|--------------------|--------|
| <input type="checkbox"/> | <a href="#">ActivitiesCluster_server1</a>  | con-app01Node01 | con-app01 | ND 7.0.0.21 | ActivitiesCluster  | ➔      |
| <input type="checkbox"/> | <a href="#">ActivitiesCluster_server2</a>  | con-app02Node01 | con-app02 | ND 7.0.0.21 | ActivitiesCluster  | ➔      |
| <input type="checkbox"/> | <a href="#">BlogsCluster_server1</a>       | con-app01Node01 | con-app01 | ND 7.0.0.21 | BlogsCluster       | ➔      |
| <input type="checkbox"/> | <a href="#">BlogsCluster_server2</a>       | con-app02Node01 | con-app02 | ND 7.0.0.21 | BlogsCluster       | ➔      |
| <input type="checkbox"/> | <a href="#">CommunitiesCluster_server1</a> | con-app01Node01 | con-app01 | ND 7.0.0.21 | CommunitiesCluster | ➔      |
| <input type="checkbox"/> | <a href="#">CommunitiesCluster_server2</a> | con-app02Node01 | con-app02 | ND 7.0.0.21 | CommunitiesCluster | ➔      |

- ▶ *Name* is the name of the server and this cannot be changed. Name is defined during installation and this is what you use to identify the server when issue commands. The server name is case sensitive
- ▶ The *Node* is the name of the instance that manages this server. You can see that we have multiple servers all managed by the same node in our installation. The role of the Node is to start and stop the servers and ensure the configuration held by the deployment manager is updated onto the servers. The name of the Node cannot be changed after installation.
- ▶ *Host Name* is the location of the installed server. This is usually a fully qualified host name derived from the name of the physical or virtual server where the server was created. It is critical that this host name is resolvable from all servers within the cell. It is possible to change this host name after install by manually editing some XML files, however, this is not recommended. Therefore, ensure that your host names are correct before installing.
- ▶ *Version* is the WebSphere Application Server version installed for this server. This cannot be changed but will automatically update if the server is upgraded or patched. Not all servers have to be running the same version but it is best practice for them to do so.
- ▶ *Cluster Name* was defined during the earlier installation of IBM Connections. The Cluster Name cannot be changed post installation.
- ▶ *Status* shows a green arrow if the server is running, a red cross if the server is stopped, and a question mark in a circle if the node agent for the server is stopped which prevents the ISC from querying the server status. A question mark also shows if the ISC has problems reaching the server, usually due to DNS or firewall issues.

From the menus you can select multiple servers and choose to stop, start, or restart their instances. These options are only available if the server's node agent is started and the server is showing either a *started*(green right arrow) or *stopped*(red X). The advantage of starting and stopping the servers from this screen is that multiple servers on different machines can be managed at once.



Alternatively, you can view the status of servers, start, and stop them from a command line on the server itself. To do this, connect to a command line on your system and navigate to the profile containing the server that you want to work with. All WebSphere Application Server profiles appear under the AppServer directory. In Windows, this is default to **C:\Program Files\IBM\WebSphere\AppServer\profiles**. We do not recommend using the \program files\ path.

On Linux or AIX, the default is (case sensitive) **/opt/IBM/WebSphere/AppServer/profiles**.

The directory for the Deployment Manager profile is *DMgr01* and for the Application Servers *AppSrv01*. To manage an application server, you'd navigate to

*/AppSrv01/bin* and run the following commands:

**startServer.sh** (or **startServer.bat** on Windows)

**stopServer.sh** (or **stopServer.bat** on Windows)

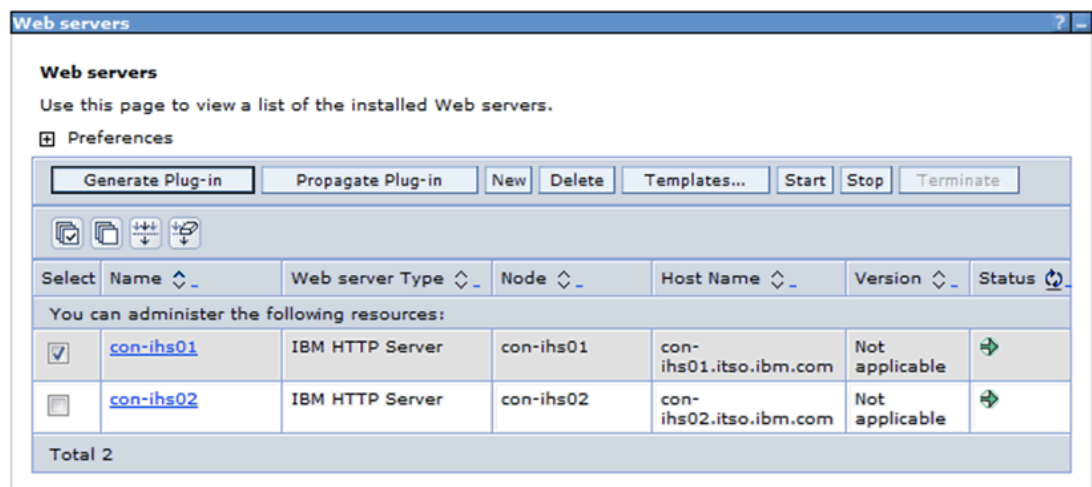
**serverStatus.sh** OR **-all** (or **serverStatus.bat** on Windows)

The stopserver and serverstatus commands prompt you for the WebSphere server credentials each time. If you want to avoid having to enter these continually, you can add them to the soap.client.props file in the \properties directory under each profile.

## 14.2.2 Web Servers

The menu Web Servers displays the integrated IBM HTTP Servers that have been configured into the ISC, because these are not WebSphere Application Server servers, they have no node agents and should always show as either started (right green arrow) or stopped (red X). The web servers can be started and stopped from this screen using the menu buttons. You can also start and stop the web servers from a command line by passing the parameters "start" or "stop" to the command httpd (for Windows) and apachectl (for Linux / AIX). For example:

**/opt/IBM/HTTPServer/bin/apachectl start**



## 14.3 Finding and using server logs

Every WebSphere Application Server server has the same directory structure by default and within that there is always a "logs" directory where the logs for that server are held. For each server instance in the profile, there is a specific folder under logs for that server. For example, if you have two servers in your AppSrv01 profile, plus the node agent, you will have three folders under "logs":

```
\AppSrv01\logs\nodeagent
\AppSrv01\logs\server1
\AppSrv01\logs\server2
```

There are four key log files that are created for every server:

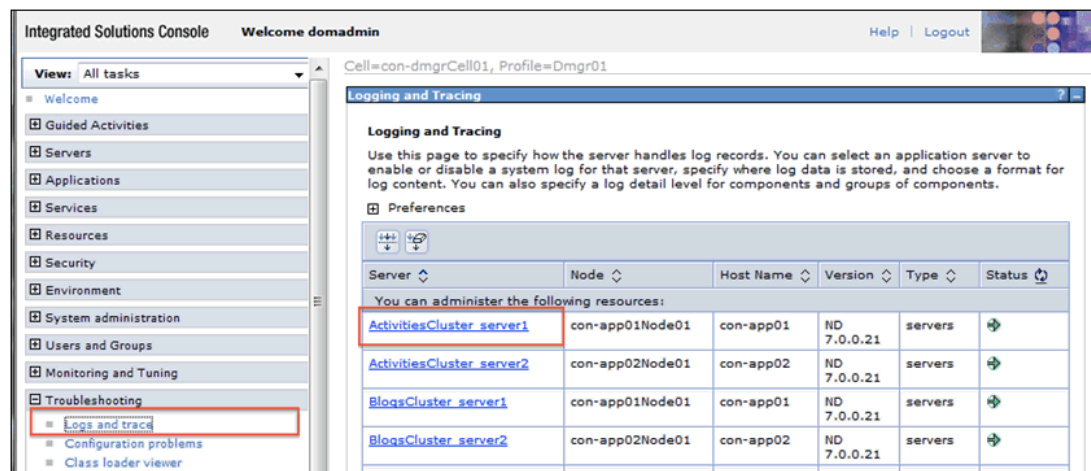
- ▶ **StartServer.log** - all activity as the server was issued a start command
- ▶ **StopServer.log** - all activity as the server was issued a stop command
- ▶ **SystemErr.log** - any errors being thrown by the server instance
- ▶ **SystemOut.log** - all activity as the server runs, essentially a server console output

There is also a directory called "ffdc" under the logs directory that contains exception log entries.

The log files can become very large and can only be deleted when the server is down. Therefore, it is a good practice to set up rollover logs. You can do this through the ISC Troubleshooting menu.

The logs and trace menu allows you to configure the logs, their location, their size, and their level of diagnostic detail. Each server is listed separately and each has specific configuration settings that apply to that server only. You cannot change the log settings for multiple servers at once.

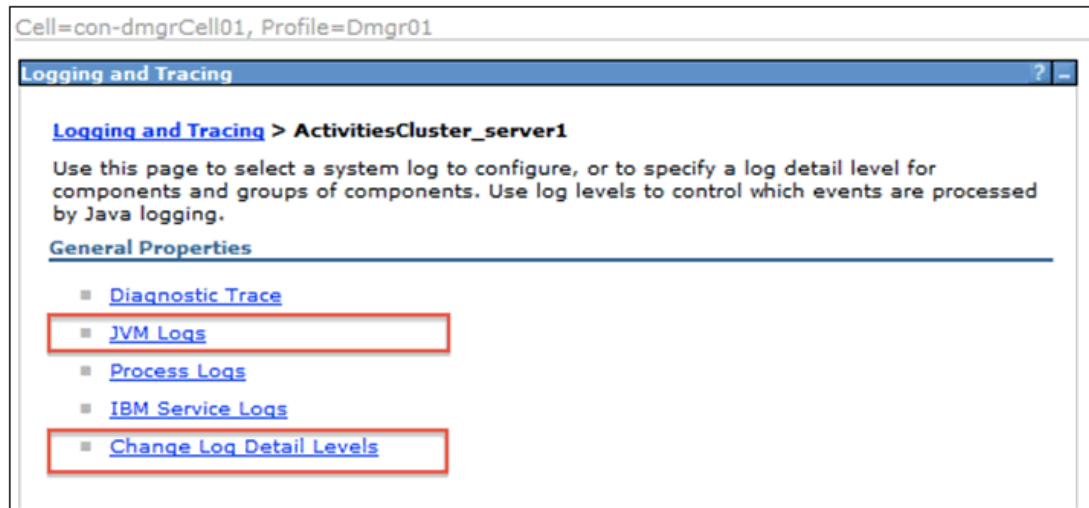
The following figure shows the ISC Logs and trace panel on our system. We start by selecting one of the listed servers.



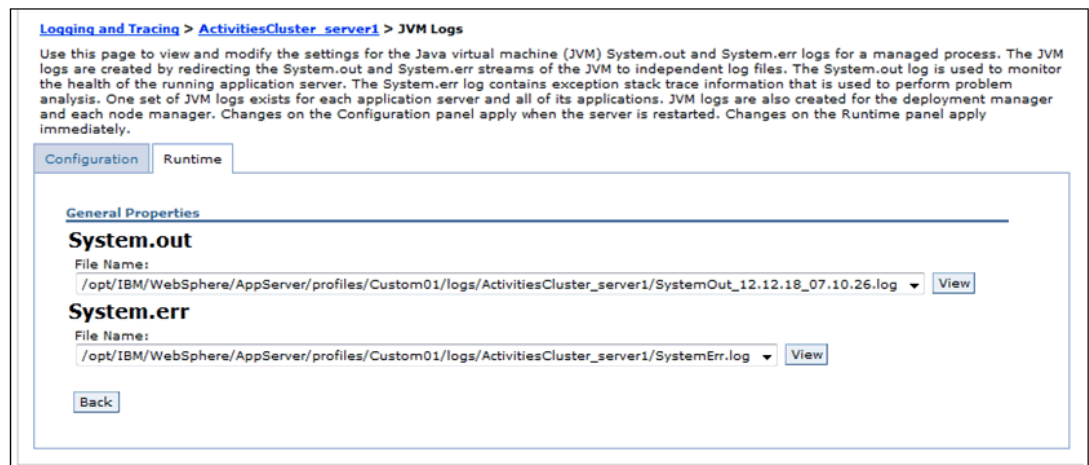
The general Properties lists options for what to do next. We use two menus:

- ▶ **JVM Logs** - where you can view and configure the size and location of the log files

- Change Log Detail Levels - where you can adjust the level of detail. In most cases the detail level is set to **\*=info** and this should not be changed unless instructed by IBM under a support call.



To start with, you can review the logs by going into JVM Logs and choosing the **“Runtime tab**. Here you see the critical SystemOut.log and SystemErr.log. These two files tell you what the server is doing and whether any errors are being generated. You can also see the location of the log files if you wanted to connect directly to the server and retrieve or read the log files from the file system.



The ISC has a built-in log file view that renders the current logs if you select "View" from the menu above. The log files are then read in line by line and you can navigate through them. The important thing to note about WebSphere Application Server log files is that they can become large and difficult to read through the small built-in viewer and it is usually a better idea to retrieve the files from the file system for reading.

The layout of a WebSphere Application Server log file is simple to spot any errors as, when properly aligned, there is a center column showing the status of each message, for example:

- I = informational message
- W = warning message
- E = error message

- F = fatal message
- C = configuration message

```

***** Start Display Current Environment *****
WebSphere Platform 7.0.0.21 (ND 7.0.0.21 cf211180.04) running with process name con-dmgrCell01/con-app01Node01/ActivitiesCluster_server1 and process id 4822
Host Operating System is Linux, version 2.6.27.19-0-default
Java version = 1.6.0, Java Compiler = j9jit24, Java VM name = IBM J9 VM
was.install.root = /opt/IBM/WebSphere/AppServer
user.install.root = /opt/IBM/WebSphere/AppServer/profiles/Custom01
Java Home = /opt/IBM/WebSphere/AppServer/java/jre
ws.ext.dirs = /opt/IBM/WebSphere/AppServer/java/lib:/opt/IBM/WebSphere/AppServer/profiles/Custom01/classes:/opt/IBM/WebSphere/AppServer/classes:/opt/IBM/WebSphere/AppServer/lib
Classpath = /opt/IBM/WebSphere/AppServer/profiles/Custom01/properties:/opt/IBM/WebSphere/AppServer/properties:/opt/IBM/WebSphere/AppServer/lib/startup.jar:/opt/IBM/WebSphere/3
Java Library path = /opt/IBM/WebSphere/AppServer/java/jre/lib/amd64/compressedrefs:/opt/IBM/WebSphere/AppServer/java/jre/lib/amd64:/opt/IBM/WebSphere/AppServer/bin:/usr/lib
***** End Display Current Environment *****
(12/16/12 9:49:10:606 EST) 00000000 ManagerAdmin I TRAS0017I: The startup trace state is "info.
(12/16/12 9:49:10:819 EST) 00000000 ManagerAdmin I TRAS0111I: The message IDs that are in use are deprecated
(12/16/12 9:49:10:872 EST) 00000000 ModelMgr I WVR08000I: Initializing core configuration models
(12/16/12 9:49:11:400 EST) 00000000 ComponentMeta I WVR01795I: The runtime provisioning feature is disabled. All components will be started.
(12/16/12 9:49:11:512 EST) 00000000 ProviderTrack I com.ibm.ffdc.osgi.ProviderTracker AddingService FFDC1007I: FFDC Provider Installed: com.ibm.ffdc.EmptyProvider(silent)
(12/16/12 9:49:11:531 EST) 00000000 ProviderTrack I com.ibm.ffdc.osgi.ProviderTracker AddingService FFDC1007I: FFDC Provider Installed: com.ibm.va.ffdc.impl.FfdcProvider@17131
(12/16/12 9:49:11:646 EST) 00000000 AdminInitializ ADM00151I: The administration service is initialized.
(12/16/12 9:49:12:082 EST) 00000000 PluginConfig I PLGC0057I: The plug-in configuration service started successfully.
(12/16/12 9:49:12:125 EST) 00000000 SSLComponent I CWPKI0001I: SSL service is initializing the configuration
  
```

To ensure the log files do not grow too large, you can also configure log file sizes for rollover and historical retention. You do this under the **"Configuration: tab:**

**Configuration** **Runtime**

**General Properties**

**System.out**

\* **File Name:**  
 \${SERVER\_LOG\_ROOT}/System.out

**File Formatting**  
 Basic (Compatible) ▾

**Log File Rotation**

☒ **File Size** ☐ **Time**

**Maximum Size**  
 20 MB

**Start Time**  
 24

**Repeat Time**  
 24 hours

**Maximum Number of Historical Log Files. Number in range 1 through 200.**  
 10

**Installed Application Output**

☒ **Show application print statements**

☒ **Format print statements**

Log file retention instructs the server to create a new instance of the SystemOut (or SystemErr) log file when it reaches a certain size or age. The recommendation is to have these files at least 20 MB in size, depending on how your internal monitoring and backup systems work. You might change to make the log file rollover time dependent instead.

