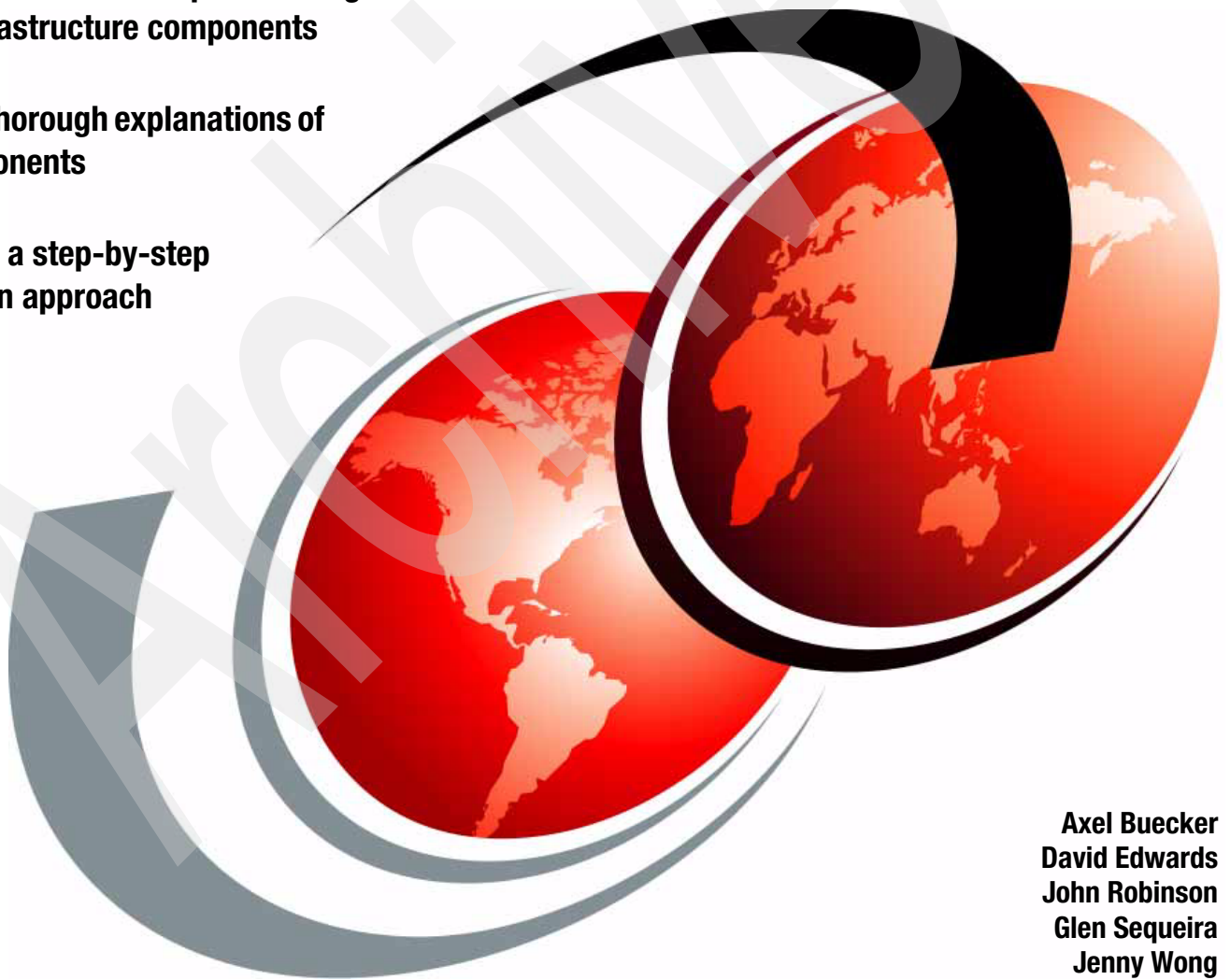


Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments

Covers the detailed setup and configuration for all infrastructure components

Provides thorough explanations of key components

Discusses a step-by-step installation approach



Axel Buecker
David Edwards
John Robinson
Glen Sequeira
Jenny Wong



International Technical Support Organization

**Setup and Configuration for IBM Tivoli Access
Manager for Enterprise Single Sign-On 8.1 for
Single-Server and Cluster Environments**

November 2010

Archived

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

Archived

First Edition (November 2010)

This edition applies to Version 8.1 of the IBM Tivoli Access Manager for Enterprise Single Sign-On.

© Copyright International Business Machines Corporation 2010. All rights reserved.

Note to U.S. Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Notices	v
Trademarks	vi
Preface	vii
The team who wrote this paper	vii
Now you can become a published author, too!	viii
Comments welcome	viii
Stay connected to IBM Redbooks	ix
Chapter 1. Installation and configuration onto a single Windows server	1
1.1 Database installation and configuration	4
1.1.1 Installing DB2	4
1.1.2 Creating a database	12
1.1.3 Creating a DB2 user	15
1.2 IBM WebSphere Application Server	16
1.2.1 Installing WebSphere Application Server 7.0	16
1.2.2 Installing IBM Update Installer for WebSphere software installation	21
1.2.3 Upgrading WebSphere Application Server	22
1.3 IMS Server	26
1.3.1 Preparing WebSphere Application Server for Global Application Security	26
1.3.2 Installing IMS	27
1.3.3 Verifying the IMS Server installation and deployment	33
1.4 HTTP Server and WebSphere Application Server plug-in	33
1.4.1 Installing HTTP Server	34
1.4.2 Configuring the IBM HTTP Server	41
1.4.3 Applying HTTP Server fix pack	48
1.5 IMS configuration	48
1.5.1 Applying the IMS fix pack	48
1.5.2 Creating IMS administrator in Active Directory	49
1.5.3 Configuration of the IMS Server	49
1.5.4 Provisioning IMS administrator and defining enterprise directory	57
1.6 AccessAgent and AccessStudio	63
1.6.1 Preparing to install AccessAgent	63
1.6.2 Installing AccessAgent	64
1.6.3 Installing AccessStudio	64
1.7 Conclusion	65
Chapter 2. Installation and configuration in a clustered environment	67
2.1 Database installation and configuration	69
2.1.1 Installing IBM DB2 Workgroup Server Version 9.7	69
2.1.2 Configuring DB2	77
2.2 WebSphere Application Server Network Deployment	80
2.2.1 WebSphere Update Installer	88
2.2.2 WebSphere fix pack	90
2.3 IBM HTTP Server	107
2.3.1 IBM HTTP Server fix pack	114
2.3.2 IBM HTTP Server plug-in pack	117
2.4 IMS Server	126
2.5 Configuration on WebSphere Application Server	135

2.5.1	Installing Native Library Invoker rar file	135
2.5.2	Installing IMS Server ear file	143
2.5.3	Administering Tivoli Access Manager for Enterprise Single Sign-On from WebSphere Application Server.	149
2.5.4	Importing root certificate to CellDefaultKeyStore	155
2.5.5	Copying \tamesso directory.	159
2.5.6	Resynchronizing nodes.	160
2.5.7	Setting up J2C authentication data	161
2.5.8	Creating data source for DB2 database	164
2.6	Configuration for IBM HTTP Server	182
2.6.1	Running the configurewebserver script.	183
2.6.2	Setting up SSL certificates	184
2.6.3	Enabling SSL on the HTTP Server	188
2.7	Adding nodeagent and server to Windows services	199
2.7.1	nodeagent	199
2.7.2	server1	201
Appendix A. Database type configuration for IMS Server.		203
Microsoft SQL Server configuration for IMS Server		204
Appendix B. Diagnosing installation problems		207
AccessAgent connection to IMS Server		208
Is the HTTP server/port accessible		208
Is the HTTPS port accessible		208
Does the host name match the SSL Cert DN		208
Is the WebSphere Application Server available for SOAP requests		208
Is WebSphere Application Server plug-in configured correctly		209
Appendix C. Using ports and networks		211
Appendix D. Uninstalling Tivoli Access Manager for Enterprise Single Sign-On		213
Standard uninstall		214
Additional WebSphere Application Server cleanup		214
File system cleanup		215
Appendix E. Creating WebSphere Application Server		217
Appendix F. Adding an IMS Server to the cluster		219
Related publications		221
IBM Redbooks publications		221
Other publications		221
Online resources		222
Help from IBM		222

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those Web sites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:


This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the web at <http://www.ibm.com/legal/copytrade.shtml>

The following terms are trademarks of the International Business Machines Corporation in the United States, other countries, or both:

DB2®
IBM®
Passport Advantage®

Redbooks®
Redpaper™
Redbooks (logo) ®

Tivoli®
WebSphere®

The following terms are trademarks of other companies:

Java, and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

This IBM® Redpaper™ publication covers the detailed step-by-step installation of IBM Tivoli® Access Manager for Enterprise Single Sign-On 8.1 onto a single-server and a clustered environment.

This paper supplements the *IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 Installation Guide* and *IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 Setup Guide*. Do not use this document in isolation. Check the relevant guides in the Tivoli Access Manager for Enterprise Single Sign-On Information Center as you perform the install.

There might be various reasons to install Tivoli Access Manager for Enterprise Single Sign-On into either a single server or a clustered environment. A small-scale deployment, a typical proof of technology, or a proof of concept might be the best examples for a single server installation, whereas larger scale deployments or requirements for high availability and scalability might be reasons to deploy in a clustered environment.

This IBM Redpaper is targeted towards administrators and engineers who are facing a Tivoli Access Manager for Enterprise Single Sign-On deployment on either a single IBM WebSphere Application Server or a clustered IBM WebSphere Application Server Network Deployment configuration.

The team who wrote this paper

This paper was produced by a team of specialists from around the world working at the International Technical Support Organization, Rochester Center.

Axel Buecker is a Certified Consulting Software IT Specialist at the ITSO, Austin Center. He writes extensively and teaches IBM classes worldwide on areas of software security architecture and network computing technologies. He holds a degree in Computer Science from the University of Bremen, Germany. He has 24 years of experience in a variety of areas related to workstation and systems management, network computing, and e-business solutions. Before joining the ITSO in March 2000, Axel worked for IBM in Germany as a Senior IT Specialist in Software Security Architecture.