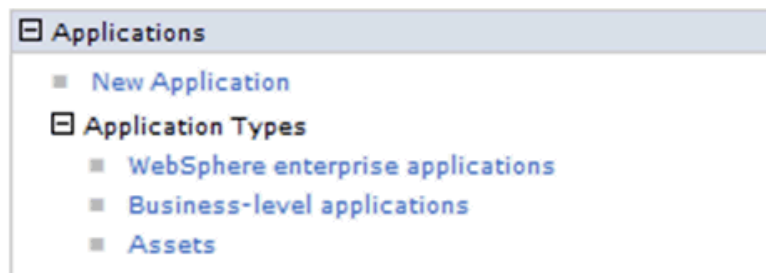
As each file is rolled over, the new file is created but the historical files are not removed unless you specifically configure that. In the configuration screen, you can also specify the number of historical files to retain, in the above example, we have chosen to create log files of 20 MB in size for SystemOut.log and retain 10 historical instances. We have the same options to set for

the SystemErr.logs. Because these are configuration settings, they will not take effect until the server they are being applied to is restarted.

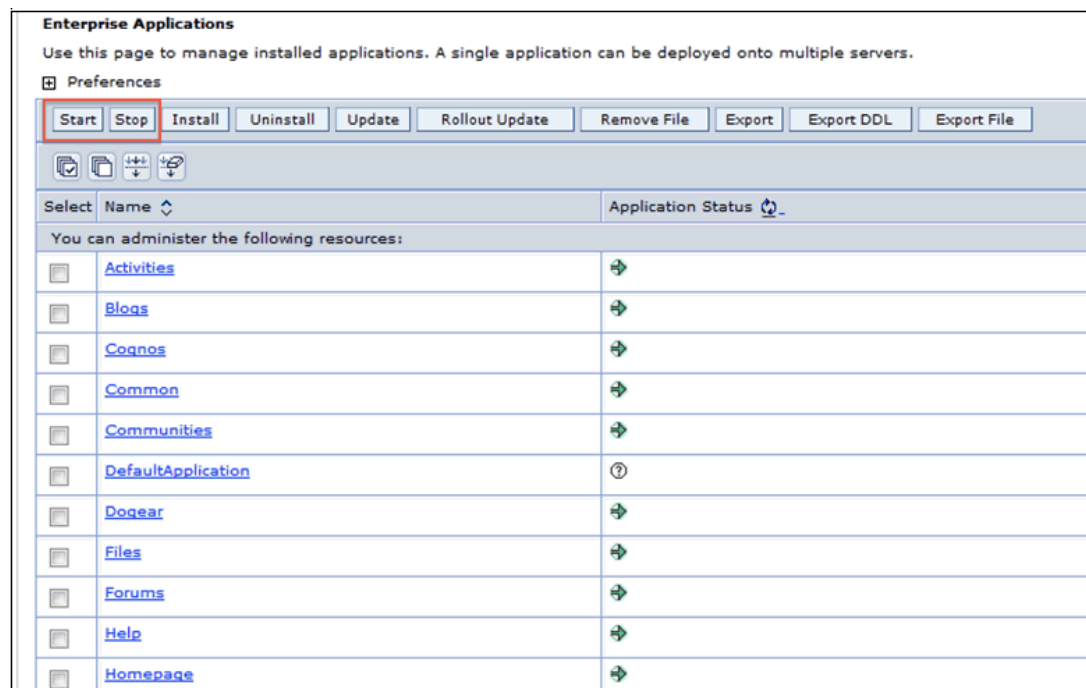
## 14.4 Working with enterprise applications

IBM Connections is installed as a series of enterprise applications hosted on a WebSphere Application Server server. In a full IBM Connections installation, you have a list of all IBM Connections applications under the *Enterprise Applications* menu. You can only use the *Start* and *Stop* menu items on this screen to manage the applications. Starting and stopping an application do not start or stop the server that hosts the application and therefore, server configuration changes do not be picked up by an application restart.

In some instances, during a patch upgrade, you might be required to update the application itself. This comes in the form of an *ear* file that is updated from this screen. This, however, is not usual practice in a standard deployment.



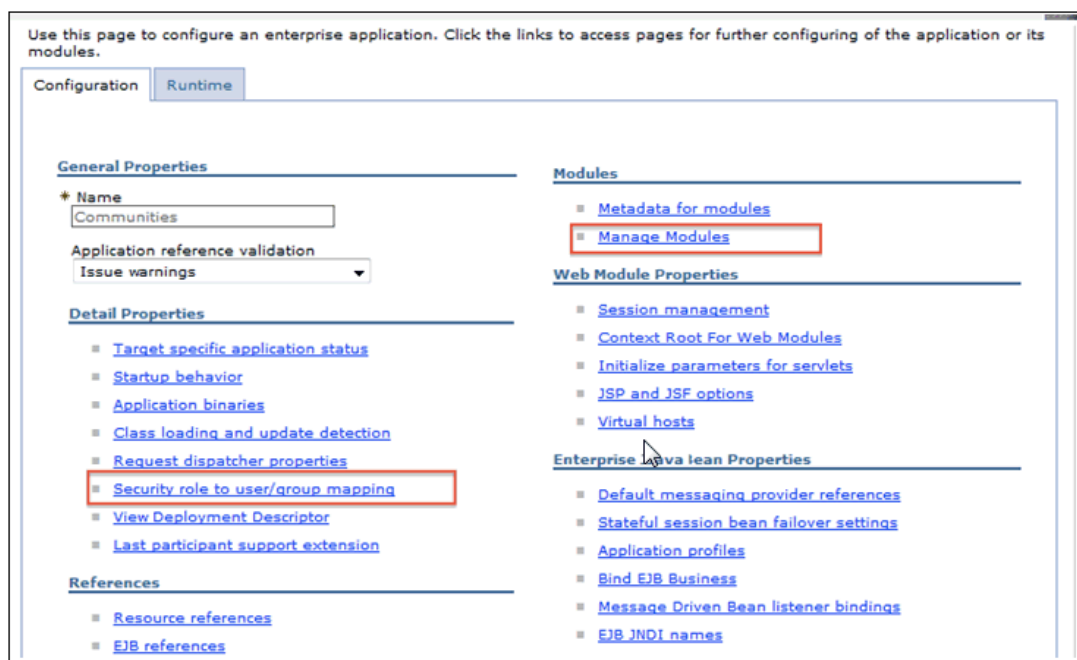
On the Enterprise Application panel, you can see which applications are successfully started (right pointing green arrow), stopped (red X), or unavailable (question mark). An application is shown as *unavailable* or *unknown* if the application's host server cannot be queried. In an IBM Connections installation, the initial server has a DefaultApplication installed. You do not need this and it can be left not running.



You do sometimes need to go into each application to work with the configuration of the application itself. This is different from the server configuration that is controlled by WebSphere. The application configuration is controlled by the designers of the application itself. An application installed on multiple servers is only listed once and uses the same configuration on each server where it runs.

If you select a particular application, there are two options that you primarily work with:

- ▶ Manage Modules - where you tell the application which server it is hosted on and which web server it is to route traffic to
- ▶ Security role to use group mapping - this is the application security written by the application designers.



### 14.4.1 Manage Modules

The Manage Modules menu takes us inside the design of each application where we can see the components that comprise the application. Each component should always be mapped to the same server and this mapping is automatically created during install of Connections. If the web server is installed after these applications or the web server is relocated post install, you might need to go in here and re-map the applications to a new server.

In the figures below, you can see that each module is mapped to a specific server, cluster, and web server instance.

**Enterprise Applications**

[Enterprise Applications](#) > [Communities](#) > **Manage Modules**

Manage Modules

Specify targets such as application servers or clusters of application servers where you want to install the modules that are contained in your application. Modules can be installed on the same application server or dispersed among several application servers. Also, specify the Web servers as targets that serve as routers for requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated, based on the applications that are routed through.

Clusters and servers:

```
WebSphere:cell=con-dmgrCell01,cluster=DogearCluster
WebSphere:cell=con-dmgrCell01,cluster=FilesCluster
WebSphere:cell=con-dmgrCell01,cluster=NewsCluster
WebSphere:cell=con-dmgrCell01,cluster=BlogsCluster
WebSphere:cell=con-dmgrCell01,cluster=HomepageCluster
```

| <input type="button" value="Remove"/> <input type="button" value="Update"/> <input type="button" value="Remove File"/> <input type="button" value="Export File"/> |   |   |             |  |
|---|---|---|-------------|--|
| <input type="checkbox"/> <input type="checkbox"/>   |   |   |             |  |
| Select  | Module                                    | URI   | Module Type | Server   |
| <input type="checkbox"/>  | <a href="#">EventPublisher</a>            | lc.events.publish.jar,META-INF/ejb-jar.xml        | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ihs02,server=con-ihs02<br>WebSphere:cell=con-dmgrCell01,node=con-ihs01,server=con-ihs01<br>WebSphere:cell=con-dmgrCell01,cluster=CommunitiesCluster |
| <input type="checkbox"/>  | <a href="#">ConsumerEJB</a>               | lc.events.subscribe.jar,META-INF/ejb-jar.xml      | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ihs02,server=con-ihs02<br>WebSphere:cell=con-dmgrCell01,node=con-ihs01,server=con-ihs01<br>WebSphere:cell=con-dmgrCell01,cluster=CommunitiesCluster |
| <input type="checkbox"/>  | <a href="#">Platform Command Consumer</a> | platformCommand.consumer.jar,META-INF/ejb-jar.xml | EJB Module  | WebSphere:cell=con-dmgrCell01,node=con-ihs02,server=con-ihs02<br>WebSphere:cell=con-dmgrCell01,node=con-ihs01,server=con-ihs01<br>WebSphere:cell=con-dmgrCell01,cluster=CommunitiesCluster |

## 14.4.2 Security Role to user and group mapping

The options for security roles are defined per application by the application designers to meet the requirements of that application. They are not 100% consistent across each application so it is important to review the documentation and understand the purpose of each role before making changes here.

It is possible to select multiple roles and map users and groups to those roles in one step. The list of groups or users are taken from your configured LDAP directory.

|  |                       |  |          |  |
|--|-----------------------|--|----------|--|
| <div> Map Users... Map Groups... Map Special Subjects ▼ </div> |                       |  |          |  |
| <input checked="" type="checkbox"/>                            |                       |  |          |  |
| <input type="checkbox"/>                                       | everyone              | Everyone                                 |          |  |
| <input type="checkbox"/>                                       | reader                | Everyone                                 |          |  |
| <input type="checkbox"/>                                       | person                | All Authenticated in Application's Realm |          |  |
| <input type="checkbox"/>                                       | metrics-reader        | Everyone                                 |          |  |
| <input type="checkbox"/>                                       | community-creator     | Everyone                                 |          |  |
| <input type="checkbox"/>                                       | community-metrics-run | All Authenticated in Application's Realm |          |  |
| <input type="checkbox"/>                                       | search-admin          | None                                     | domadmin |  |
| <input type="checkbox"/>                                       | global-moderator      | None                                     | domadmin |  |
| <input type="checkbox"/>                                       | admin                 | None                                     |          |  |
| <input type="checkbox"/>                                       | dsx-admin             | None                                     | domadmin |  |

- *Everyone* means all users who can access the application, even anonymous ones.
- *All Authenticated in Application's Realm* means all users who can login and be validated by your defined LDAP servers.

In a Connections environment there are some applications that do not support anonymous access (such as Profiles or Activities) because the application's functionality is based around a user being logged in.

## 14.5 Using wsadmin to modify and update application settings

Most of the application options and administration tasks need to be performed by using a command line interface called "wsadmin". You use wsadmin to start the command interface and then attach to each application to issue application-specific commands.

To run wsadmin, you always do the same thing, although it exists in the \bin directory under every server profile. In an IBM Connections environment, you usually run the command from the deployment manager's profile because your deployment manager handles the configuration of all other servers and applications. wsadmin is extremely case sensitive regardless of your platform. To start, use the following commands:

- Windows:

```
wsadmin -lang jython -username -password -port 8879
```

- Linux:

```
wsadmin.sh -lang jython -username -password -port 8879
```

This is run from \dmgr01\bin.

If you are prompted for which server to connect to, choose **server 1**. Once you have connected to the wsadmin command window, you can work with the applications by choosing which application you want to issue commands to and you do this by running the following command:

```
execfile("nameofapplicationfile")
```



For example, the Profiles application would be **execfile("profilesAdmin.py")**. Each application has its own command lines that are specific to its functionality. It is important to review the documentation and options for the application you want to work with.

After you have made changes or issued commands through the wsadmin interface, you must type **quit** to terminate it and write the changes back to the application itself.

One of the most common uses of wsadmin is to retrieve and edit the XML files that define how IBM Connections looks and behaves. Although it is possible to make changes to the XML files directly if you find them on the file system, using wsadmin is a best practice method for working with these files because it validates the changed XML before overwriting the configuration. Attempting to change XML files manually outside of wsadmin could result in faulty XML causing the application to fail completely.

## 14.6 Where is the IBM Connections data

The data for the IBM Connections applications falls into the following areas:

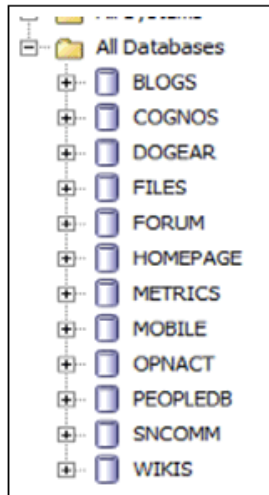
- ▶ Primary application data: This is held in dedicated databases on a DB2, SQL Server, or Oracle server
- ▶ Shared data: Supplemental application data such as attachments uploaded into applications that are located on a file system location accessible to every server
- ▶ Local data: Supplemental application data such as search indexes or application statistics that are located on a file system accessible to the application that owns the data
- ▶ Configuration information about the IBMConnections environment

### 14.6.1 Databases

Prior to installing the IBM Connections applications, you have to first create the databases for each application and the installer uses those databases to build the original environment. All databases must be hosted on the same enterprise database server and must be of the same type, either DB2, Oracle, or SQL Server.

The following databases are created for each application, we do not recommend attempting to use different database names than those suggested by the default install. The databases have self explanatory names with the exception of-:

- ▶ OPNACT - used by Activities
- ▶ SNCOMM - used by Communities



## 14.6.2 Local and shared data

When building an IBM Connections server and before starting the installation, consideration should be given to the location of the shared data. The shared data includes all file uploads across all applications and the location must be accessible to all servers. Location and capacity of the shared data store must be planned for and, ideally, leave room for data growth over time.

To find where the applications are storing their data, you can use the Integrated Solutions Console (ISC) because the location of each application's data appears as a WebSphere variable. Log into the ISC for the deployment manager and choose WebSphere variables from the menus.



There are many variables across all the applications that each have their own roles. However, you can filter the list down to those you are interested in. In the figure below, we have filtered by `*CONTENT_DIR` that shows us the defined content directories.

**WebSphere Variables**

Use this page to define substitution variables. Variables specify a level of indirection for some system-defined values, such as file system root directories. Variables have a scope level, which is either server, node, cluster, or cell. Values at one scope level can differ from values at other levels. When a variable has conflicting scope values, the more granular scope value overrides values at greater scope levels. Therefore, server variables override node variables, which override cluster variables, which override cell variables.

Scope: Cell=**con-dmgrCell01**

Preferences

New Delete

Filter: \*CONTENT\_DIR

To filter the following table, select the column by which to filter, then enter filter criteria (wildcards: \*,?,%).

Filter: Name Search terms: \*CONTENT\_DIR Go

You can administer the following resources:

| Select                   | Name                                    | Value   | Scope               |
|--------------------------|---|---|---------------------|
| <input type="checkbox"/> | <a href="#">ACTIVITIES_CONTENT_DIR</a>  | /opt/IBM/Connections/data/shared/activities/content | Cell=con-dmgrCell01 |
| <input type="checkbox"/> | <a href="#">BLOGS_CONTENT_DIR</a>       | /opt/IBM/Connections/data/shared/blogs/upload       | Cell=con-dmgrCell01 |
| <input type="checkbox"/> | <a href="#">FILES_CONTENT_DIR</a>       | /opt/IBM/Connections/data/shared/files/upload       | Cell=con-dmgrCell01 |
| <input type="checkbox"/> | <a href="#">FILES_EVENT_CONTENT_DIR</a> | \${FILES_CONTENT_DIR}                               | Cell=con-dmgrCell01 |
| <input type="checkbox"/> | <a href="#">FORUM_CONTENT_DIR</a>       | /opt/IBM/Connections/data/shared/forums/content     | Cell=con-dmgrCell01 |

There are other variables that define data locations by application and you might want to review them all (by disabling the filter) if you are looking to document all possible locations.

### 14.6.3 Configuration information

The configuration information for the Connections environment falls into three areas:

- WebSphere configuration files:

These are both held centrally by the Deployment Manager and distributed out to each of the Network Deployed nodes. The originals, held by the Deployment Manager can be found in the config directory underneath the Deployment Manager's profile, that is, */profiles/DMgr01/config*

- IBM Connections specific application configuration files:

You can find these files in the IBM Connections installation directory. This directory can be identified by reviewing the WebSphere variables in the Integrated Solutions Console, that is, */IBM/LotusConnections*

- IBM HTTP Server plugins, keystores, and configuration.

You can find these files within the "config" and "plugins" directories underneath the HTTPServer install directory, that is, */IBM/HTTPServer/*

## 14.7 Backing up and protecting data

### 14.7.1 Databases

It is critical that your IBM Connections data in its entirety is backed up and secured. Although the WebSphere Application Server servers might start and the applications appear to start, without access to the databases and data stores, the applications will not work.

The primary application data is stored on your Enterprise database server and a backup and data retention policy should be put in place to manage those databases. Although each application has its own database, in some situations, information is stored outside of the expected applications. For example, Communities data is stored across multiple applications such as Forums, Files, and Activities. For this reason, it is not often possible, certainly not with Communities, to restore a single database in order to roll back your application to a point in time.

There are tools available from IBM to restore deleted Communities, however, they are difficult to deploy and cannot restore all data.

It is critical that all IBM Connections servers are stopped before a database restore is attempted.

### 14.7.2 Local and shared data

Many customers forget to back up the local and shared data stores. The shared data stores especially which contain the file uploads from each application must be restored alongside the databases or the linked to files will not be present. The location of the shared and local data stores can be found under WebSphere variables in the Integrated Solutions Console.

### 14.7.3 Server configuration

To create a backup of the IBM Connections WebSphere server configuration, you can use the **backupconfig** program that is found in the bin directory under every WebSphere profile. However, for our purposes, we would rely on the Deployment Manager's configuration. The Deployment Manager, which manages all other servers in the cell, has the original copies of all the configuration files for every server. It will deploy these configuration files out to each of its managed servers if they are updated. For this reason, backing up the Deployment Manager configuration is what we need to concentrate on.

You can find the backupconfig file in */profiles/DMgr01/bin*

The syntax for the file can simply be **backupConfig.sh / backupconfig.bat**

However, in that form, the process will stop the Deployment Manager server completely and create a zip file in the bin directory of all the configuration files. If you do not want to have the Deployment Manager stopped in order to backup the configuration, you can use the -nostop (case sensitive) switch. You can also pass the command the name and location of the backup file that you want to create, that is

**backupConfig c:\backups\dmgr050113.zip -nostop -username -password**

This command creates a backup file called dmgr050113.zip in the backups directory of the C drive without stopping the Deployment Manager server itself.

If you do not have your server credentials stored in the soap.client.props file in the *properties* sub directory, you will be prompted for them during the backup, or you could pass the command line the -username and -password switches to avoid being prompted.

To restore the backup files, again move to the bin directory underneath the Deployment Manager profile and run the **restoreConfig** command. Once more, you can use the -nostop switch to prevent the server being stopped but since this is a restore process you do actually want the server stopped whilst the restore happens. For example

**restoreConfig -username -password**



# Performance tuning

In an IBM Connections environment, there are many moving parts, most of which are dependent on each other. Poor performance or availability of one element can lead to a poor user experience overall.

The critical elements that can affect IBM Connections functionality are

- ▶ Database server
- ▶ Databases
- ▶ IBM HTTP Server
- ▶ DNS
- ▶ LDAP
- ▶ SMTP
- ▶ WebSphere servers being able to access the shared data area on an accessible networked location

The critical elements that can affect IBM Connections performance are

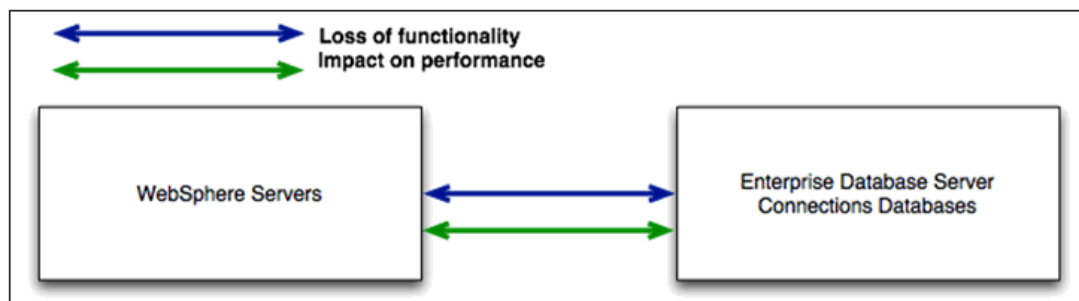
- ▶ LDAP performance
- ▶ Database server performance
- ▶ Database performance
- ▶ IBM HTTP Server performance and caching

## 15.1 Database server performance

The databases and database servers are the primary dependency for your IBM Connections environment.

The databases themselves and the database servers are responsible for serving up the data in the IBM Connections environment. Loss of database data, inaccessible databases, or poor server performance affects the whole user experience. Consider that if the databases or

database server is going to be brought off-line, this must be coordinated with downtime on the IBM Connections environment.



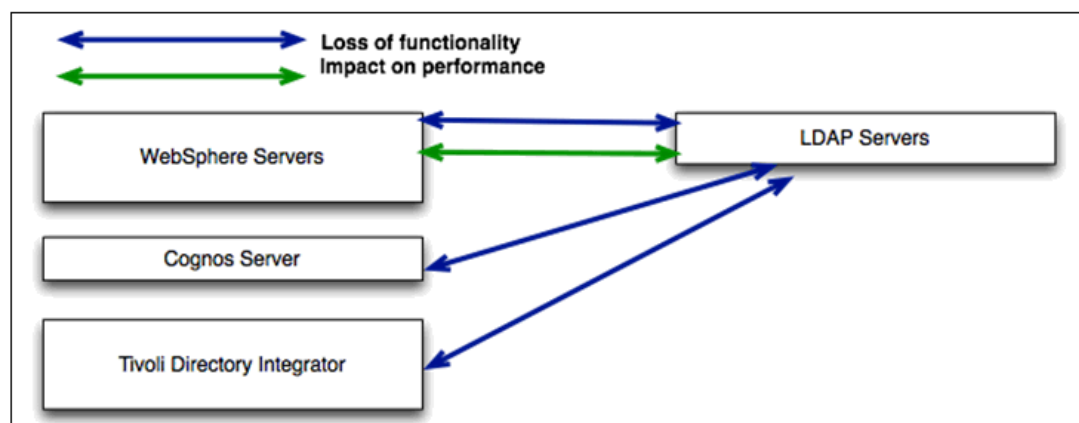
The database servers should always be deployed in a high availability configuration to lessen the risk of system downtime. DB2, SQL Server, and Oracle all have high availability options and the licensing for IBM Connections includes limited DB2 HADR options.

## 15.2 LDAP performance

The LDAP servers are responsible for authenticating users who are attempting to log into the Connections environment as well lookups throughout the applications. Poor performing LDAP servers will be reflected in a slow IBM Connections user experience. Inaccessible LDAP servers will prevent users from logging in at all.

The following IBM Connections elements are LDAP dependent:

- ▶ WebSphere servers hosting IBM Connections use LDAP to authenticate users and also throughout the system to perform lookups
- ▶ Cognos Server uses LDAP to authenticate users who are trying to access reports
- ▶ Tivoli Directory Integrator uses LDAP to synchronize user data into the Profiles application, this is either done via manually scheduled tasks or through continuously running Assemblyline



If you do not have multiple LDAP servers configured on your network to resolve to a single host name, you can use the federated repository configuration inside the Integrated Solutions Console to set up multiple failover servers in case your primary server becomes unavailable.

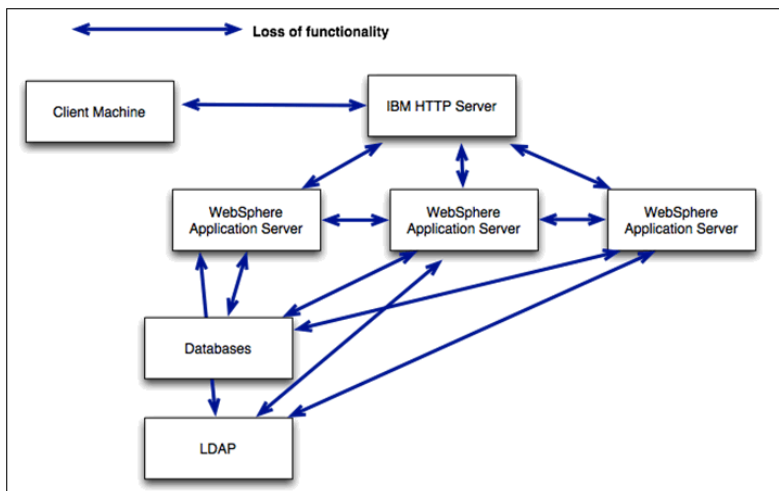
The screenshot shows the 'Global security' console window. The breadcrumb path is 'Global security > Federated repositories > ldap-dom'. Below this, it states: 'Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.' The 'General Properties' section includes a 'Repository identifier' field with the value 'ldap-dom'. The 'LDAP server' section has a 'Directory type' dropdown set to 'IBM Lotus Domino', a 'Primary host name' field with 'ldap-dom.itso.ibm.com', and a 'Port' field with '389'. A red box highlights the 'Failover server used when primary is not available:' section, which contains a 'Delete' button, a table with columns 'Select', 'Failover Host Name', and 'Port', and a 'None' entry. The 'Security' section on the right includes fields for 'Bind distinguished name' (domadmin), 'Bind password' (masked), 'Login properties' (uid), 'LDAP attribute for Kerberos principal name' (krbPrincipalName), 'Certificate mapping' (EXACT\_DN), and 'Certificate filter'.

One key thing to avoid in LDAP directories is the use of heavily nested groups for assigning membership or ownership throughout the IBM Connections environment. LDAP lookups perform particularly slowly against nested groups and that will be reflected in the user experience.

## 15.3 DNS performance

The availability and performance of dynamic name server (DNS) is critical for both the user accessing the Connections environment and the servers attempting to communicate between each other to provide services.

As you can see from the figure below, DNS availability and performance is critical to all aspects of your IBM Connections environment.



- In any WebSphere environment, all the servers must be able to communicate amongst each other and they do this using the fully qualified host names for each server that were in place when the servers were installed.



- ▶ The IBM HTTP Server uses its plugin configuration file that contains the fully qualified host names of each WebSphere Application Server server to redirect traffic to the correct one hosting the application being requested.
- ▶ The WebSphere Application Server servers will attempt to connect to the databases using the fully qualified host name that they have been given for locating the enterprise database server.
- ▶ Authentication onto the IBM Connections environment is done through LDAP and the LDAP server is found using a DNS lookup of the LDAP host name as defined in the Deployment Manager's configuration.

In any network environment, not every request is looked up every time from the DNS servers and in fact many requests , especially those on the IHS server, are cached from previous lookups. However, a poor performing or unavailable DNS will cause the Connections environment to slow down, start throwing errors, and eventually fail completely.

# Troubleshooting IBM Connections

Troubleshooting the IBM Connections product can appear to be a difficult task when considering all of the software where the problem could be caused by.

This section is designed to simplify the various tasks that you can perform to diagnose the problem or when working with IBM Software Group Support.

- ▶ 16.1, “What can be found in WebSphere Application Server logs” on page 256
- ▶ 16.2, “How to troubleshoot IBM Connections Applications” on page 258
- ▶ 16.3, “Adding additional tracing to the logs” on page 262
- ▶ 16.4, “Gathering information for support” on page 264
- ▶ 16.5, “Using the IBM SWG Support Portal to upload files to a PMR” on page 266

## 16.1 What can be found in WebSphere Application Server logs

The WebSphere Application Server logs that are pertinent to IBM Connections are the following:

- ▶ *startServer.log*: This log file contains messages generated by the WebSphere Application Server from start-up to when the Server is open for e-business.
- ▶ *SystemOut.log*: This log file contains messages generated by the WebSphere Application Server from start-up, throughout run-time, and then to completion of shut-down.
- ▶ *Trace.log*: This log file contains messages generated by the trace-options enabled at Configuration and/or Runtime, in-addition to the messages found in the SystemOut.log.

The messages in the WebSphere Application Server logs has the following syntax format:

**<Application prefix><Error code><Message level code>**

All application prefixes used by the IBM Connections Applications (except for Files & Wikis) start with CLFxxxxxxx, for example, CLFRA0001E.

The Application prefixes and message level codes are defined in the product documentation at:

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=IBM\\_Connections\\_log\\_file\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=IBM_Connections_log_file_ic40&content=pdcontent))

by go to **Product Documentation** → **IBM Connections 4.0 documentation** → **Troubleshooting and support** → **Troubleshooting checklist** → **Troubleshooting tips** → **IBM Connections log file.**

The description of common error codes generated by the IBM Connections Applications that contained in the WebSphere Application Server logs are also defined in the product documentation at:

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Error\\_codes\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Error_codes_ic40&content=pdcontent)

by go to **Product Documentation** → **IBM Connections 4.0 documentation** → **Troubleshooting and support** → **Troubleshooting checklist** → **Troubleshooting tips** → **Error codes.**

The following table shows the default WebSphere Application Server log file locations:

| Server type                 | Operating system  | Path  |
|-----------------------------|-------------------|---|
| Deployment Manager (Dmgr01) | Microsoft Windows | C:\IBM\WebSphere\AppServer\profiles\Dmgr01\logs\dmgr  |
| Application Server          | Microsoft Windows | C:\IBM\WebSphere\AppServer\profiles\logs\             |
| Node Agent                  | Microsoft Windows | C:\IBM\WebSphere\AppServer\profiles\logs\nodeagent\   |
|                             |                   |   |
| Deployment Manager (Dmgr01) | AIX               | /usr/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/    |
| Application Server          | AIX               | /usr/IBM/WebSphere/AppServer/profiles/logs/           |
| Node Agent                  | AIX               | /usr/IBM/WebSphere/AppServer/profiles/logs/nodeagent/ |
|                             |                   |   |
| Deployment Manager (Dmgr01) | Linux             | /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/logs/    |
| Application Server          | Linux             | /opt/IBM/WebSphere/AppServer/profiles/logs/           |
| Node Agent                  | Linux             | /opt/IBM/WebSphere/AppServer/profiles/logs/nodeagent/ |

Each log file contains a header of information about the WebSphere Application Server that generated it. See the following example.