David Edwards is a Consulting IT Specialist with the Tivoli Technical Sales team in IBM Australia. He has 22 years of experience in IT covering areas as diverse as application development, CICS® systems programming, and distributed systems management. He also has been a product specialist in the Tivoli Security products. He holds a Bachelor of Science (Chemistry and Applied Mathematics) degree from Monash University and a graduate diploma in Computer Science from Swinburne University. He has written extensively on the Tivoli Systems Management and Security products, including co-authoring four Redbooks publications, and authored a number of IBM Redpapers publications and developerWorks® articles.

John Robinson is a Software Engineering Manager at the IBM ADL Gold Coast site in Australia. He manages test and ID activities for several Tivoli security products. He holds bachelor's and master's degrees in Electrical Engineering and Computer Systems Engineering. Prior to this role, he lead the Tivoli Security Integration Factory team for eight years. He has over 20 years of experience with software engineering, specializing in security software architecture, design, and development. He has been involved with Tivoli Access

Manager for Enterprise Single Sign-On for the past two years, and has developed many of the access profiles currently in use.

Glen Sequeira is a Managing Consultant in the IBM Software Services for Tivoli (ISST) security practice team. He works on solution design and deployment of security products from the IBM Tivoli portfolio. Glen has over 18 years of experience in software engineering and deployment. Before joining the ISST team in 2006, he was a part of the IBM software development team on various Tivoli products. He has been working with the Tivoli Access Manager for Enterprise Single Sign-On product since 2008. Glen holds a degree in Computer Engineering from the University of Bombay, India.

Jenny Wong works as a Software Engineer for Tivoli Security Solutions Team at the IBM ADL Gold Coast site in Australia. She holds dual bachelor's degrees in Applied Mathematics and Information Technology. Since joining IBM in 2009, she has worked on various Tivoli Security products. She started to work on the IBM Tivoli Access Manager for Enterprise Single Sign-on product in the Tivoli Security Integration Factory during her first year rotation in the company, where she was involved in the development and testing of various profiles that are shipped in the product to date. Prior to joining IBM, Jenny was an intern at the Gold Coast lab and received a scholarship to undertake a full-year industry project at the lab as part of her final studies at the university.

Thanks to the following people for their contributions to this project:

Hans Aribowo, David Cecil, Aditya Cetlur, Rajeev Kumar, Jessilou Noelle Lawas, Song Lin, Dolcita Montemayor, Daniel KJ Ng, Prasanna Puranik, Sriram Saroop
IBM

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks® publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

ibm.com/redbooks

- Send your comments in an email to:

redbooks@us.ibm.com

- ▶ Mail your comments to:

IBM Corporation, International Technical Support Organization
Dept. HYTD Mail Station P099
2455 South Road
Poughkeepsie, NY 12601-5400

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>

Archived

Installation and configuration onto a single Windows server

In this chapter we cover the installation of IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 onto a single-server Windows® environment, where all components (server and database) are located on a single machine. We cover the installation of the supplied middleware (IBM DB2 and IBM WebSphere Application Server). Other deployment options are available, but are not covered.

This section supplements the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, and *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Setup Guide*, GC23-9692. Do not use this chapter in isolation. Check the relevant guides in the Tivoli Access Manager for Enterprise Single Sign-On Information Center as you perform the install.

In Figure 1-1 we provide an overview of the key components and installation and configuration steps for a single-server Tivoli Access Manager for Enterprise Single Sign-On 8.1 deployment. Figure 1-1 depicts the key dependencies between the steps and illustrates the overall interaction between components in the environment.

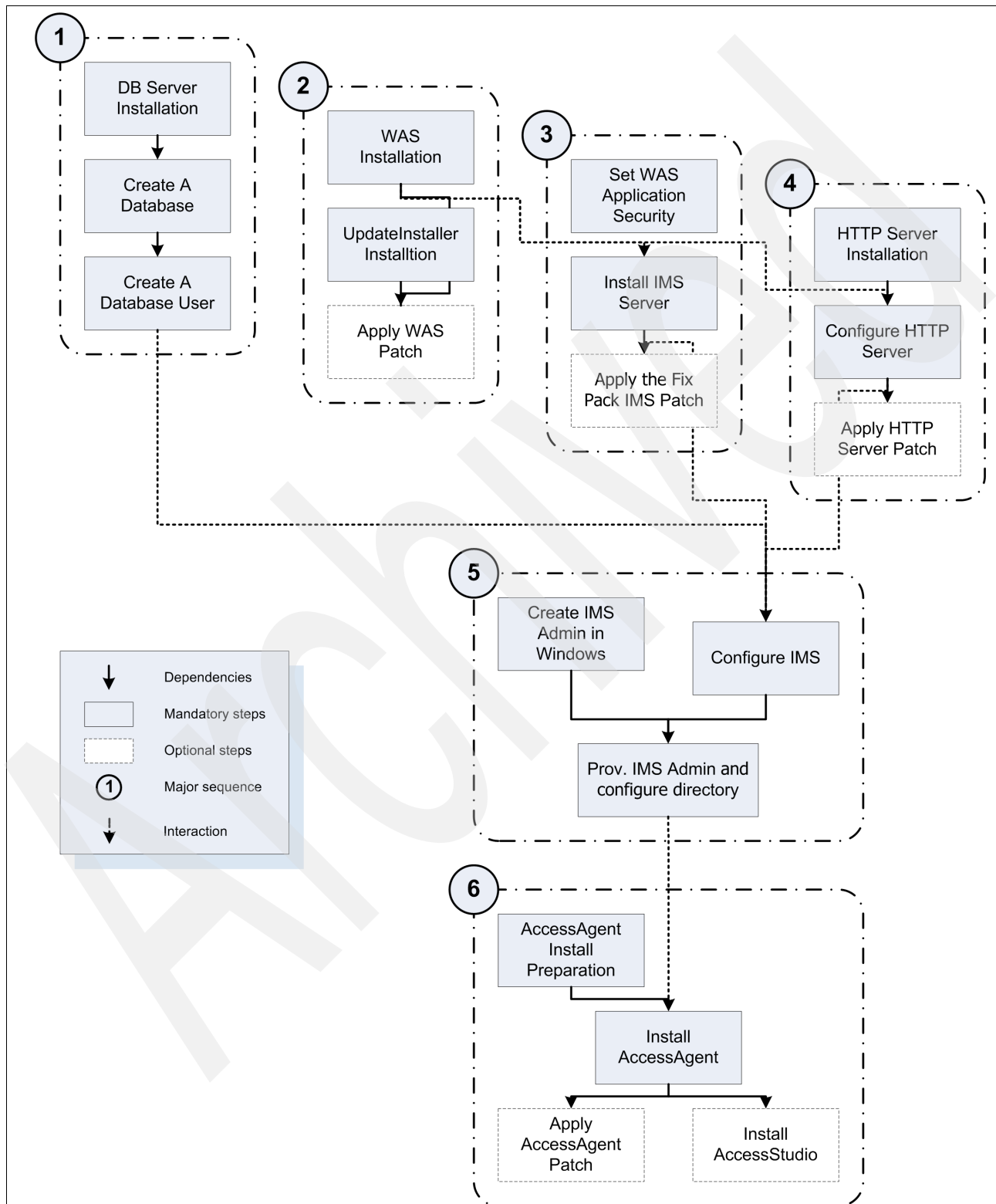


Figure 1-1 Dependencies and interaction between the key components

This chapter is divided into the following sections:

- ▶ 1.1, “Database installation and configuration” on page 4
- ▶ 1.2, “IBM WebSphere Application Server” on page 16 (including the IBM Update Installer)
- ▶ 1.3, “IMS Server” on page 26
- ▶ 1.4, “HTTP Server and WebSphere Application Server plug-in” on page 33 (including generation of the WebSphere Application Server plug-in for HTTP Server)
- ▶ 1.5, “IMS configuration” on page 48 (base configuration and definition of IMS administrator and enterprise directory)
- ▶ 1.6, “AccessAgent and AccessStudio” on page 63
- ▶ 1.7, “Conclusion” on page 65

There are a number of optional steps in Figure 1-1 on page 2 (shown as boxes with dashed outlines), such as the fix pack application steps. These might not be covered in this document in the strict order in which they are shown in the diagram (and the AccessAgent fix pack installation is not covered at all).

Note: It is required that you install the IMS Fix Pack 1. There are specific scenarios in which the fix pack is installed before IMS configuration. See the Tivoli Access Manager for Enterprise Single Sign-On Release Notes document for details:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc/references/RN_description.html

1.1 Database installation and configuration

Tivoli Access Manager for Enterprise Single Sign-On supports various versions of IBM DB2®, Microsoft® SQL Server, and Oracle databases. The following section walks you through the installation of the IBM DB2 database.

1.1.1 Installing DB2

The DB2 installation comes on a CD (or in the CD image) as a Windows executable such as DB2_ESE_V95_Win_x86.exe. The steps for the DB2 9.5 installation are:

1. Start up the DB2 Setup Launchpad wizard provided on the installation CD. Click **Install New** to launch the DB2 Setup Wizard (Figure 1-2).