---

```

***** Start Display Current Environment *****
WebSphere Platform 7.0.0.21 [ND 7.0.0.21 cf211150.04] running with process name
<cell_name>\<node_name>\<server_name> and process id xxxx (where xxxx are numerical digits)

```

```

Host Operating System is <operating_system_name>, version
<version_of_operating_system>
Java version = <version of java>, Java Compiler = j9jit24, Java VM name = IBM J9 VM
was.install.root = <path_to_was_root_program_directory>
user.install.root = <path_to_was_server_program_directory_root>
Java Home = <path_to_jre_in_was_root_program_directory>
ws.ext.dirs =
/opt/ibm/WebSphere/AppServer/java/lib:/opt/ibm/WebSphere/AppServer/profiles/AppSrv01/clas
sses:/opt/ibm/WebSphere/AppServer/classes:/opt/ibm/WebSphere/AppServer/lib:/opt/ibm/WebS
phere/AppServer/installedChannels:/opt/ibm/WebSphere/AppServer/lib/ext
:/opt/ibm/WebSphere/AppServer/web/help:/opt/ibm/WebSphere/AppServer/deploytool/itp/plugi
ns/com.ibm.etools.ejbdeploy/runtimeClasspath =
/opt/ibm/WebSphere/AppServer/profiles/AppSrv01/properties:/opt/ibm/WebSphere/AppServ
er/properties:/opt/ibm/WebSphere/AppServer/lib/startup.jar:/opt/ibm/WebSphere/AppSer
ver/lib/bootstrap.jar:/opt/ibm/WebSphere/AppServer/lib/jsf-nls.jar:/opt/ibm/WebSpher
e/AppServer/lib/lmproxy.jar:/opt/ibm/WebSphere/AppServer/lib/urlprotocols.jar:/opt/i
bm/WebSphere/AppServer/deploytool/itp/batchboot.jar:/opt/ibm/WebSphere/AppServer/dep
loytool/itp/batch2.jar:/opt/ibm/WebSphere/AppServer/java/lib/tools.jar
Java Library path =
/opt/ibm/WebSphere/AppServer/java/jre/lib/s390x/compressedrefs:/opt/ibm/WebSphere/Ap
pServer/java/jre/lib/s390x:/opt/ibm/WebSphere/AppServer/bin:/opt/ibm/Connections/dat
a/shared/search/stellent/dcs/olexport:/usr/lib
***** End Display Current Environment *****

```

---

A message whose application prefix, error code, and message level code that can indicates an IBM Connections Application is starting is the WSVR0200I message. For example:

---

```

[09/21/12 9:14:19:397 EST] 0000001d ApplicationMg A   WSVR0200I: Starting
application: Profiles

```

---

A message whose application prefix, error code, and message level code that can indicates an IBM Connections Application has started is the WSVR0221I message. For example:

---

```

[09/21/12 9:14:39:427 EST] 0000001d ApplicationMg A   WSVR0221I: Application
started: Profiles

```

---

## 16.2 How to troubleshoot IBM Connections Applications

IBM Connections Applications problem can arise or be caused by any point in the stack of software in which comprise its topology:

- ▶ Client (for example, Web-browser)
- ▶ Proxy-server or load-balancer
- ▶ IBM HTTP Server
- ▶ WebSphere Application Server, Deployment Manager, Application Server, or Node Agent
- ▶ Database server
- ▶ Tivoli Directory Integrator Server
- ▶ LDAP Server
- ▶ Network file system or local file system

You can use the following troubleshooting steps to narrow the scope of the problem and identify its cause:

1. Check if the client and server environment are supported.

Most common problems are caused by the version or brand of software not-being supported. It is always an idea to review the IBM Connections system requirements documents to rule out incompatibility as the cause. For the IBM Connections system requirements, see Detailed System Requirements for IBM Connections at <http://www-01.ibm.com/support/docview.wss?rs=899&uid=swg27012786>.

2. Record the time and date at which the problem was encountered.

This is critical to identifying the problem because the information can be used to correlate data between software within the IBM Connections topology.

3. Determine whether any error messages are being reported when the problem occurs.

The first place to check is on the device that encountered the problem. For example, if a problem with an IBM Connections Application was encountered with a web browser, look for error messages reported either by the web browser itself or the Java console of the browser. Sometimes the error reported by the device indicates a problem with the device's configuration, such as not accepting cookies or an untrusted security certificate.

4. Review WebSphere Application Server log files.

After you have determined whether the device which encountered the problem reported an error, then review the SystemOut.log file(s) generated by the WebSphere Application Server which hosts the IBM Connections Application that you encountered a problem with. Use the date and time of the error you recorded in step 2 to narrow the scope of data to analyze and correlate with the problem encountered. Typically, when an error occurs within an IBM Connections Application, it is reported with a backtrace of J2EE class function calls that can help determine what Application reported the exception and perhaps even what part of it.

For example, let us briefly examine the following exception generated by an IBM Connections Application. We numbered the line for explanation purpose.

---

```
1.[1/18/13 6:54:46:178 CST] 00000096 SeedlistValid W
com.ibm.lotus.connections.search.admin.seedlist.SeedlistValidation validateSeedlist CLFRW0263I: Seedlist
validation failed. Refer to the log for details.
2.com.ibm.lotus.connections.search.registries.exceptions.CrawlerUnavailableException: CLFRW0313E: Attempt by
crawler registry to retrieve an unconfigured search service files, wikis. Check your LotusConnections-config.xml
file.
3.atcom.ibm.lotus.connections.search.registries.impl.CrawlerRegistryImpl.getCrawler(CrawlerRegistryImpl.java:152)
4.atcom.ibm.lotus.connections.search.admin.seedlist.SeedlistValidation.validateSeedlist(SeedlistValidation.java:5
1)
5.atcom.ibm.lotus.connections.search.service.admin.mbean.SearchService.validateSeedlist(SearchService.java:1144)
6.atsun.reflect.NativeMethodAccessorImpl.invoke0(Native Method)
7.atsun.reflect.NativeMethodAccessorImpl.invoke(NativeMethodAccessorImpl.java:60)
8.atsun.reflect.DelegatingMethodAccessorImpl.invoke(DelegatingMethodAccessorImpl.java:37)
9.atjava.lang.reflect.Method.invoke(Method.java:611)
10.atcom.sun.jmx.mbeanserver.StandardMBeanIntrospector.invokeM2(StandardMBeanIntrospector.java:105)
11.atcom.sun.jmx.mbeanserver.StandardMBeanIntrospector.invokeM2(StandardMBeanIntrospector.java:39)
12.atcom.sun.jmx.mbeanserver.MBeanIntrospector.invokeM(MBeanIntrospector.java:220)
13.atcom.sun.jmx.mbeanserver.PerInterface.invoke(PerInterface.java:132)
14.atcom.sun.jmx.mbeanserver.MBeanSupport.invoke(MBeanSupport.java:274)
15.atcom.sun.jmx.interceptor.DefaultMBeanServerInterceptor.invoke(DefaultMBeanServerInterceptor.java:848)
16.atcom.sun.jmx.mbeanserver.JmxMBeanServer.invoke(JmxMBeanServer.java:773)
17.atcom.ibm.ws.management.AdminServiceImpl$1.run(AdminServiceImpl.java:1331)
18.atcom.ibm.ws.security.util.AccessController.doPrivileged(AccessController.java:118)
19.atcom.ibm.ws.management.AdminServiceImpl.invoke(AdminServiceImpl.java:1224)
20.atcom.ibm.ws.management.connector.AdminServiceDelegator.invoke(AdminServiceDelegator.java:181)
21.atcom.ibm.ws.management.connector.ipc.CallRouter.route(CallRouter.java:242)
22.atcom.ibm.ws.management.connector.ipc.IPCConnectorInboundLink.doWork(IPCConnectorInboundLink.java:353)
23.atcom.ibm.ws.management.connector.ipc.IPCConnectorInboundLink$IPCConnectorReadCallback.complete(IPCConnectorIn
boundLink.java:595)
24.atcom.ibm.ws.ssl.channel.impl.SSLReadServiceContext$SSLReadCompletedCallback.complete(SSLReadServiceContext.ja
va:1784)
25.atcom.ibm.ws.tcp.channel.impl.AioReadCompletionListener.futureCompleted(AioReadCompletionListener.java:165)
26.atcom.ibm.io.async.AbstractAsyncFuture.invokeCallback(AbstractAsyncFuture.java:217)
27.atcom.ibm.io.async.AsyncChannelFuture.fireCompletionActions(AsyncChannelFuture.java:161)
28.atcom.ibm.io.async.AsyncFuture.completed(AsyncFuture.java:138)
29.atcom.ibm.io.async.ResultHandler.complete(ResultHandler.java:204)
30.atcom.ibm.io.async.ResultHandler.runEventProcessingLoop(ResultHandler.java:775)
31.atcom.ibm.io.async.ResultHandler$2.run(ResultHandler.java:905)
32.atcom.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1604)
```

---

Line1: Contains the Application prefix of an exception reported by the IBM Connections Search Application and its description.

Line 2: Contains another class-function call that reported an exception which caused the Seedlist validation to fail reported in Line 1. It also provides a suggestion to resolve the problem. Although it does not point out the exact problem, the details collected thus far can be a rather powerful suggestion. For example, the search services defined in the LotusConnections-config.xml file of the WebSphere Application Server that generated this exception appears to contain a syntax-related problem with this string of characters: files, wikis

Line 3: Contains the class-function call that led to the exception generated in Line 2 which caused the exception generated in Line 1.

Here is an exception example that is related to an IBM Connections Application, but was not generated by an IBM Connections Application.

---

```
1.09/15/12 16:17:28:290 EST] 00000095 IndexReplicat W Places index replication failed
2.com.ibm.lotus.search.replication.ReplicationException: java.io.FileNotFoundException:
/opt/ibm/Connections/data/local/catalog/index/Places/tmpDeltaIndex/taxonomyIndex/_0.fnm (No such file or
directory)
3.at com.ibm.lotus.search.replication.IndexUpdater.addIndex(IndexUpdater.java:238)
4.atcom.ibm.lotus.search.replication.IndexUpdater.updateIndex(IndexUpdater.java:142)
5.atcom.ibm.lotus.search.engine.IndexReplicationService.replicate(IndexReplicationService.java:93)
6.atcom.ibm.lotus.search.engine.messaging.CollectionCommittedMessage.handle(CollectionCommittedMessage.java:54)
7.atcom.ibm.lotus.search.engine.messaging.AdminTopicMessageDrivenBean.onMessage(AdminTopicMessageDrivenBean.java:
70)
8.atcom.ibm.ejs.container.MessageEndpointHandler.invokeMdbMethod(MessageEndpointHandler.java:1093)
9.atcom.ibm.ejs.container.MessageEndpointHandler.invoke(MessageEndpointHandler.java:778)
10.at $Proxy134.onMessage(Unknown Source)
11.atcom.ibm.ws.sib.api.jmsra.impl.JmsJcaEndpointInvokerImpl.invokeEndpoint(JmsJcaEndpointInvokerImpl.java:192)
12.atcom.ibm.ws.sib.ra.inbound.impl.SibRaDispatcher.dispatch(SibRaDispatcher.java:900)
13.atcom.ibm.ws.sib.ra.inbound.impl.SibRaSingleProcessListener$SibRaWork.run(SibRaSingleProcessListener.java:552)
14.at com.ibm.ejs.j2c.work.WorkProxy.run(WorkProxy.java:399)
15.at com.ibm.ws.util.ThreadPool$Worker.run(ThreadPool.java:1604)
16.Caused by: java.io.FileNotFoundException:
/opt/IBM/Connections/data/local/catalog/index/Places/tmpDeltaIndex/taxonomyIndex/_0.fnm (No such file or
directory)
17.at java.io.RandomAccessFile.open(Native Method)
18.at java.io.RandomAccessFile.<init>(RandomAccessFile.java:229)
19.atorg.apache.lucene.store.SimpleFSDirectory$SimpleFSIndexInput$Descriptor.<init>(SimpleFSDirectory.java:69)
20.atorg.apache.lucene.store.SimpleFSDirectory$SimpleFSIndexInput.<init>(SimpleFSDirectory.java:90)
21.atorg.apache.lucene.store.NIOFSDirectory$NIOFSIndexInput.<init>(NIOFSDirectory.java:91)
22.at org.apache.lucene.store.NIOFSDirectory.openInput(NIOFSDirectory.java:78)
23.at org.apache.lucene.store.FSDirectory.openInput(FSDirectory.java:353)
24.at org.apache.lucene.index.FieldInfos.<init>(FieldInfos.java:68)
25.atorg.apache.lucene.index.SegmentReader$CoreReaders.<init>(SegmentReader.java:118)
26.at org.apache.lucene.index.SegmentReader.get(SegmentReader.java:578)
27.at org.apache.lucene.index.SegmentReader.get(SegmentReader.java:556)
28.at org.apache.lucene.index.DirectoryReader.<init>(DirectoryReader.java:113)
29.atorg.apache.lucene.index.ReadOnlyDirectoryReader.<init>(ReadOnlyDirectoryReader.java:29)
30.at org.apache.lucene.index.DirectoryReader$1.doBody(DirectoryReader.java:81)
31.atorg.apache.lucene.index.SegmentInfos$FindSegmentsFile.run(SegmentInfos.java:736)
32.at org.apache.lucene.index.DirectoryReader.open(DirectoryReader.java:75)
33.at org.apache.lucene.index.IndexReader.open(IndexReader.java:428)
34.at org.apache.lucene.index.IndexReader.open(IndexReader.java:274)
35.atcom.ibm.ilel.facet.taxonomy.lucene.LuceneTaxonomyWriter.addTaxonomies(LuceneTaxonomyWriter.java:749)
36.atcom.ibm.lotus.search.replication.IndexUpdater.addIndex(IndexUpdater.java:202)
```

---

Line 1: This only lists the date/time, the number of the thread which generated it, the name of the service, the Message-level code, and then a description of the Exception.

Line 2: This lists the class-function call which reported the exception and a brief description of the issue. Again, although it-is brief, it does offer a powerful amount of information that can be used to further investigate the cause of the problem.

Line 3: This lists the class-function call which led to the exception reported in Line 2.

#### 5. Review Troubleshooting tips document.

After you have identified whether any exceptions or error codes are being reported in the SystemOut.log of the WebSphere Application hosting the IBM Connections Application where the problem occurred within, the next step is to review the issues listed in the

Troubleshooting tips section of the Product Documentation to see if the problem you are having is addressed at:

Product Documentation > IBM Connections 4.0 documentation > Troubleshooting and support > Troubleshooting checklist > Troubleshooting tips

[http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res\\_title=Troubleshooting\\_tips\\_ic40&content=pdcontent](http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Troubleshooting_tips_ic40&content=pdcontent)

6. Check if you have the latest product fixes installed.

Fixes for IBM Connections are packaged in several different ways. The difference between the packages are the number of fixes included and the amount of testing which the fixes underwent before making publically available:

► Fix Packs:

Fix Packs contain a substantial amount of fixes for problems that were frequently reported or identified to have a high-impact. These also contain the most amount of fixes in a single package. Although they undergo a significant amount of testing, these are not released as often as Component Refreshes. And sometimes new features are also featured in Fix Packs, though not often.

► Component Refreshes:

Component Refreshes (CRs) also contain multiple fixes for problems that were frequently reported or identified to have a high-impact. Although they do not usually contain as many fixes as a Fix Pack, they do however undergo a significant amount of testing. These are released much more frequently than a Fix Pack.

► iFixes

An iFix is a single fix associated with an IBM Authorized Problem Analysis Report (APAR). These are delivered to address a specific problem, as opposed to CRs & FPs which are to address a variety of problems.

**Note:** For Information about obtaining fixes for the IBM Connections product, see Fix lists for IBM® Connections

<http://www-01.ibm.com/support/docview.wss?uid=swg27019738>

7. Search IBM Knowledge Bases for a related problem report

If you have the latest product fixes installed, then proceed to search the IBM Knowledge Bases for a related problem report at IBM Connections 4.0 Known Issues

<http://www-01.ibm.com/support/search.wss?rs=3265&tc=SSYGQH&atr=SWVersion&atr=4.0>.

8. Report problem to IBM Support.

If you are not able to locate a report of the same or similar problem, begin to collect diagnostic data to send to IBM Support. The data required by IBM Software Group to begin troubleshooting your issue can be identified within one of the following MustGather TechNotes for each IBM Connections Application.

**Note:** The new MustGathers are published often, so be sure to utilize your favorite search-engine if you are not able to locate one for the IBM Connections Application you are having a problem with in this list:Collecting Data:

- ▶ IBM Connections 4.0 Activities  
<http://www.ibm.com/support/docview.wss?uid=swg21608844>
- ▶ Collecting Data: IBM Connections 4.0 Blogs  
<http://www.ibm.com/support/docview.wss?uid=swg21608485>
- ▶ Collecting Data: IBM Connections Bookmarks 4.0  
<http://www.ibm.com/support/docview.wss?uid=swg21609614>
- ▶ Collecting data: IBM Connections 4.0 Cognos and Metrics  
<http://www.ibm.com/support/docview.wss?uid=swg21610705>
- ▶ Collecting Data: IBM Connections 4.0 Communities  
<http://www.ibm.com/support/docview.wss?uid=swg21610336>
- ▶ Collecting Data: IBM Connections 4.0 Forums  
<http://www.ibm.com/support/docview.wss?uid=swg21609775>
- ▶ Collecting data: IBM Connections 4.0 Cognos and Metrics  
<http://www.ibm.com/support/docview.wss?uid=swg21610705>
- ▶ Collecting Data: IBM Connections 4.0 Mail 1.0  
<http://www.ibm.com/support/docview.wss?uid=swg21614358>
- ▶ Collecting Data: IBM Connections 4.0 Installation and Migration  
<http://www.ibm.com/support/docview.wss?uid=swg21609917>
- ▶ Collecting Data: IBM Connections 4.0 Profiles  
<http://www.ibm.com/support/docview.wss?uid=swg21610506>

#### 9. Contact IBM Software Group

Contact IBM Software Group either through 1-800-IBM-SERV or an Electronic Service Request (ESR) through the IBM Support Portal to report the problem at:

IBM Software Group - Service requests & PMRs

<http://www.ibm.com/support/electronic/uprtransition.wss?category=2>.

If you choose to open the PMR using telephone, you can submit the data for analysis once you are issued a PMR number. And there are several ways of submitting data to IBM (FTP, Email, or Web-browser) that are described in this TechNote at:

Using ECuRep to exchange information with IBM Technical Support for Lotus software

<http://www.ibm.com/support/docview.wss?uid=swg21138787>

## 16.3 Adding additional tracing to the logs

Sometimes you must enable tracing options within the WebSphere Application Server hosting the IBM Connections Applications at where you are having a problem with. Enabling trace might occur when you are following the instructions within one of the MustGather TechNotes or requested by a Problem Management Record (PMR) that you opened with IBM Software Group Support to report a problem.

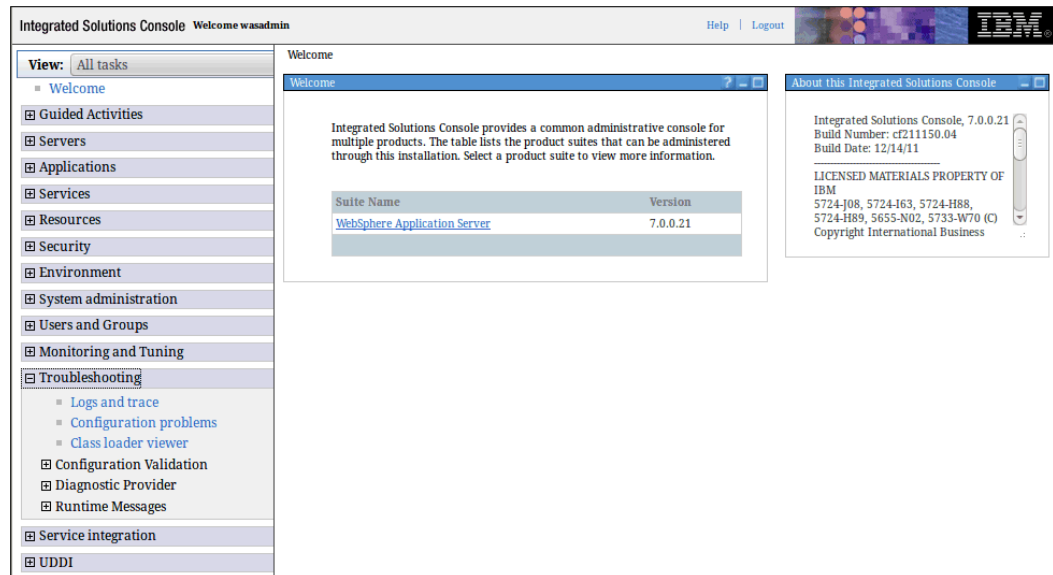
To enable the tracing options, use this procedure:

1. Open a web browser.
2. Navigate to the following URL.



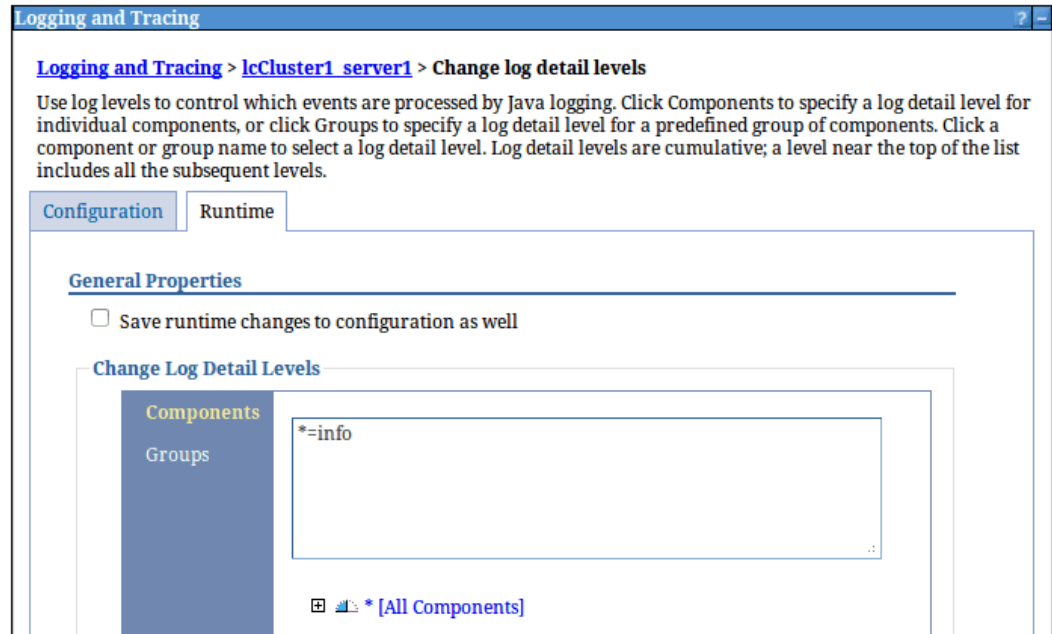
**Note:** Your environment might have been configured use a port other than the default listed below: <https://:9043/ibm/console/logon.jsp>

3. Enter the user name and password of the WebSphere Application Server Administrator. Click **Submit**.
4. One the Welcome page of the WebSphere Integrated Solutions Console (ISC), the left is a navigation pane whose contents displays on the right:



5. Go to **Troubleshooting** → **Logs and trace** and select the server on which you want to enable the trace options.
6. Go to **Change log detail levels**.

If the problem you are having occurs when the WebSphere Application Server itself was starting up, click the **Configuration tab**, otherwise, click the **Runtime tab**.



7. Copy and paste the trace options specified in the MustGather TechNote or by IBM SWG Support, click **Apply** and then **OK**.
8. If you pasted trace-options into the Configuration tab, you must then restart the WebSphere Application Server on which the trace options were enabled. The runtime trace options take effect immediately.
9. After you complete generating the data with the trace options, revisit the Change log detail levels page for the same WebSphere Application Server and change them back to the default of “\*=info”.

## 16.4 Gathering information for support

IBM Software Group Support maintains and creates new MustGather TechNotes for the IBM Connections product which detail what information and data is needed for a given problem with a specific IBM Connections Application to troubleshoot it with.

**Note:** For information and data that you must gather for IBM SWG Support for a given problem, see

- ▶ 16.1, “What can be found in WebSphere Application Server logs” on page 256
- ▶ 16.2, “How to troubleshoot IBM Connections Applications” on page 258

In addition, collecting a trace with the Fiddler2 client can also provide valuable information to expedite the process of troubleshooting with a problem that occurs within a web browser. You can download Fiddler 2 client from this URL:

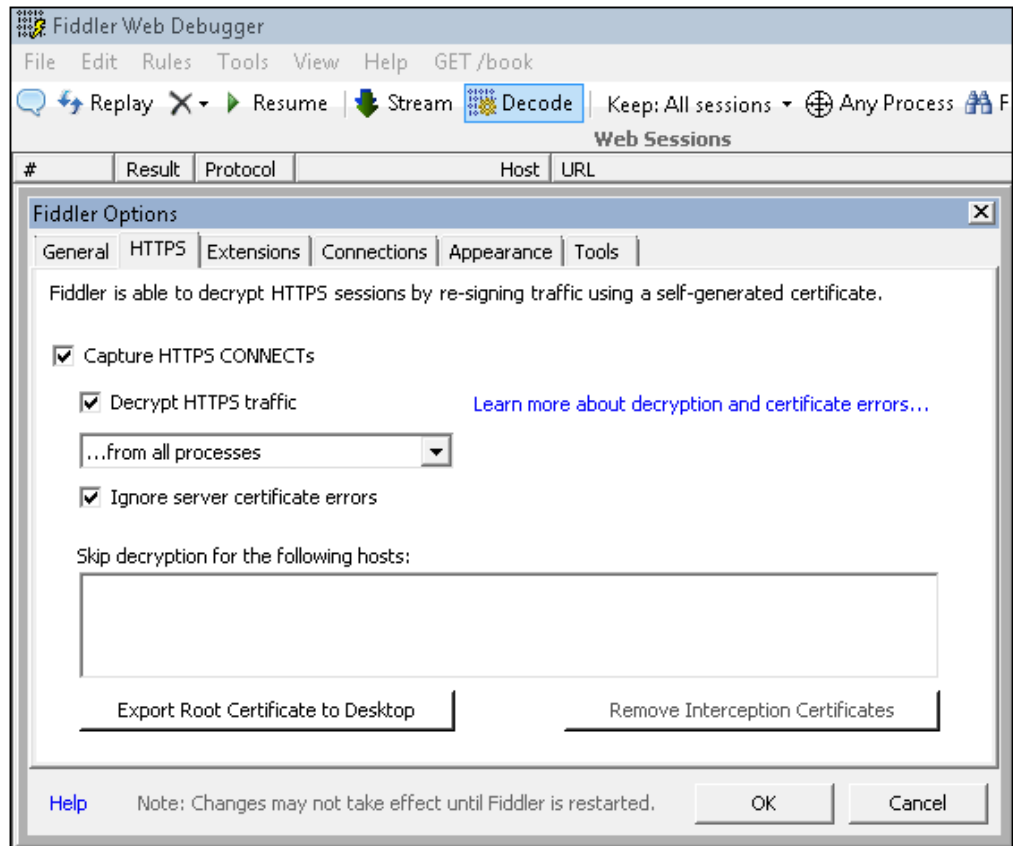
<http://www.fiddler2.com/fiddler2/version.asp>

After downloaded and installed the Fiddler client, you must then configure it to decrypt HTTPS traffic that most of the traffic between a device and IBM Connections Applications use. To configure the decryption of HTTPS traffic within the Fiddler-client, follow this procedure:

1. Open the Fiddler client.
2. Go to **Tools menu** → **Options**.

Select the following options:

- **Capture HTTPS CONNECTs**
- **Decrypt HTTPS traffic** and **...from all processes**
- **Ignore server certificate errors**



3. You might be prompted to install a security certificate from the Fiddler client. This is required to decrypt HTTPS traffic sent and received by your web browser.
4. Close and restart the Fiddler client for the changes to take effect.
5. Now you are ready to capture a Fiddler trace while reproducing a problem with a web browser and an IBM Connections problem.

When instructed either by a MustGather TechNote or IBM SWG Support to collect and submit a Fiddler trace of the reported problem, use this procedure:

1. Close all programs that contain an HTTP client on your Workstation.
2. Open a single web browser with a single tab.
3. Open the Fiddler client.
4. Press **F12** on your keyboard to begin capturing HTTP/HTTPS traffic with the Fiddler client.
5. Reproduce the problem you are having.
6. After you have reproduced the problem, switch back to the Fiddler client and press **F12** again to stop capturing traffic.

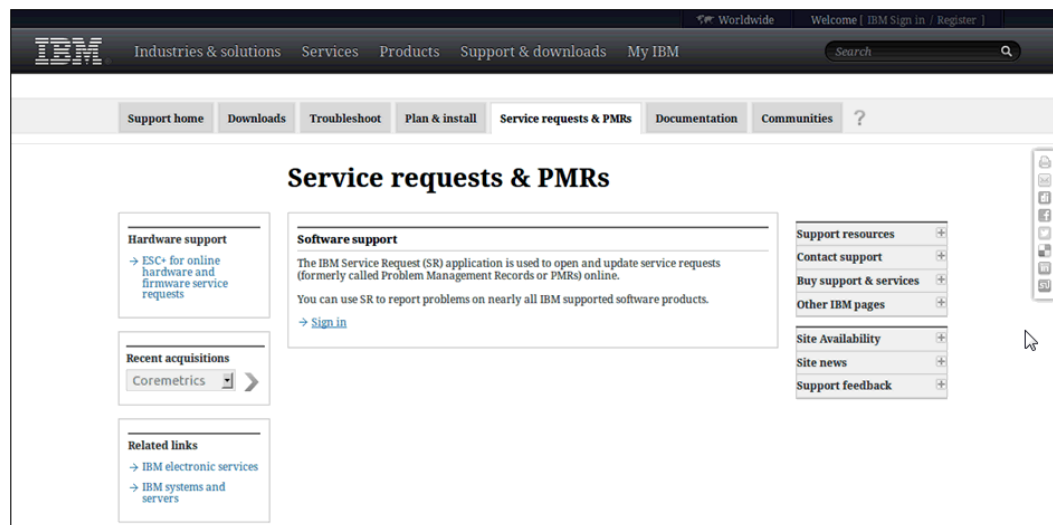
7. Go to **File menu** → **Save** → **All sessions**. A pop-up window appears.
8. Select where to save the Fiddler trace file and give it a file name which is prefixed with your PMR number.
9. Submit a copy of that file to IBM SWG Support for analysis.