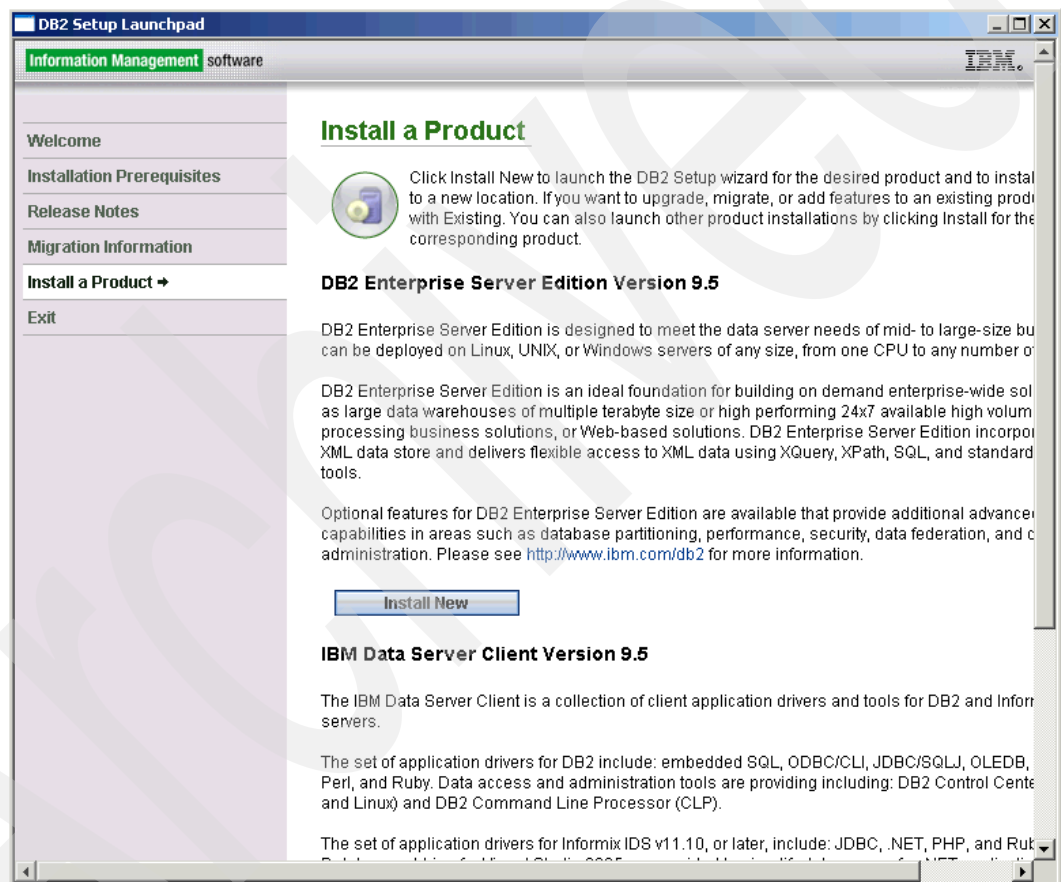


Figure 1-2 DB2 Setup Launchpad

Click **Next** to begin the process of installing DB2 Enterprise Server in the DB2 Setup Wizard (Figure 1-3).

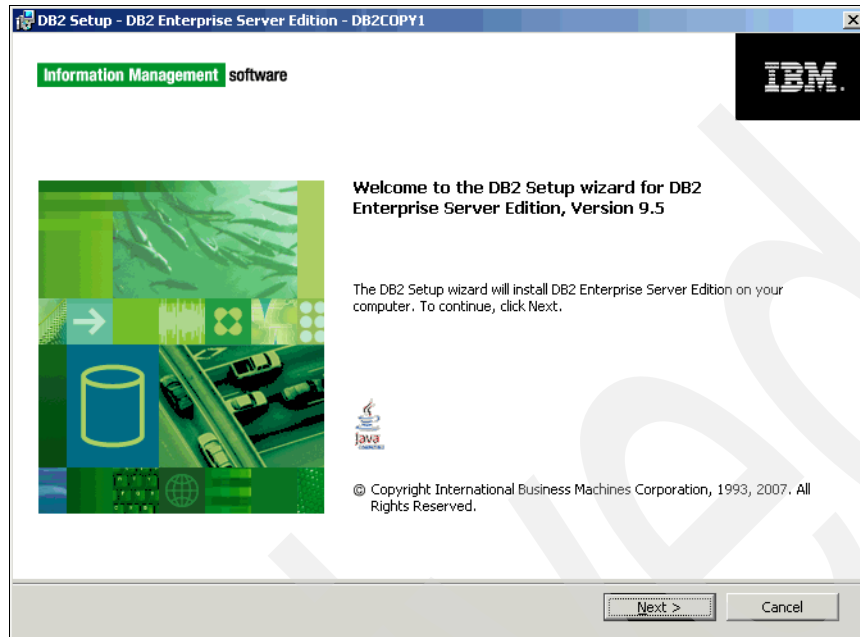


Figure 1-3 Begin DB2 Server installation

2. Click through the install until you get to the Select the installation type page (Figure 1-4). There are three options:
 - Typical
 - Compact
 - Custom

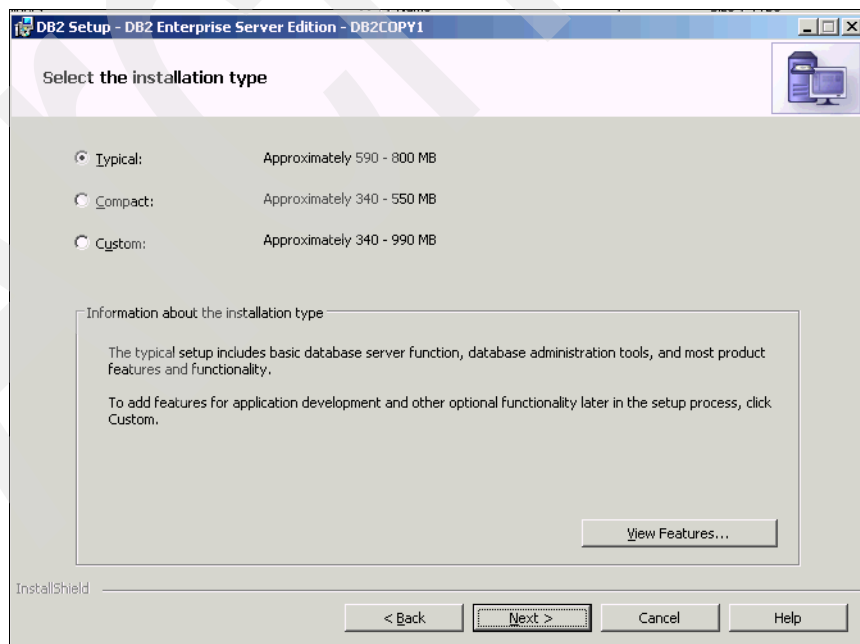


Figure 1-4 Installation type for DB2 Server

Select the installation type that best suits your needs. Select **Next** to continue to the “Select the installation, response file creation, or both” page (Figure 1-5). Choose to install DB2 on this computer. When finished, click **Next**.

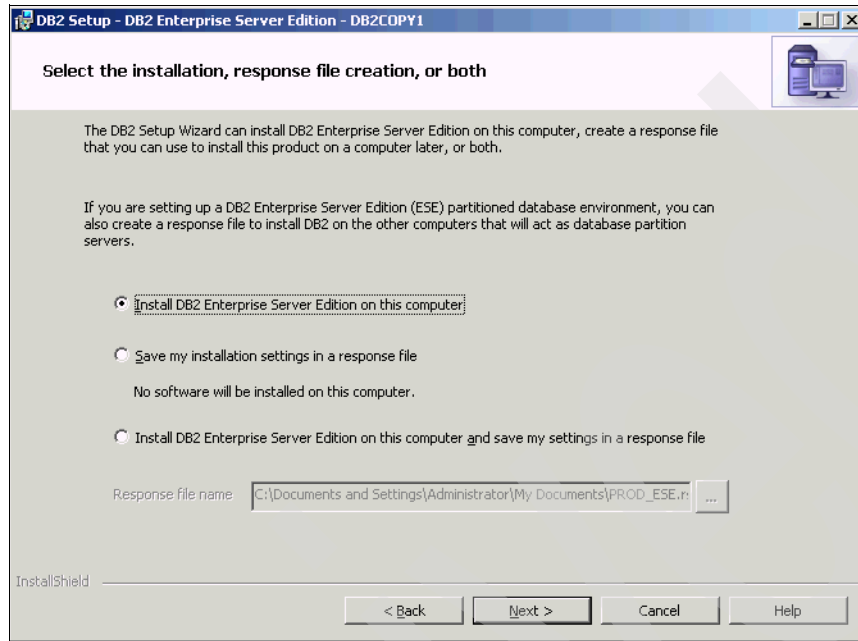


Figure 1-5 Select the installation or response file creation for DB2

3. On the Select the installation folder page, select the install location (Figure 1-6). Click **Change** to select a different folder or type a directory. When finished, click **Next**.

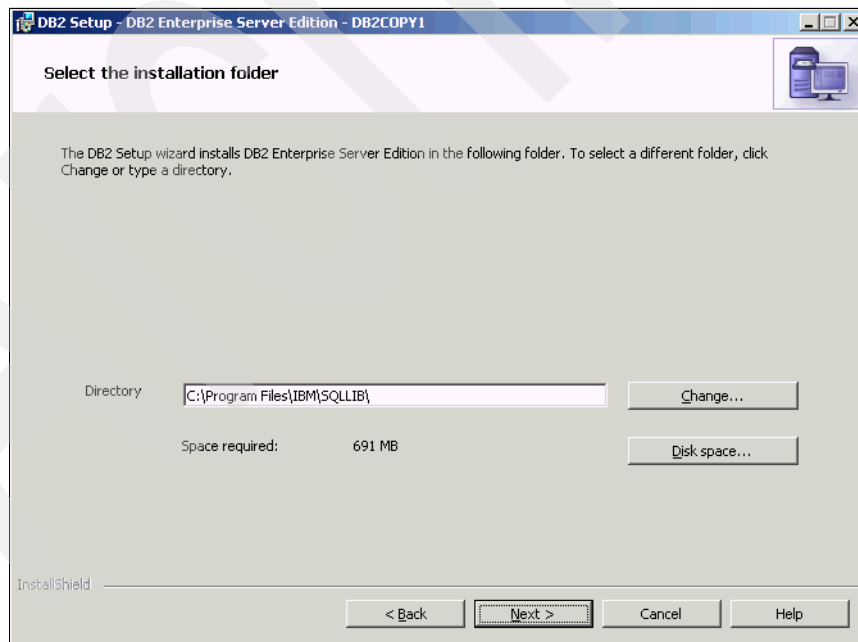


Figure 1-6 Installation folder

4. On the Set user information for the DB2 Administrator Server page (Figure 1-7), define a local DB admin account and specify a password. This creates an operating system account either locally or in a Domain Controller if you specify a domain. A local account is sufficient in this case. When finished, click **Next**.