## 16.5 Using the IBM SWG Support Portal to upload files to a PMR

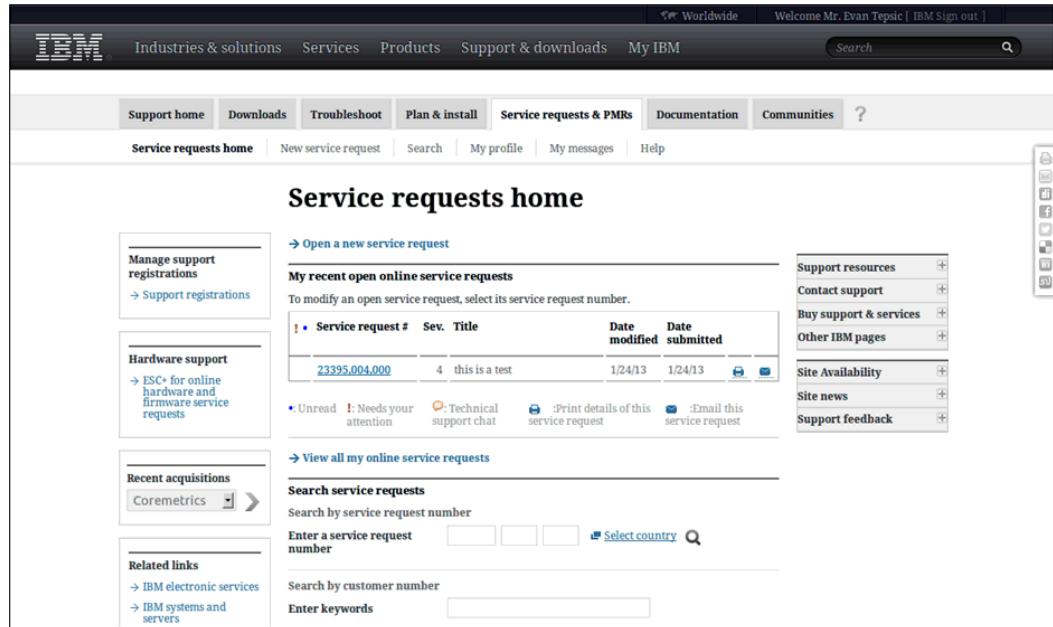
To use the IBM SWG Support Portal to upload files to a PMR, use the following procedure:

1. Open a web browser.
2. Navigate to this URL: <https://www-947.ibm.com/support/servicerequest/Home.action>

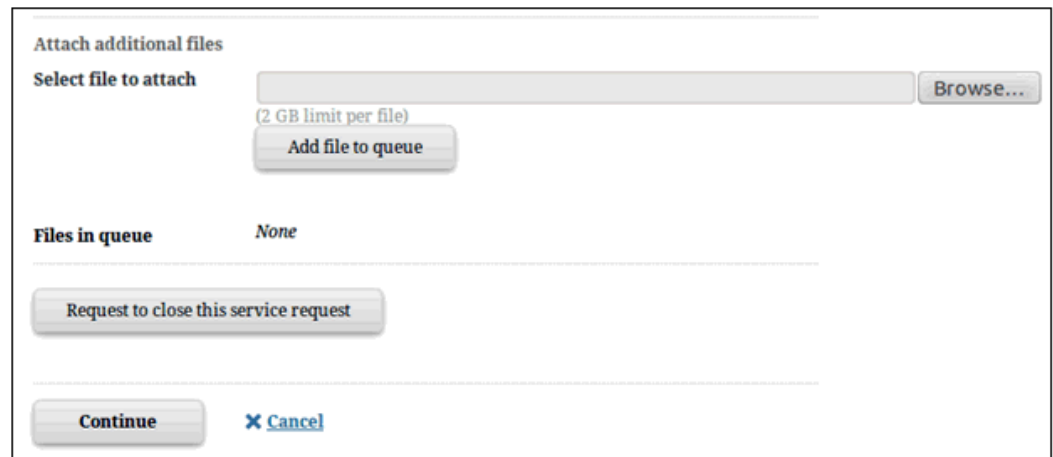
The following page is displayed:



3. Sign in with your IBM Account user name and password.
4. After submitting your credentials, you are navigated to a page that lists any Open PMRs you have under the Customer ID associated with your IBM Account.



5. Click the PMR number to which you want to upload files.
6. Use the Attach additional files section on the bottom of the page to upload your files.



7. A pop-up window containing a summary of the information and data you want to send IBM appears. You also have the option to specify how you want to be contacted. Click **Submit**.
8. After files upload completes, a page stating whether the update was successful will appear. Unless an error occurred, this is the last step in the process.

# IBM Greenhouse

IBM launched the IBM Greenhouse

(<https://greenhouse.lotus.com/wpsgh/wcm/connect/ghcontent/lotus+greenhouse+next+site/home/lgh+next+homepage+>) to show off and allow users to try at no charge IBM Collaboration Solutions software without the requirement of deploying it in their own environments. Included in the IBM Greenhouse are the following software products:

- ▶ IBM Connections
- ▶ IBM Sametime
- ▶ IBM Mashup Center
- ▶ IBM Websphere Portal
- ▶ IBM Quickr for Domino
- ▶ IBM Quickr for Websphere Portal
- ▶ IBM Forms Builder Experience
- ▶ IBM Symphony
- ▶ IBM Notes Traveler
- ▶ IBM iNotes Social Edition
- ▶ IBM Lotus Designer
- ▶ IBM Docs

IBM encourages everyone to create a public

account([https://greenhouse.lotus.com/gh\\_next/lotusgreenhouserequests.nsf/MainDocumentSelf?openForm](https://greenhouse.lotus.com/gh_next/lotusgreenhouserequests.nsf/MainDocumentSelf?openForm)) that then also grants you access to the IBM Collaboration Software Solutions Catalog. The catalog is a collection of free and downloadable widgets, plugins, and more for your own environment. All of the catalog is searchable.

Also found inside IBM Greenhouse is the IBM Greenhouse Labs

(<https://greenhouse.lotus.com/wpsgh/wcm/connect/ghcontent/lotus+greenhouse+next+site/home/labs/lgh+next+labs?pageDesign=ghdesign/LGH+Next+PT+Labs+-+GH+Anon>). The labs allowing trying out alpha code to help build future product directions. Many of these are simply ideas while some become integrated or their own products in the future. IBM Symphony through the web is an example because it was known as Concord during IBM Greenhouse Labs testing. These products are added and evolve consistently so visit the IBM Greenhouse Labs site

(<https://greenhouse.lotus.com/wpsgh/wcm/connect/ghcontent/lotus+greenhouse+next+site/home/labs/lgh+next+labs?pageDesign=ghdesign/LGH+Next+PT+Labs+-+GH+Anon>)

[te/home/labs/lgh+next+labs?pageDesign=ghdesign/LGH+Next+PT+Labs+-+GH+Anon](http://te/home/labs/lgh+next+labs?pageDesign=ghdesign/LGH+Next+PT+Labs+-+GH+Anon))for current projects.

## A.1 The IBM Greenhouse Collaborations Solutions Catalog

The IBM Collaboration Solutions and WebSphere Portal Business Solutions Catalog on IBM Greenhouse is a rich, web 2.0 style catalog designed to dynamically deliver widgets, plug-ins, portlets, and sample applications across the entire IBM Collaboration Solutions and WebSphere Portal software portfolio. The catalog contains a robust array of IBM, Business Partner, and individually created solutions. Whether you are looking for an industry solution for your enterprise or something to customize your end-user experience, you can find it in this catalog.

IBM Business Partners, individuals, and IBM employees can all submit solutions to be included in the catalog. With over 1600 solutions and 10,000 downloads at the time of writing, the catalog is a no-charge resource sortable by solution area, product, or industry. You can also search across industry, product, solutions tags and titles to find a listing.

### What can I find in the catalog?

Containing an initial 30 widgets designed to customize and enhance your IBM Notes experience, the catalog evolves quickly to include value-add and business solutions that span the entire IBM Collaboration Solutions and WebSphere Portal portfolio. Check back often to find new widgets, plug-ins, portlets, sample applications, and more.

### What browsers are compatible

The catalog is tested for compatibility with Firefox 2.x, Firefox 3.x, Internet Explorer 6.x, Internet Explorer 7.x, Internet Explorer 8.x, and IBM Notes embedded browsers (IE6, IE7 & IE8).

### Enabling the "My Widgets" sidebar panel in IBM Notes 8.x

By default, IBM Notes 8.x users do not see the My Widgets sidebar panel. To display this panel, select **File** → **Preferences** → **Widgets** and enable the "Show Widget Toolbar and the My Widgets Sidebar panel" option. This brief video (<https://greenhouse.lotus.com/plugins/plugincatalog.nsf/about.xsp#>) demonstrates how to enable this functionality.

### Video to demonstrate "drag & drop" installation

To install widgets that are listed in the catalog, after accepting the license agreement, you can drag the install icon to the "My widgets" sidebar panel in IBM Notes. This brief video (<https://greenhouse.lotus.com/plugins/plugincatalog.nsf/about.xsp#>) demonstrates drag & drop widget installation.

## A.2 Searching the IBM Greenhouse Collaboration Solutions Catalog

The IBM Greenhouse Collaborations Solutions Catalog in IBM Greenhouse allows searching by solution area, product, industry, text and tags. The date last updated, community rating and number of downloads is shown next to each solution. You can also click any catalog solution provider name and show only solutions uploaded by that account.

The following figure shows a sample image of the search area the IBM Greenhouse Collaborations Solution Catalog.

The screenshot displays the search interface of the IBM Greenhouse Collaborations Solution Catalog. It is divided into two main sections: 'Filter Results' and 'Tags'.

**Filter Results:** This section contains four dropdown menus for filtering: 'Solution Area' (set to 'All Solution Areas'), 'Product' (set to 'All Products'), and 'Industry' (set to 'All Industries'). Below these is a 'Search Text' input field with a magnifying glass icon and a 'reset' link.

**Tags:** This section features a search input field with a magnifying glass icon. Below the input is a horizontal slider bar. A list of tags is displayed, including 'lotus connections', 'domino portal notes', 'quickr widget sametime', 'Lotus\_Notes wcm plugin', 'CRM profiles email', 'communities integration', 'plug-in websphere\_portal', 'Xpages productivity portlet', 'administration', 'knowledge\_management', and 'sharepoint lotus\_domino'. At the bottom of the tags section are links for 'View as cloud', 'list', and 'all'.

► ***Solution Area:***

There are over 20 solution areas available to search against from B2B Integration to Unified Communications.

► ***Product:***

The products search covers many of the products found in the IBM Greenhouse. While not every product has had a solution entered into the catalog, make sure to search the entire catalog for results to make sure you find them by tag or text in case they were not categorized appropriately.

► ***Industry:***

From banking to telecommunications, the searches allow you to sort industry specific solutions from the catalog.

► ***Text:***

You can enter any text into this box to help you narrow your results. Boolean type searching (such as using a minus sign to discard results) is not allowed.

► ***Tags:***

Each entry in the Solutions Catalog is tagged to help you do a simple search or use the provided slider to narrow the results.

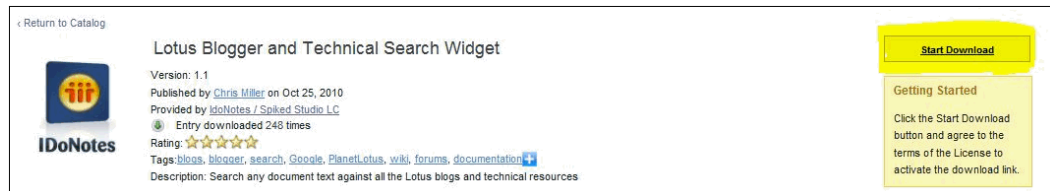


## A.3 Downloading from the IBM Greenhouse Collaboration Solutions Catalog

The IBM Greenhouse Collaboration Solutions Catalog allows you to directly download code after searching.

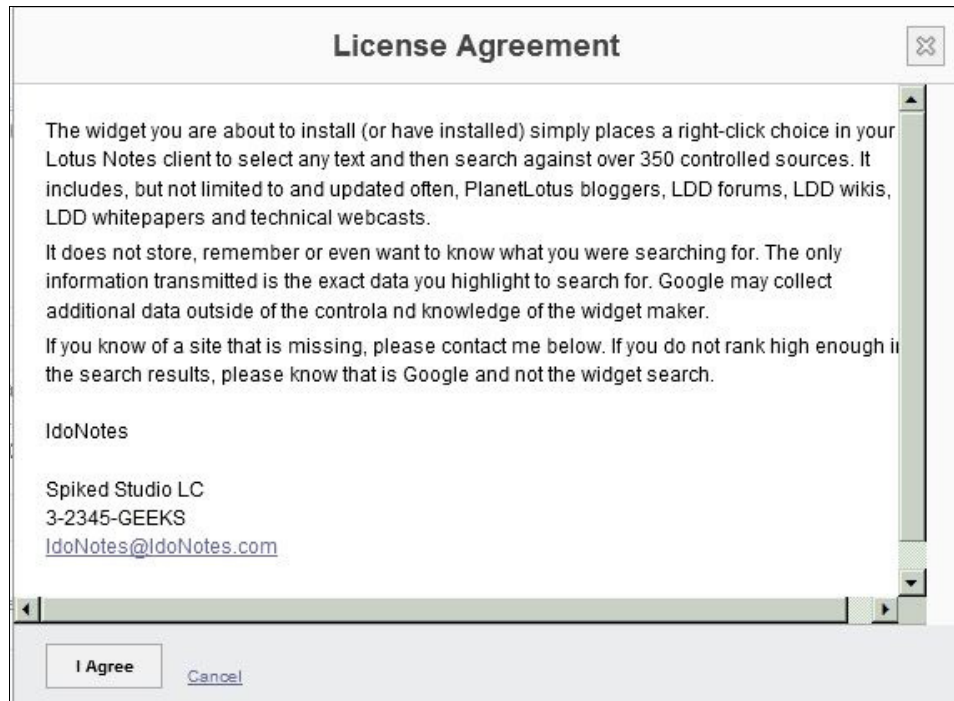
Complete the following steps to download content:

1. Log in to IBM Greenhouse.
2. Click **Start Download** as highlighted on the upper right in the figure below. The application prompts you to log in if you have not already done so.



3. License Agreement:


The license agreement is from the widget creator, usually an IBM Business Partner. The license agreement is to protect the creator of the free utility and notify you of any licensing requirements for usage. While most of the catalog solutions are free, some are for personal use and not meant to deploy to everyone in the enterprise without a purchased license. Make sure to read each one before continuing.



4. Download option:

Some of the solutions in the catalog might be a template or portlet, while others allow you to deploy it immediately into the IBM Notes client with a simple drag and drop (depending on your security policies) as the figure shown below.

[Return to Catalog](#)

  
**IDoNotes**

### Lotus Blogger and Technical Search Widget


Version: 1.1

Published by [Chris Miller](#) on Oct 25, 2010

Provided by [IDoNotes / Spiked Studio LLC](#)

Entry downloaded 248 times

Rating: ★★★★★ (click stars to vote)

**Download Options**  
 Drag and drop install



## Working with Tivoli Directory Integrator for custom Profiles

There are two methods to populate data into IBM Connections Profiles database:

- ▶ Profiles Administration REST API

You can use Profiles Administration REST API to populate profiles data from different type of systems, developed in different languages, and running on different platforms. You also can use this API in certain complex situations. For example, when Tivoli Directory Integrator plug-in for a specific systems is not available, is not functional enough, is too complicated to develop.

- ▶ Tivoli Directory Integrator (TDI) with plug-ins

Created specially for IBM Connections, TDI plug-ins provides a variety APIs that can help reduce low level programming for accessing external resource and obtaining data from them.