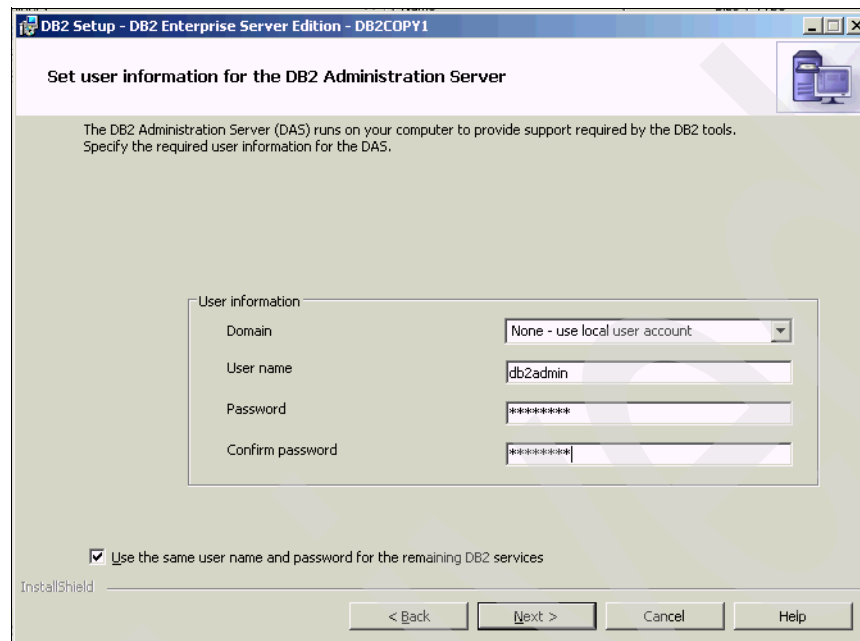


Figure 1-7 Set user information for DB2 Administration Server

5. On the Set up a DB2 instance page (Figure 1-8), select the option to create a default DB2 instance. When finished, click **Next**.

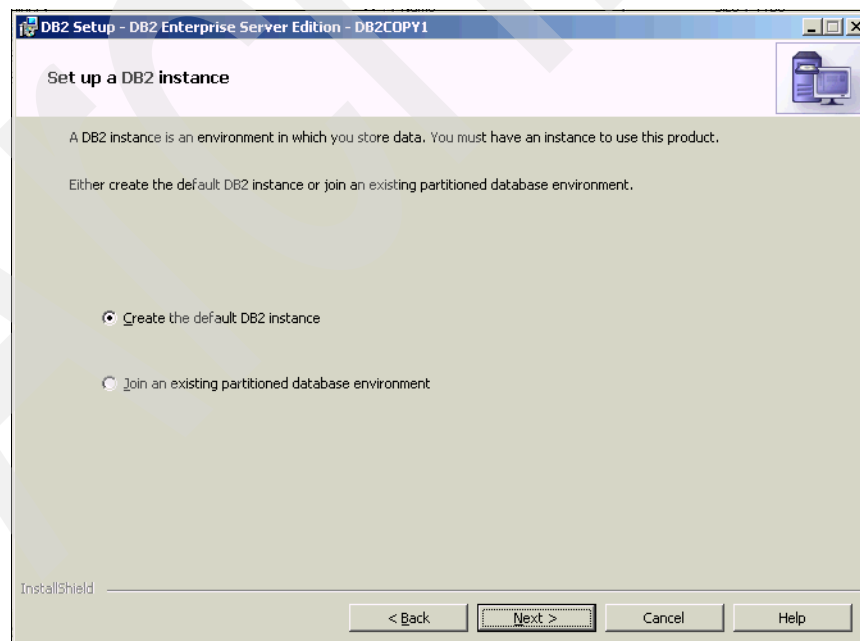


Figure 1-8 Creating a DB2 instance

6. On the Set up partitioning options for the default DB2 instance page (Figure 1-9), select **Single partition instance**. When finished, click **Next**.

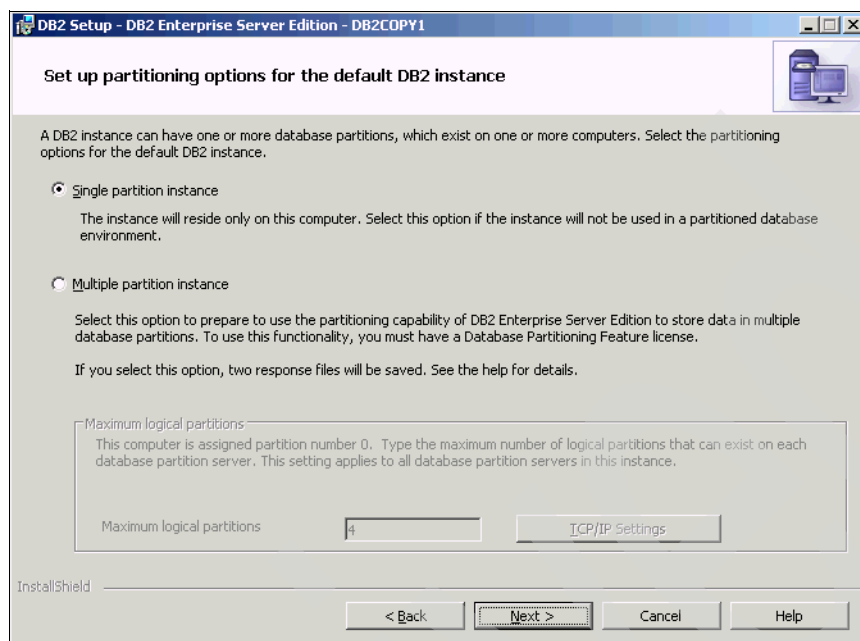


Figure 1-9 Partitioning options for DB2 instance

7. On the Configure DB2 instances page (Figure 1-10), you are presented with the single default (DB2) instance. You do not have to specify the configuration options for the default instance. When finished, click **Next**.

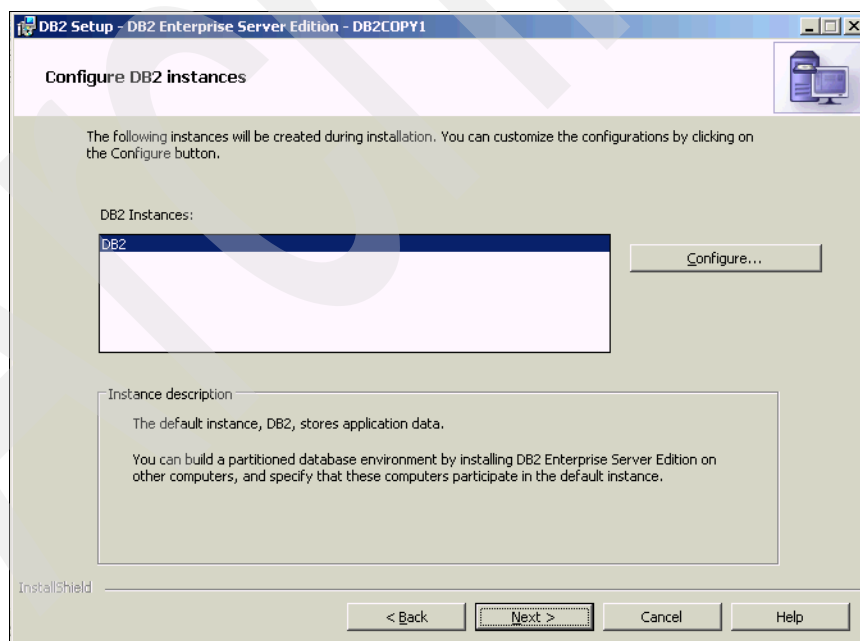


Figure 1-10 Configure DB2 instance

8. On the Prepare the DB2 tools catalog page (Figure 1-11), you do not need a DB2 tools catalog. When finished, click **Next**.

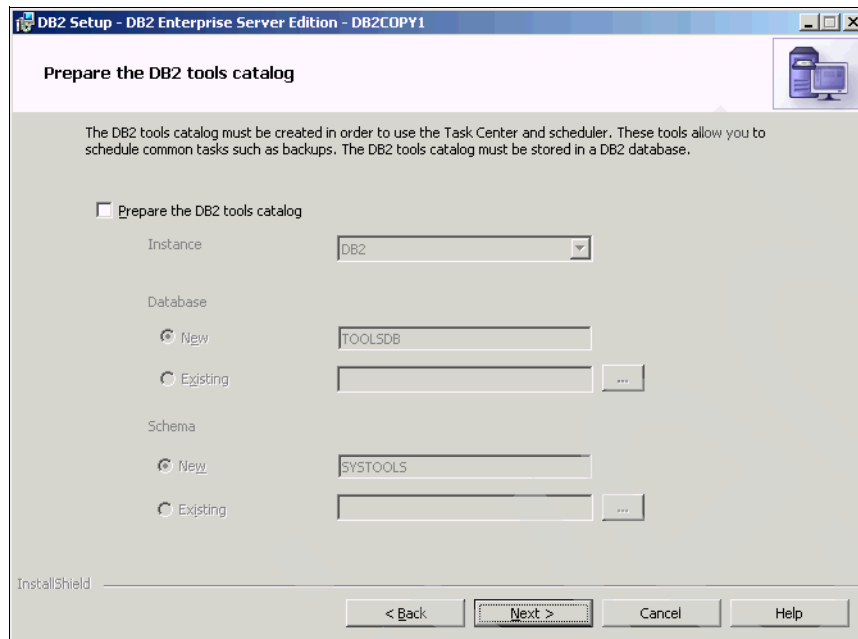


Figure 1-11 DB2 tools catalog

9. On the Set up notifications page (Figure 1-12), you do not need to set up notifications. When finished, click **Next**.