In this appendix, we discuss, through example, how to populate Profiles database with Tivoli Directory Integrator. We cover the following topics:

- ▶ What is customizable?
- ▶ Creating and using custom functions to manipulate data
- ▶ Creating custom mapping
- ▶ Setting up Tivoli Directory Integrator properties files

## B.1 What is customizable?

As an IBM Connections System administrator, you can load the profile attributes from LDAP Server, files (such as a CSV file), relational database, and other systems such as human resource system. Profile customization through TDI include:

- ▶ Mapping profile attribute to a custom attribute at LDAP
- ▶ Adding extended fields
- ▶ Creating custom functions, using JavaScript.
- ▶ Customizing user login attribute
- ▶ Customizing search

The most common source of user data is the LDAP directory, to load data from the enterprise LDAP directory to Profiles database, you can use IBM Tivoli Directory Integrator (TDI) and IBM Connections TDI Solutions Package.

### B.1.1 IBM Tivoli Directory Integrator

Tivoli Directory Integrator provides the functionality to join different software components an integrated software solution. TDI features includes:

- ▶ It is an integration tool that can easily move, copy, and transform data between applications and systems.
- ▶ It has a set of connectors that connect to different types of systems and protocols, such as LDAP, JDBC, JMS, SMTP, HTTP (client), JMX, JNDI, IBM MQ, Notes, and so on.
- ▶ It has an integrated and agile development tool IDE. Based on the power of Eclipse Platform, the TDI development environment is both comprehensive and extensible.

### B.1.2 TDI solutions package

The IBM Connections 4 comes with a set of ready-to-use TDI solution files that can allow IBM Connections System Administrator to easily load their Profiles data with user entries. The TDI Solution Package is located in the /TDISOL subdirectory. In our environment, the location is /opt/IBM/LotusConnections/TDISOL

This directory contains two archive files, **tdisol.tar** and **tdisol.zip**, for Linux and Windows, respectively. TDI deployment is simple and straight forward. You just extract the files to a local directory on a server from which you plan to run the Profiles load and synchronization scripts and configure certain files. It is not required to run TDI on the same server as IBM Connections. You can place TDI on the database server to reduce network latency or on its own server.

#### Profiles TDI solution directory

The following are the subdirectory under the TDI solution directory:

- ▶ *conf*: Used to configure Profiles extensions properties
- ▶ *etc*: Contains log4j.properties where logging can be enabled
- ▶ *lib*: Database driver and profiles backend library files
- ▶ *logs*: Task log files (except for Wizard)
- ▶ *packages*: Used to develop TDI connectors
- ▶ *samples*: Additional optional sample files
- ▶ *TDISysStore*: Local Derby database for TDI specific storage

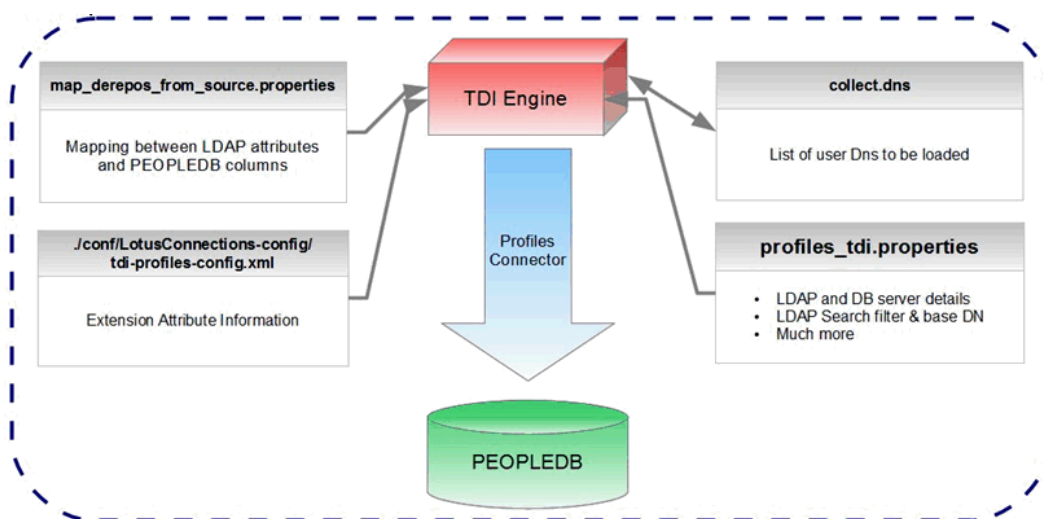
The files for maintaining the Profiles include:

- ▶ *profiles\_tdi.properties*: This file contains the property values relevant to your configuration. See the IBM Connections 4 Wiki for a full explanation of all parameters.
- ▶ *profiles\_tdi.xml*: This the TDI solution file that contains all TDI “assembly lines”.
- ▶ *map\_dbrepos\_from\_source.properties*: Defines mappings from the enterprise directory (or input sources) to the Profiles database. The mapping can consist of:
  - LDAP Attribute: Specifies the LDAP attribute to assign to the database field
  - JavaScript™ function: Specifies a JavaScript function whose return value is the value assigned to the database field. The function name is specified in between “{}” in the mapping file, map\_dbrepos\_from\_source.properties.
- ▶ *profiles\_functions.js*: JavaScript mapping functions
- ▶ *collect.dn*: Contains the distinguished names from the LDAP directory.
- ▶ *tdi-profiles-config.xml*: Defines mapping for custom extension attributes to fields in your source LDAP directory
- ▶ *t.bat* or *\*.sh*: Scripts to run Profiles TDI tasks

### B.1.3 How user data is load to Profiles database

The following figure show how TDI works. Aafter loading source data for each user, TDI engine updates Profiles database (PEOPLEDB) using the Profiles Connector. The following is the execution flow of load user data to the Profiles in IBM Connections:

1. Based on values in profiles\_tdi.properties, TDI searches LDAP and creates a file (default: collect.dns) of users to be imported.
2. Based on map\_dbrepos\_from\_source.properties and collect.dns, TDI loads data for each user into PEOPLEDB, using the Profiles Connector, available in TDI Solution.
3. If extension attributes are specified in tdi-profiles-config.xml, these are also loaded during step 2.



## B.2 Creating and using custom functions to manipulate data

In this section, we use an example to explain how to create and use custom functions to manipulate data. IBM Connections is an integrated and secure platform that many leading companies use to help their employees engage with networks of experts in the context of critical business processes in order to act with confidence, and to anticipate and respond to emerging opportunities. It is common that the experts are located in different time zones around the world. Having time zone information in the user profile will be convenient for finding a proper time to contact the expert.

Here we show how to add time zone information into profile. In our example, the user profile has office address. We use the city to determine the time zone. The steps are as follows:

1. Creating mapping function.
2. Adding the mapping function to profile\_functions.js
3. Setting field attributes
4. Synchronizing profile data

### B.2.1 Create a function that maps the city for timezone

IBM Tivoli Directory Integrator (TDI) functions are JavaScript scripts, TDI includes the IBM JSEngine to provide a fast and reliable scripting environment. Create a new function that maps city to time zone according to the following table:

| Office    | Time Zone         |
|-----------|-------------------|
| New York  | America/New_York  |
| London    | Europe/London     |
| Bangalore | Asia/Kolkata      |
| São Paulo | America/Sao_Paulo |

The following is a simple time zone mapping function:

---

```
function func_setTimeZone(fieldname) {
    var location = work.getString("city");

    if (location == "sao paulo") {
        result = "America/Sao_Paulo";
    }
    else if (location == "new york") {
        result = "America/New_York";
    }
    else if (location == "bangalore") {
        result = "Asia/Kolkata";
    }
    else if (location == "london") {
        result = "Europe/London";
    }

    return result;
}
```

---

## B.2.2 Adding function to profile\_functions.js

Under the TDI solution directory, the profiles\_functions.js file contains functions for manipulating data within IBM Connections. The default location of TDI Solution directory is */opt/IBM/TDIPopulation/TDISol/linux*.

Add this new time zone mapping function to profiles\_functions.js.

## B.2.3 Map function within the file map\_dbrepos\_from\_source.properties

Set the time zone field in the map\_dbrepos\_from\_source.properties file to use the mapping function. In this example, we specify the following property in map\_dbrepos\_from\_source.properties:

```
timezone={func_setTimeZone}
```

## B.2.4 Synchronize the data

Run the update script sync\_all\_dns to update the Profile database with the values in the LDAP server:

- ▶ AIX and Linux:

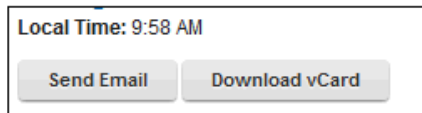
```
# chmod +x sync_all_dns.sh
./sync_all_dns.sh}}
```

- ▶ Microsoft Windows:

```
> sync_all_dns.bat
```

### Checking the result

After finished the update script, you can check the **Local Time** file in user profiles page:



## B.3 Creating custom mapping

An extended attribute is a container for fields that are not in the default schema of a Profile, within database of IBM Connections. The Profiles application provides a set of default attributes. The attributes of a Profile are common to most of the companies. Because every organization's directory structure is unique, the Profiles application provides the ability to add additional custom extension attributes. For example, you might want to add an extra attribute for your organization that allows employees to specify their mentor.

The extension attribute is a method for managing additional customer specific data in Profiles. Examples of using extension attributes includes:

- ▶ Social media IDs field for Facebook or Twitter IDs.
- ▶ Birthday field
- ▶ Company Division field to hold the internal name of a division of a company



- Company Organization Unit Code field

An extension attributes can be populated with value from a external source such as LDAP directory, HR system, or it can be null, so the user can update the value. An extension can be set as editable or read-only.

You can create a custom mapping at IBM Connections 4 by adding custom extension attributes in Profiles application. In this section, we explain what is an extension attribute and how the extension attributes are stored in Profiles.

### B.3.1 How extension attributes are stored in Profiles (PEOPLEDDB)

Because the extension attributes are not part of the default schema, extension attributes have their own table, PROFILE\_EXTENSIONS.

The following table shows the main columns of PROFILE\_EXTENSIONS.

| Column name      | Primary Key | Null Value | Description                       |
|------------------|-------------|------------|-----------------------------------|
| PROF_KEY         | X           |            | profile key                       |
| PROF_PROPERTY_ID | X           |            | name of the extension attribute   |
| PROF_NAME        |             |            | Label for the extension attribute |
| PROF_DATA_TYPE   |             |            | type of extension attribute       |
| PROF_VALUE       |             |            | value of the extension attribute  |

Profiles adds extension attributes by inserting rows in this table. The following figure shows an example of the extension attribute rows in the PROFILE\_EXTENSIONS table.

| PROF_KEY              | PROF_PROPERTY_ID | PROF_NAME | PROF_DATA_TYPE | PROF_VALUE  |
|-----------------------|------------------|-----------|----------------|-------------|
| 8f2059-a0ca-4683-...  | division         |           | String         | ITSO Canada |
| 8f2059-a0ca-4683-...  | twitterid        |           | String         | @aberzat    |
| 8f2059-a0ca-4683-...  | org_nr           |           | String         | 20315       |
| 20bb555-6975-49fd...  | division         |           | String         | ITSO Brazil |
| 20bb555-6975-49fd...  | twitterid        |           | String         | @eniobasso  |
| 20bb555-6975-49fd...  | org_nr           |           | String         | 3045        |
| 9fd35cb-40e6-4ff4-... | division         |           | String         | ITSO India  |
| 9fd35cb-40e6-4ff4-... | org_nr           |           | String         | 20113       |
| 8567955-05a1-49eb..   | division         |           | String         | ITSO USA    |
| 8567955-05a1-49eb..   | twitterid        |           | String         | @bzechman   |
| 8567955-05a1-49eb..   | org_nr           |           | String         | 11321       |

### B.3.2 Adding a custom mapping

The basic steps for adding a custom mapping is as follows:

1. Add an extension attribute to the Profiles application.
2. Create a custom Label file.
3. Add the custom label file to IBM Connections.
4. (Optional) Configure IBM Connections TDI Solution to populate extension attributes.

## Adding an extension attribute to Profiles Application

To add a custom extension attributes to Profiles Application, you use wsadmin to change profiles-config.xml and update Profiles application. The wsadmin client is an IBM WebSphere Application Server scripting environment that you can used to access and change properties that govern the IBM Connections configuration.

1. On the WebSphere Application Server Deployment Manager (Deployment Manager) server, created a temporary directory to checkout the configuration file:

- AIX/Linux: # **mkdir -p /root/temp**
  - Microsoft Windows: **cd c:/prof/temp**

2. Go to the Deployment Manager binary directory

- AIX/Linux: # **cd /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin**
  - Microsoft Windows: **cd c:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin**

3. Run **wsadmin**:

- AIX/Linux: # **./wsadmin.sh -lang jython -user wasadmin -password <your password>**
- Microsoft Windows: > **wsadmin.bat -lang jython -user wasadmin -password**

4. Load Profiles administration scripts:

```
wsadmin> execfile("profilesAdmin.py")
```

5. Check out files:

- AIX/Linux: **wsadmin**  
**>ProfilesConfigService.checkOutConfig("/root/temp",AdminControl.getCell())**
- Microsoft Windows: **wsadmin**  
**>ProfilesConfigService.checkOutConfig("c:/prof/temp",AdminControl.getCell())**

6. Edit the profiles-config.xml file using a text editor to add elements. The follow is our example. We define the extension attribute by adding the following code to the element under :

---

```
<simpleAttribute extensionId="division" length="64" />
<simpleAttribute extensionId="twitterid" length="64" />
<simpleAttribute extensionId="org_nr" length="64" />
```

---

7. To display the extension attribute., add child element under the element.

In our example, we specify the values for bundleIdRef and labelKey to be used with our custom Label files. The following table shows the XML attributes associated with extensionAttribute.

| Column name    | Description   |
|----------------|---|
| showLabel      | Specifies whether to display a label for the extension attribute in the user interface. The attribute takes a Boolean value.    |
| hideIfEmpty    | Specifies whether to hide the attribute if it does not have a value. This attribute takes a Boolean value.                      |
| editable       | Specifies if the extension attribute can be edited by users. This attribute takes a Boolean value.                              |
| prependHtml    | Specifies the HTML code prefixed to the value. This attribute takes a string value.   |
| appendHtml     | Specifies the HTML code appended to the value. This attribute takes a string value.   |
| bundleIdRef    | Specifies the referenced bundle ID of the label. This attribute takes a string value.   |
| extensionIdRef | The ID of the extension. This ID is associated with the property key in the resource file. This attribute takes a string value. |
| labelKey       | Specifies the referenced key name of the label. This attribute takes a string value.  |

The following is our example:

---

```
<extensionAttribute showLabel="true" hideIfEmpty="true" editable="false"
prependHtml="" appendHtml="&lt;br&gt;" bundleIdRef="MyLabels"
extensionIdRef="division" labelKey="label.itso.division" />
```

```
<extensionAttribute showLabel="true" hideIfEmpty="true" editable="false"
prependHtml="" appendHtml="&lt;br&gt;" bundleIdRef="MyLabels"
extensionIdRef="twitterid" labelKey="label.itso.twitterid" />
<extensionAttribute showLabel="true" hideIfEmpty="true" editable="false"
prependHtml="" appendHtml="&lt;br&gt;" bundleIdRef="MyLabels"
extensionIdRef="org_nr" labelKey="label.itso.org_nr" />
```

---

Save and exit.

8. Check in files using the following commands:

```
wsadmin> ProfilesConfigService.checkInConfig()
```

9. Exit wsadmin:

```
wsadmin> exit
```

## Creating a custom Label file

You can use a property file to display descriptive labels for the new extension attributes in Profiles page:

1. Go to the **/customization/strings** directory:

- AIX/Linux: # **cd /opt/LotusConnections/customization/strings**
- Microsoft Windows: > **cd \IBM\LotusConnections\customization\strings**

2. Create the label file:

The format of the properties file must be the following:

Label = value

We name our file **com.itso.resources.properties** and we define the following labels:

---

```
label.itso.division=Division:
label.itso.twitterid=Twitter Id:
label.itso.org_nr=Organization Number:
```

---

3. Save and close the file.

## Adding the custom label file to IBM Connections

To add labels to the custom extension attributes, you must add the changes in LotusConnections-config.xml and update IBM Connections using wsadmin:

1. Using the steps described in the Adding an extension attribute to *Profiles Application* section to start wasadmin and check out the configuration file.

2. Load IBM Connections administration scripts:

```
wsadmin> execfile("connectionsConfig.py")
```

3. Check out configuration file:

- AIX/Linux: wsadmin  
>**LCCConfigService.checkOutConfig("/opt/temp",AdminControl.getCell())**
- Microsoft Windows: wsadmin  
>**LCCConfigService.checkOutConfig("c:/prof/temp,AdminControl.getCell())**

4. Edit the the LotusConnections-config.xml file and add the label file to section as follows:

5. Check in file:

```
wsadmin> LCCConfigService.checkInConfig()
```

6. Exit wsadmin:

wsadmin> exit

## Restart IBM Connections

Access the IBM Solution Console using the user name defined as the primary administrator and restart IBM Connections applications.

## (Optional) Configure IBM Connections TDI Solution to populate extension attributes

You can use IBM Connections TDI Solution Scripts to populate custom extension attributes by adding extension attributes to **tdi-profiles-config.xml** and run **populate\_from\_dn\_file** or **sync\_all\_dns\_scripts** as follows:

1. Open the /TDISOL/conf/LotusConnections-config/tdi-profiles-config.xml file in a text editor.

In our environment, the default location of TDI Solution directory is

**/opt/IBM/TDIPopulation/TDISol/linux/conf/LotusConnections-config/tdi-profiles-config.xml**.

2. To define the extension attribute, add the element under as follows:

```
<simpleAttribute extensionId="division" sourceKey="division" userTypeString="String" length="64" />
```

---

```
<simpleAttribute extensionId="division" sourceKey="division"
userTypeString="String" length="64" />
<simpleAttribute extensionId="twitterid" sourceKey="twitterid"
userTypeString="String" length="64" />
<simpleAttribute extensionId="org_nr" sourceKey="org_nr"
userTypeString="String" length="64" />
```

---

where

| Column name    | Required | Description  |
|----------------|----------|--|
| extensionId    | X        | The ID of the extension attribute.   |
| sourceKey      | X        | The name of the LDAP attribute that maps to the extension attribute.   |
| userTypeString |          | An administrator-defined string defining the data type of the extension attribute. This string does not display in the user interface or API.              |
| length         |          | Length of Extension attribute  |
| userLabel      |          | An administrator-defined label for the extension attribute that is populated into the database. This string does not display in the user interface or API. |

Save and exit.

The following figure shows how data is inserted inside tdi-profiles-config.xml.

```

<tdiConfig id="tdi-profiles"
  xmlns="http://www.ibm.com/profiles-config"
  xmlns:tns="http://www.ibm.com/profiles-config"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xsi:schemaLocation="http://www.ibm.com/profiles-config profiles-config.xsd">
  <profileExtensionAttributes>
    <!-- Connections 4 Redbook - Start-->
    <simpleAttribute extensionId="division" sourceKey="division" userTypeString="String" length="64" />
    <simpleAttribute extensionId="twitterid" sourceKey="twitterid" userTypeString="String" length="64" />
    <simpleAttribute extensionId="org_nr" sourceKey="org_nr" userTypeString="String" length="64" />
    <!-- Connections 4 Redbook - End-->
    <!--
      This extension attribute is required by the 'MyLinks' profile widget
    -->
    <xmlFileAttribute
      extensionId="profileLinks"
      schemaFile="profile-links.xsd"
      indexBindingExpr="/linkroll/link/@name | /linkroll/link/@url">
      <indexFields>
        <indexField fieldName="linkName" fieldExpr="/linkroll/link/@name" />
      </indexFields>
    </xmlFileAttribute>
  </profileExtensionAttributes>
</tdiConfig>

```

3. Running the scripts in IBM Connections TDI Solution directory to populate or synchronize the profile data:

If this is initial population, use **populate\_from\_dn\_file** script, as follow:

- ▶ AIX/Linux:

```
# chmod +x populate_from_dn_file.sh
# ./populate_from_dn_file.sh
```

- ▶ Microsoft Windows:

```
> populate_from_dn_file.bat
```

If your data is already loaded, use **sync\_all\_dns** script to synchronize data:

- ▶ AIX/Linux:

```
# chmod +x sync_all_dns.sh
# ./sync_all_dns.sh
```

- ▶ Microsoft Windows:

```
> sync_all_dns.bat
```

## B.4 Setting up Tivoli Directory Integrator properties files

In this section, we explain to the main property files necessary to set up IBM Connections TDI Solutions Package, that are:

- ▶ profiles\_tdi.properties
- ▶ map\_dbrepos\_from\_source.properties

### B.4.1 PROFILES\_TDI.PROPERTIES file

This file includes the following properties:

- ▶ source\_ldap\_url  
The LDAP web address used to access the source LDAP system.
- ▶ source\_ldap\_user\_login

Login user name used for authentication.

- ▶ `source_ldap_user_password`

Login password used for authentication.

- ▶ `source_ldap_search_base`

The search base (the location from where the search begins) of the iterating directory.

- ▶ `source_ldap_search_filter`

Search filter used when iterating the directory.

- ▶ `source_ldap_use_ssl`

Required if you are using SSL to authenticated.

- ▶ `dbrepos_jdbc_driver`

The JDBC driver implementation class name used to access the Profiles database repository.

For DB2, the default is `com.ibm.db2.jcc.DB2Driver`, for example:

---

```
dbrepos_jdbc_driver=com.ibm.db2.jcc.DB2Driver
```

---

For Oracle, the default is `oracle.jdbc.driver.OracleDriver`, for example:

---

```
dbrepos_jdbc_driver=oracle.jdbc.driver.OracleDriver
```

---

If you are using a Microsoft SQL Server database, change the value to reference a SQL Server driver, for example:

---

```
dbrepos_jdbc_driver=com.microsoft.sqlserver.jdbc.SQLServerDriver
```

---

- ▶ `sbrepos_jdbc_url`

JDBC web address used to access the Profiles database repository.

- ▶ `dbrepos_username`

User name under which the database tables, which are part of the Profiles database repository, are accessed.

- ▶ `dbrepos_password`

Password associated with the user name under which the database tables, which are part of the Profiles database repository, are accessed.

The following is example of our environment

---

```
source_ldap_url=ldap://ldap-dom.itso.ibm.com:389
source_ldap_use_ssl=false
source_ldap_user_login=cn=domadmin
source_ldap_search_base=o=itso
source_ldap_search_filter=(&(uid=*)(objectclass=dominoPerson))
#source_ldap_user_password=<PUT_YOUR_LDAP_PASSWORD_HERE>
{protect}-source_ldap_user_password={encr}xkPPGXwafVULAhCCWQ1CwgdR41StVqDPc0UkWIiB
6QDL0nYzZKERZDcAZ6ZvVMfB0Sq4f0eIcGUq5qkh3r1QI2gwwV+vj780Lv/IXLXR9j8KApW0Mp7XEX0zpp
ks4SDvyja30X854KQ4/eUy8fCeBdkgIyXCT22Mbc3xP/b11ms=
```

---

## B.4.2 MAP\_DBREPOS\_FROM\_SOURCE.PROPERTIES file

This file include the following properties:

- ▶ displayName

User name which will be displayed in IBM Connections

- ▶ distinguishedName

Full hierarchical name. Example:

uid=Sandra Smith,o=Renovations,c=US

- ▶ email

User Internet Address

- ▶ loginId

Attribute to be used as username at login

- ▶ uid

User unique ID

- ▶ guid

The guid property identifies the global unique ID of a user. This property's value is created by the LDAP directory and is unique, complex, and never changes.

- IBM Tivoli Directory Server:

---

```
guid=ibm-entryUuid
```

---

- IBM Lotus® Domino® Directory:

---

```
guid={function_map_from_dominoUNID}
```

---

- Microsoft™ Active Directory:

---

```
guid={function_map_from_objectGUID}
```

---

- Sun Java™ System Directory Server:

---

```
guid=nsuniqueid
```

---

- eNovelle System Directory Server:

---

```
guid={unction_map_from_GUID}
```

---

- ▶ surname

User Last name

The following is example of our environment

---

```
displayName=cn
distinguishedName=$dn
email=mail
loginId=mail
uid={func_map_to_db_UID}
guid={function_map_from_dominoUNID}
surname=sn
```

---

## Downloading the software from Passport Advantage and PartnerWorld

You can obtain IBM Connections, including its prerequisites, from IBM Passport Advantage. Before downloading, find the appropriate product part numbers for your operating system from the Required Parts list in the following IBM TechNote website:  
<http://www-01.ibm.com/support/docview.wss?uid=swg24033179>

When you have part number ready, use the following steps to download the software for IBM Connections software from IBM Passport Advantage:

1. Sign into IBM Passport Advantage from a web browser with your IBM ID and password using the following URL:  
[http://www-01.ibm.com/software/lotus/passportadvantage/pao\\_customer.html](http://www-01.ibm.com/software/lotus/passportadvantage/pao_customer.html)
2. Accept the terms of the IBM PartnerWorld Software Usage agreement:



IBM PartnerWorld > Software Access Catalog >

## Software Access Catalog

Please note that before you can begin shopping in the IBM Software Access Catalog, you must scroll down to read and accept the terms of this attachment.

### IBM PartnerWorld Agreement PartnerWorld Software Usage Attachment

The terms of this IBM PartnerWorld Software Usage Attachment are in addition to and prevail over the terms of the IBM PartnerWorld Agreement - International Basic General Terms (PWA). Additionally, the terms of this Attachment are in addition to and prevail over the terms of the IBM International Program License Agreement (IPLA) and the IBM International License Agreement for Non-Warranted Programs (ILAN) (whichever of these which are supplied with the Programs) and their associated License Information (LI). For all applicable Programs, any of the following actions by you constitutes your acceptance of the terms of the above Agreements, the License Information and the terms of this Attachment: downloading, installing, copying, accessing or using the Programs.

Additional details regarding this Attachment are specified on the PartnerWorld website.

#### 1.0 Scope of Use

You may install and use a commercially reasonable number of copies (unless we specify otherwise) of each Program only for the purposes specified in this Attachment. A commercially reasonable number of copies is no more than the number of active employees who are registered and associated with your company's PartnerWorld Country Enterprise profile and using the Programs for the approved usages as defined in this Attachment. However, we specify in the Schedule the maximum number of copies you are authorized to make of certain Programs.

Your authorization to use the Programs under this Attachment is limited to those Programs that are currently available in the Software Access Catalog. You agree to check the Software Access Catalog on a quarterly basis to ensure that the Programs you are using are still available in the Software Access Catalog, and, if not, to cease using the Programs as specified in Section 3 (Termination of Usage).

Unless we specify otherwise, under the terms of this Attachment, Programs may only be used and installed within your Country Enterprise as defined in the PWA.

3. Search the product you need using the part-numbers or product names:

IBM PartnerWorld >

## Software Access Catalog Downloads

**Note:** The Software Access Catalog will be unavailable Thursday, January 17 at 5pm EST through Sunday, January 20 at 5:00pm EST due to system maintenance. We apologize for any inconvenience this may cause.

### Overview

IBM's Software Access Catalog allows you to download IBM software products at no charge. The products downloaded may only be used for demonstration, evaluation, development, testing, education, and limited internal "Run Your Business" purposes as specified in the [PartnerWorld Software Usage Attachment](#).

Note that some products require a license key for operation. Look for links to more details in the "Related links" list on the left side of this page.

#### Find by search text

Type all or part of a product name and click Search or click one of the pop-up suggestions. You can select additional filters below.

Search

► Search filter options

#### Find by brand

Select a brand. You must select additional filters below.

Select a brand Search

► Search filter options

#### Find by part number

Enter single or multiple part numbers (separated by commas) and click Search. Example: CR1V9NA, C47EHML

Search

#### Your previous searches

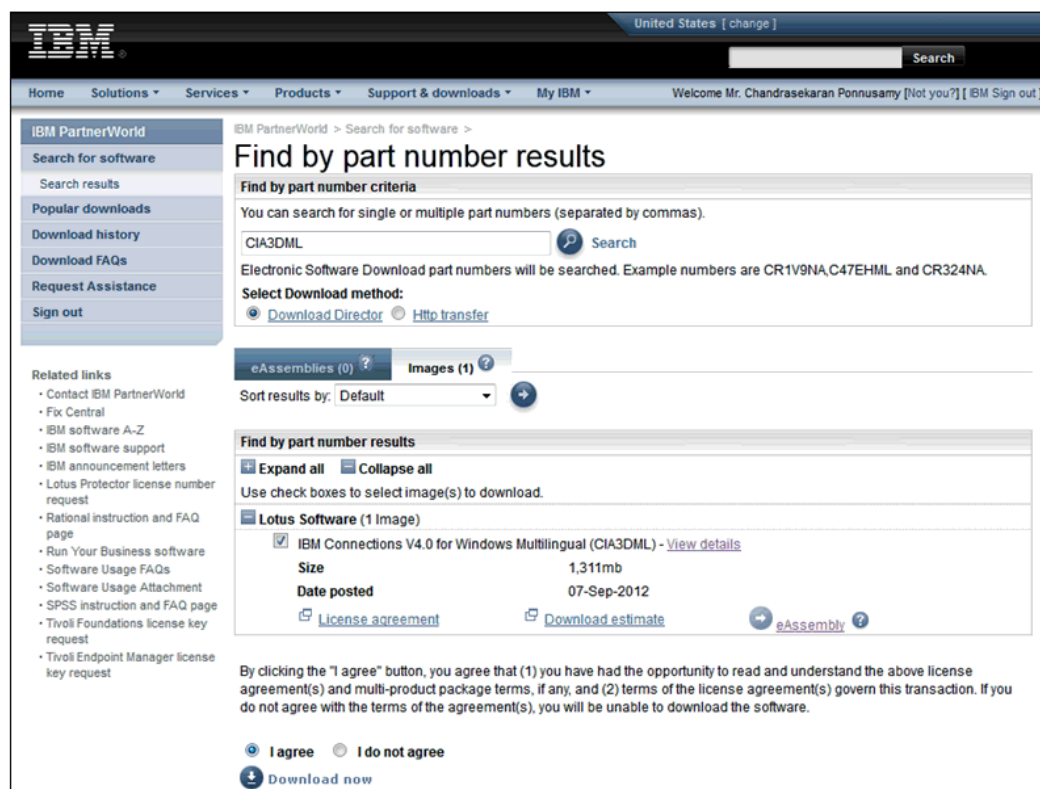
Select one of the options below

- Find by search text
- Find by brand
- Find by part number

#### Related links

- Contact IBM PartnerWorld
- Fix Central
- IBM software A-Z
- IBM software support
- IBM announcement letters
- Lotus Protector license number request
- Rational instruction and FAQ page
- Run Your Business software
- Software Usage FAQs
- Software Usage Attachment
- SPSS instruction and FAQ page
- Tivoli Foundations license key request
- Tivoli Endpoint Manager license key request

4. Expand the corresponding sections to locate the correct image. Select **I Agree** and click **Download** to begin downloading the software:.



The following website contains demonstrations about how to access and download software from IBM Passport Advantage:

- IBM Passport Advantage Login: Online Access Guide:  
<http://www.youtube.com/watch?v=9pY0fSad5p0>
- IBM Passport Advantage: Downloading Products from Passport Advantage:  
<http://www.youtube.com/watch?v=HuatqV8jpu4>





# Installing and Deploying IBM Connections

Produced in  
collaboration with:



**Redbooks**®