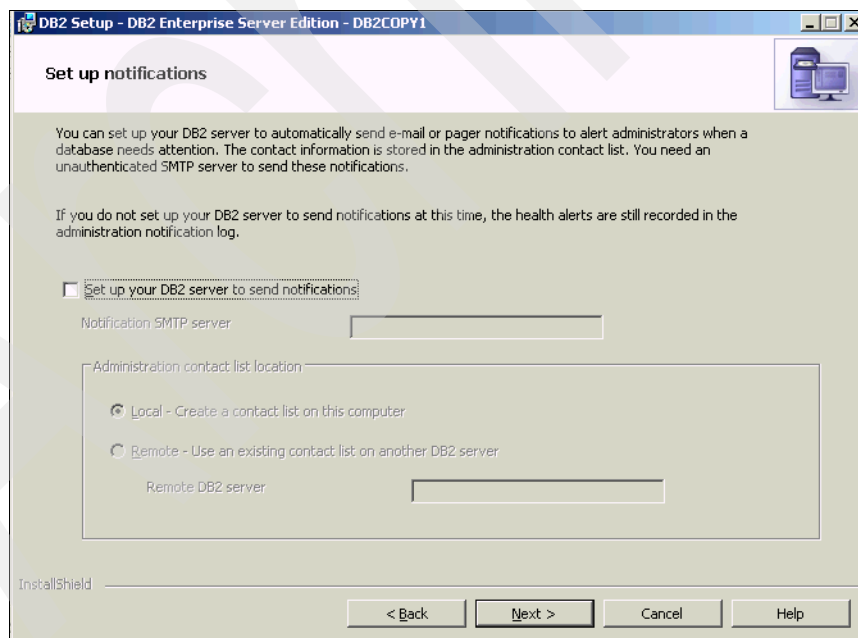


Figure 1-12 Notifications

10. On the Enable operating system security for DB2 objects page (Figure 1-13), enable the operating system security for the database server and accept the defaults. When finished, click **Next**.

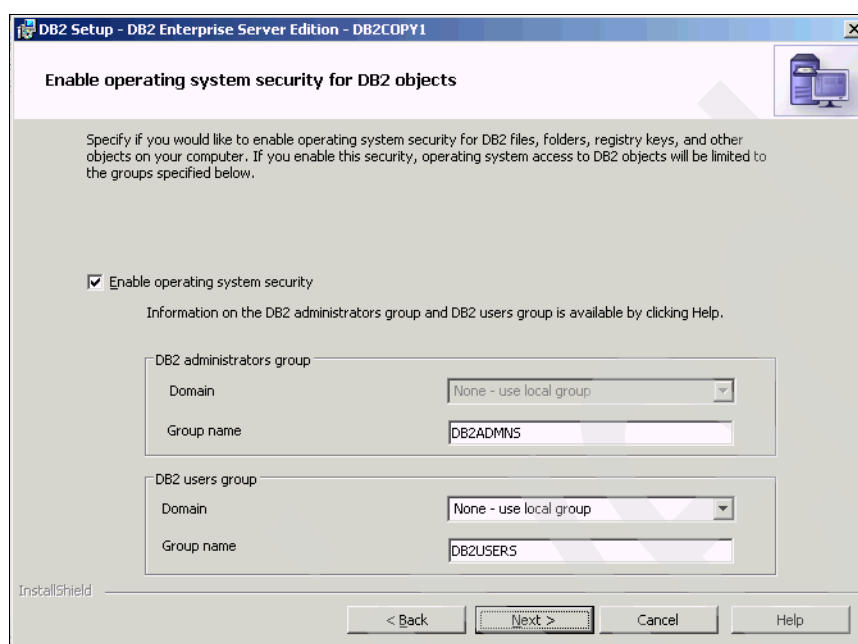


Figure 1-13 Enable operating system security for DB2 objects

11. On the Start copying files page (Figure 1-14), verify the settings on the Start copying files page and click **Install**.

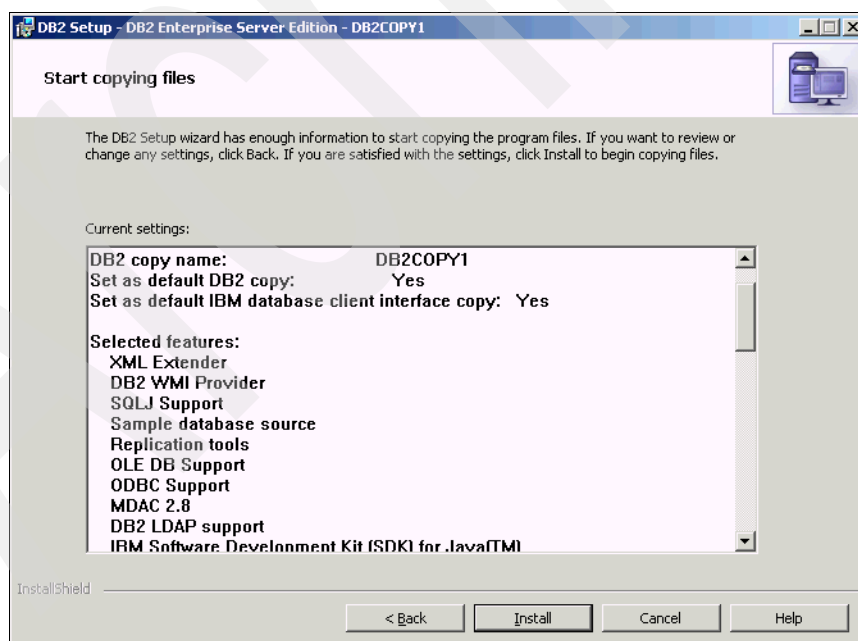


Figure 1-14 Review DB2 installation settings

12. The Setup is complete page displays upon the completion of the install (Figure 1-15). Note the port number. It is 50000 by default. Click **Next** to complete the install and exit the installer.

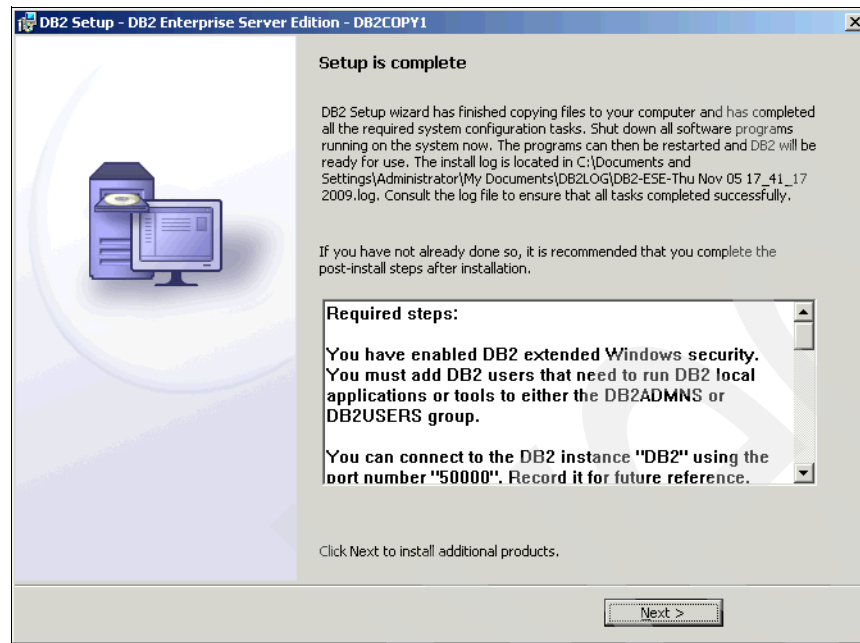


Figure 1-15 Setup complete confirmation

The DB2 server installation is now complete.

Note: There might be a slightly different page for 9.5 than for 9.7. Fundamentally, both are the same and are considered standard. There are a few key differences when creating a database (8 K blocksize, UTF-8) that should be highlighted. There are different installation media for DB2 9.5 or 9.7. Some unpack the installation package, some need to be unpacked manually, while for some you might need to run setup.exe. See the *IBM DB2 Server Installation Guide* from the respective version for the appropriate installation steps. On 9.7, the First Steps dialog displays automatically. On the First Steps dialog there is a Create a Database button. This does not let you specify the special settings the IMS DB needs. Close the First Steps dialog and create a database as per the following section.

1.1.2 Creating a database

After the DB2 Server is installed, create the IMS database using either the DB2 Control Centre UI (start menu) or by entering the appropriate commands in the command-line processor (start menu). The steps are:

1. In the Control Center (Figure 1-16), select the **All Databases** entry in the tree and right-click **Create Database**. We are creating a Standard database. You can also use the **Create New Database** link in the lower-right pane.

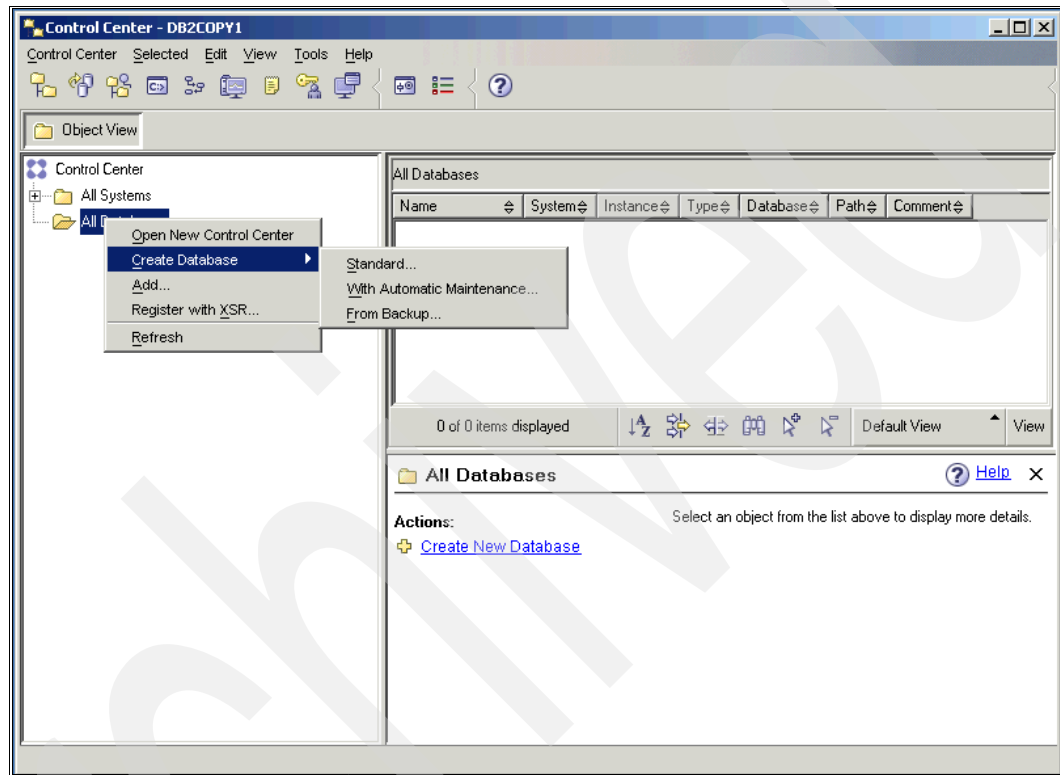
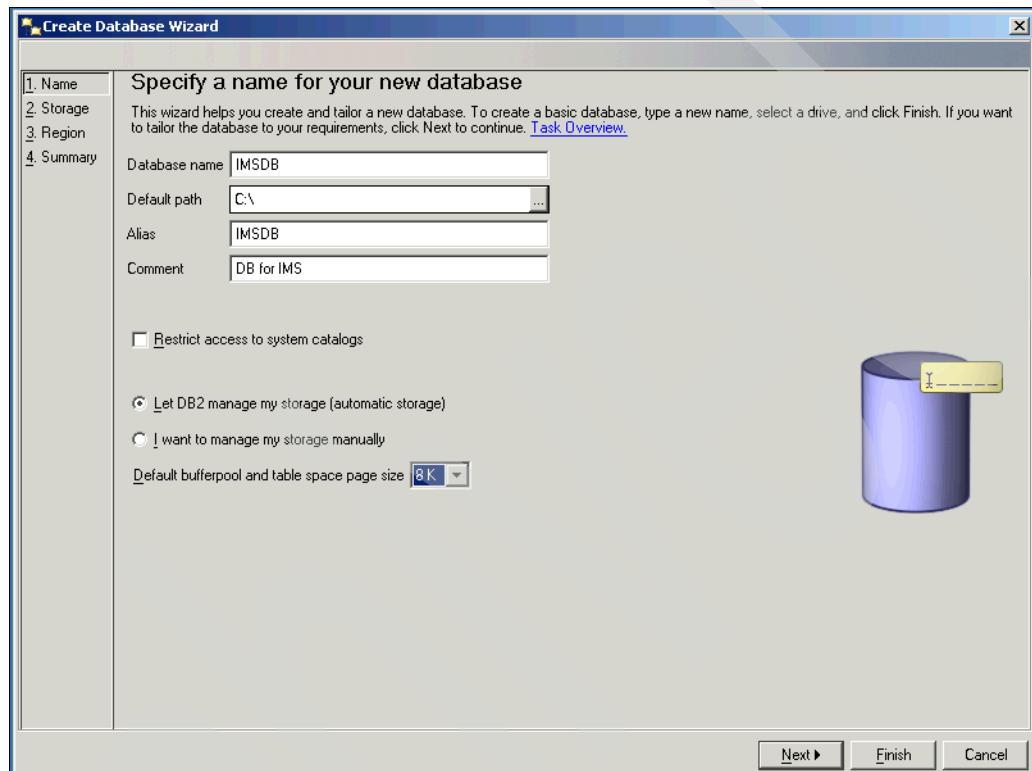


Figure 1-16 Create a new database

2. On the Specify a name for your new database page (Figure 1-17), provide a database name, alias, and comment. Only the name is required.

Note: It is important that the buffer pool and table space page size is set to 8 K (the default is 4 K).



The image shows a screenshot of the 'Create Database Wizard' window. The title bar reads 'Create Database Wizard'. On the left, there is a vertical list of steps: 1. Name, 2. Storage, 3. Region, and 4. Summary. The 'Name' step is currently selected. The main area of the window is titled 'Specify a name for your new database'. Below this title, there is a paragraph of text: 'This wizard helps you create and tailor a new database. To create a basic database, type a new name, select a drive, and click Finish. If you want to tailor the database to your requirements, click Next to continue. [Task Overview](#).' Below the text are four input fields: 'Database name' with the value 'IMSDb', 'Default path' with the value 'C:\', 'Alias' with the value 'IMSDb', and 'Comment' with the value 'DB for IMS'. Below these fields are three radio button options: 'Restrict access to system catalogs' (unchecked), 'Let DB2 manage my storage (automatic storage)' (checked), and 'I want to manage my storage manually' (unchecked). Below the radio buttons is a label 'Default bufferpool and table space page size' followed by a dropdown menu showing '8K'. On the right side of the window, there is a 3D cylinder icon representing a database. At the bottom right, there are three buttons: 'Next >', 'Finish', and 'Cancel'.

Figure 1-17 New name for the database

The following figures show the page for the Create New Database wizard. On the first page (Name) you can specify the database name. Pick the name for the database (such as IMSDB). Click **Next** to continue to the Storage page (Figure 1-18). You can accept the defaults.

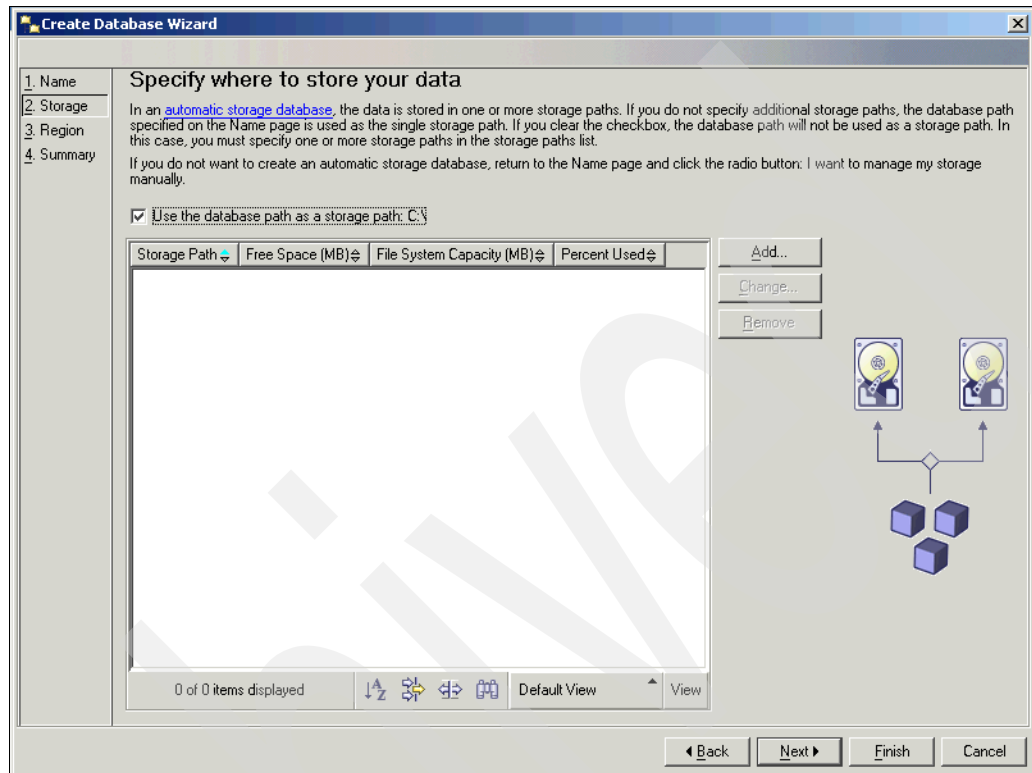


Figure 1-18 Specify location to store data

3. Click **Next** to continue to the Region page (Figure 1-19). On this page configure the code set to UTF-8 (this is not the default). When finished, click **Next** to go to the Summary page. The last page of the wizard is the summary page. Review the options, and click **Finish** to create the database.

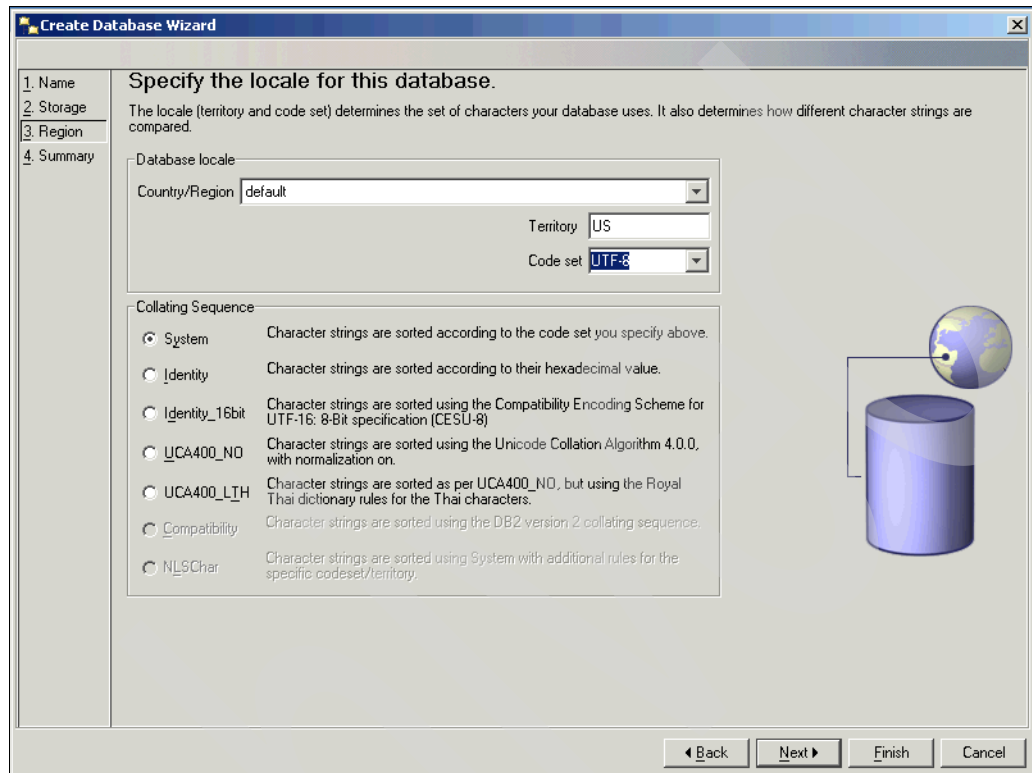


Figure 1-19 Locale for database

You have created a database.

1.1.3 Creating a DB2 user

Next you have to create a database owner that the IMS Server will use to create the schema and load data. Create an operating system user (who can be local) and grant him administrative privileges (member of the local administrators group).

In the DB2 Control Center:

1. Browse to the newly created database (previous section).
2. Click **User and Group Objects**.
3. Right-click **DB Users** and click **Add**.
4. Specify the administrator user that you just created.
5. On the Authorities page, check the **Connect to database** check box, the **Create tables** check box, and the **Create packages** check box.

You can also do this using an SQL statement in the command-line processor.

This completes the database preparation for the IMS Server.

1.2 IBM WebSphere Application Server

This section details the installation and configuration of the various middleware components and IMS itself.

1.2.1 Installing WebSphere Application Server 7.0

WebSphere® Application Server 7.0 normally comes on three CD images: the base install CD and two supplemental CDs (Supplemental CD 1 and Supplemental CD 2).

Note: Passport Advantage® users have easy access to software upgrades. For more information see:

<http://www.ibm.com/software/howtobuy/passportadvantage/>

Make sure that the installation user has the following permissions:

- ▶ Act as part of the operating system
- ▶ Log on as a service

Click **Control Panel** → **Administrative Tools** → **Local Security Policy** → **Local Policies** → **User Rights Assignments**.

Below are the steps for installing WebSphere Application Server 7.0. Use C1G2GML or the Tivoli Access Manager for Enterprise Single Sign-On 32-bit assembly pack.

1. Start the launchpad from the installation CD. On the WebSphere Application Server launchpad (Figure 1-20), select **WebSphere Application Server Installation** from the navigation list on the left. Click the **Launch the installation wizard for WebSphere Application Server** link to install WebSphere Application Server using an installation wizard.

Note: The following figures only show the exceptional information. The standard steps, such as licence agreement, have been skipped. You can install the sample applications if you like, but they are not required for Tivoli Access Manager for Enterprise Single Sign-On.

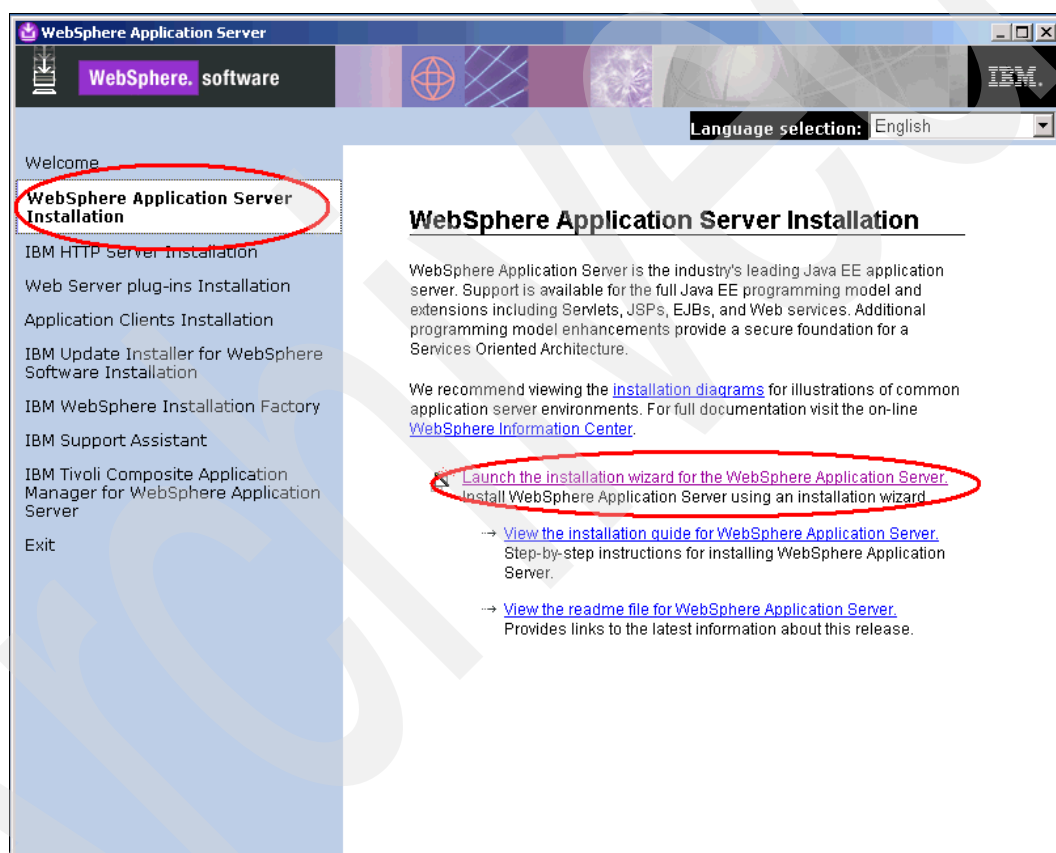


Figure 1-20 WebSphere Application Server Launchpad

2. In the installation wizard, click through the standard pages until the WebSphere Application Server Environments page is displayed (Figure 1-21). Select **Application server** as the type of WebSphere Application Server environment to install for a stand-alone WebSphere Application Server single-server image. When finished, click **Next**.

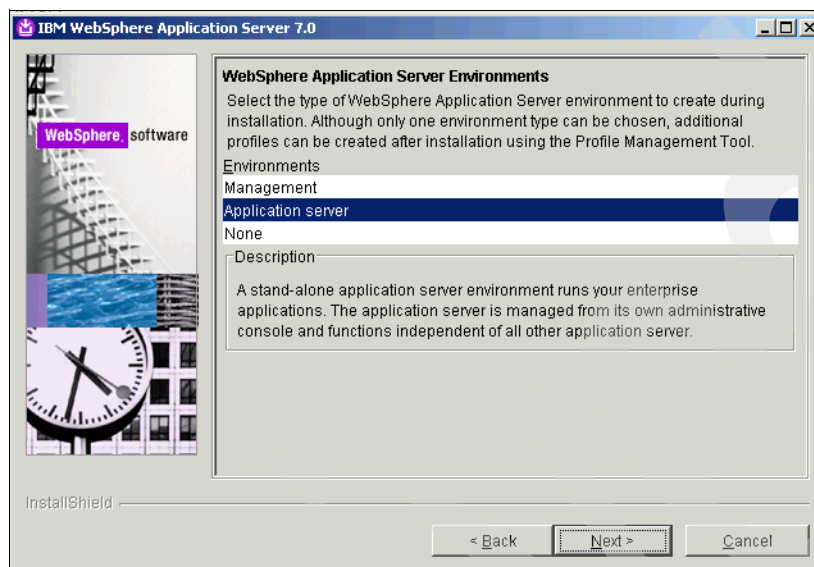


Figure 1-21 Stand-alone WebSphere Application Server environment

3. Continue until you see the Enable Administrative Security page (Figure 1-22). Enable administrative security (the user name is WebSphere Application Server admin account that you want created in WebSphere Application Server, not an operating system account). Input a WebSphere Application Server administrator account user name of your preference. Enter a password for the WebSphere Application Server administrator account and re-enter the password for confirmation. This enforces login to the WebSphere Application Server Integrated Solutions Console (ISC) later on. When finished, click **Next**.

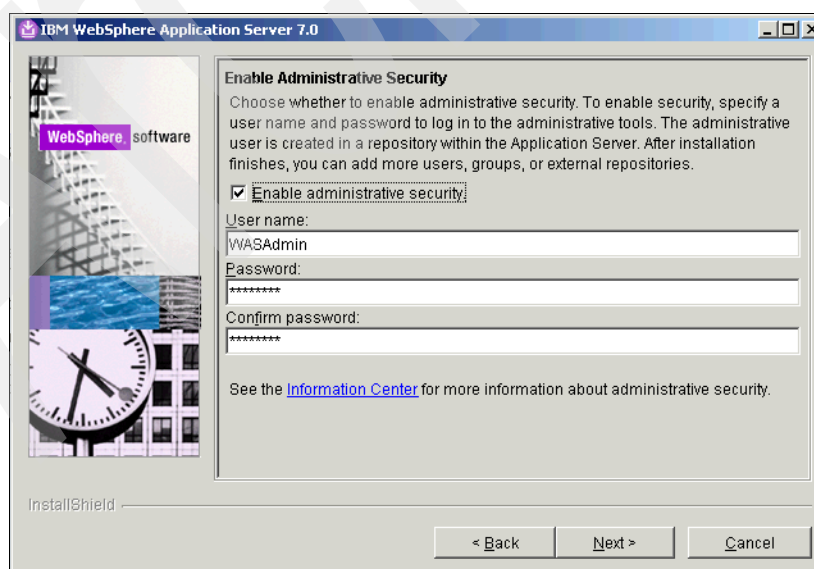


Figure 1-22 Enabling Administrative Security

4. Continue to click **Next** until the Installation Summary page displays (Figure 1-23). Check the settings and click **Next** to complete the installation.

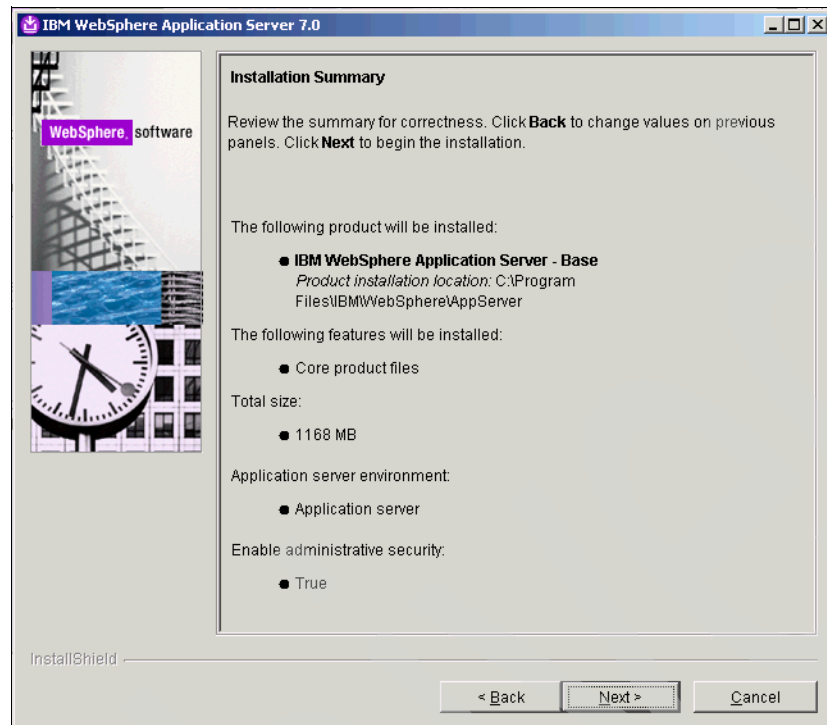


Figure 1-23 Installation Summary

5. When WebSphere Application Server is installed, the First steps page displays (Figure 1-24). Run the Installation verification to confirm it has been installed and configured correctly. If the installation is a success, the installation verification confirmation produces output like that shown in Figure 1-25 on page 21.

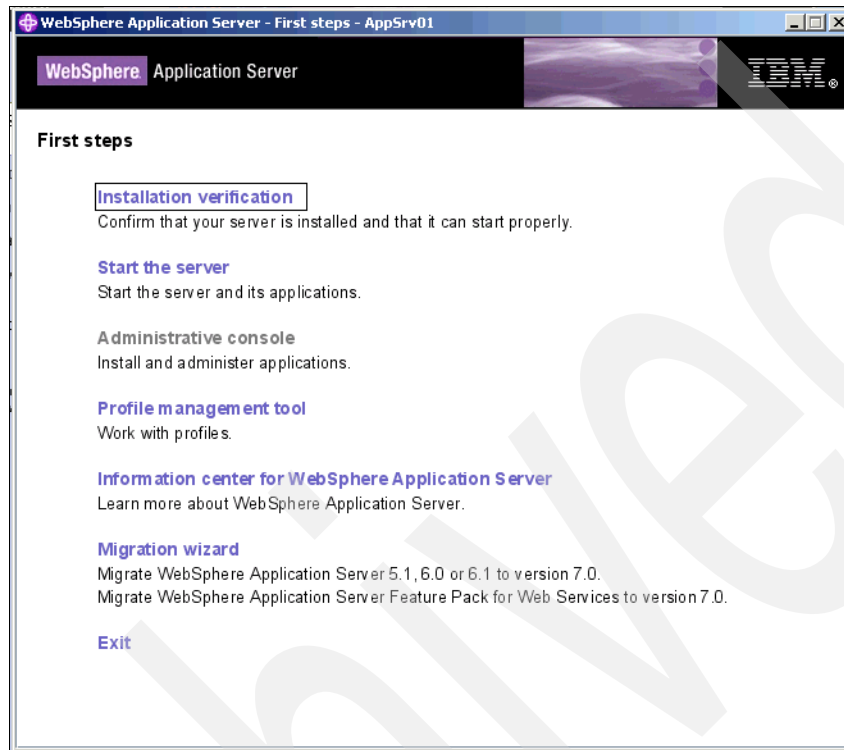
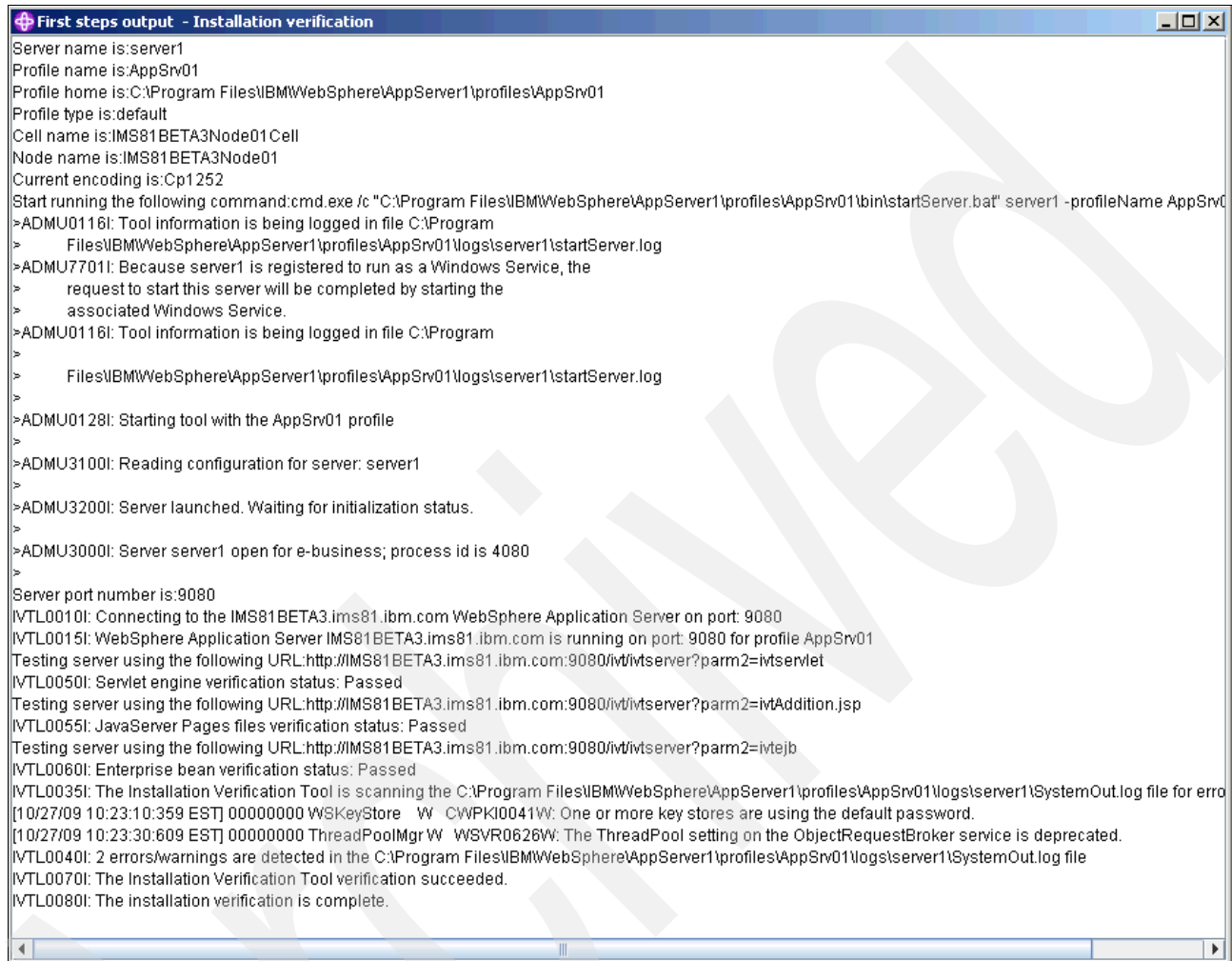


Figure 1-24 First Steps options

6. To confirm a successful WebSphere Application Server installation, check for the last two lines ...verification succeeded and ...verification is complete and look for any errors. If you do not see any errors, WebSphere Application Server 7.0.0 is installed correctly and is ready for fix pack installation.



```
First steps output - Installation verification
Server name is:server1
Profile name is:AppSrv01
Profile home is:C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01
Profile type is:default
Cell name is:IMS81BETA3Node01 Cell
Node name is:IMS81BETA3Node01
Current encoding is:Cp1252
Start running the following command:cmd.exe /c "C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\startServer.bat" server1 -profileName AppSrv01
>ADMU0116I: Tool information is being logged in file C:\Program
>   Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>ADMU7701I: Because server1 is registered to run as a Windows Service, the
>   request to start this server will be completed by starting the
>   associated Windows Service.
>ADMU0116I: Tool information is being logged in file C:\Program
>   Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\startServer.log
>ADMU0128I: Starting tool with the AppSrv01 profile
>ADMU3100I: Reading configuration for server: server1
>ADMU3200I: Server launched. Waiting for initialization status.
>ADMU3000I: Server server1 open for e-business; process id is 4080
>
Server port number is:9080
IVTL0010I: Connecting to the IMS81BETA3.ims81.ibm.com WebSphere Application Server on port: 9080
IVTL0015I: WebSphere Application Server IMS81BETA3.ims81.ibm.com is running on port: 9080 for profile AppSrv01
Testing server using the following URL:http://IMS81BETA3.ims81.ibm.com:9080/ivt/ivtserver?parm2=ivtServlet
IVTL0050I: Servlet engine verification status: Passed
Testing server using the following URL:http://IMS81BETA3.ims81.ibm.com:9080/ivt/ivtserver?parm2=ivtAddition.jsp
IVTL0055I: JavaServer Pages files verification status: Passed
Testing server using the following URL:http://IMS81BETA3.ims81.ibm.com:9080/ivt/ivtserver?parm2=ivtEjb
IVTL0060I: Enterprise bean verification status: Passed
IVTL0035I: The Installation Verification Tool is scanning the C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log file for errors
[10/27/09 10:23:10:359 EST] 00000000 WSKKeyStore W WCPKJ0041W: One or more key stores are using the default password.
[10/27/09 10:23:30:609 EST] 00000000 ThreadPooMgr W WSVR0626W: The ThreadPoo setting on the ObjectRequestBroker service is deprecated.
IVTL0040I: 2 errors/warnings are detected in the C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\logs\server1\SystemOut.log file
IVTL0070I: The Installation Verification Tool verification succeeded.
IVTL0080I: The installation verification is complete.
```

Figure 1-25 Installation verification

Note: Do not install the IBM HTTP Server (IHS) at this point. If you install the IBM HTTP Server before installing the Tivoli Access Manager for Enterprise Single Sign-On IMS component, there will be no IMS definitions configured to the IBM HTTP Server. As a result, you need to regenerate the WebSphere Application Server plug-in later if the IBM HTTP Server were to be installed before Tivoli Access Manager for Enterprise Single Sign-On IMS.

7. Stop WebSphere Application Server.

1.2.2 Installing IBM Update Installer for WebSphere software installation

The IBM Update Installer for WebSphere software installation is required to install WebSphere Application Server, HTTP Server, and Tivoli Access Manager for Enterprise Single Sign-On IMS fix packs.

The Tivoli Access Manager for Enterprise Single Sign-On IMS 8.x fix pack installations require the IBM Update Installer to be at 7.0.0.1 or later. If you are planning on installing the IMS fix packs, download and install the 7.0.0.1 (or later) Update Installer here:

<http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg21205991#updi70>

Follow the installation instructions provided on the IBM Update Installer support site.

1.2.3 Upgrading WebSphere Application Server

Download the latest fix pack from the WebSphere Application Server support site:

<http://www-01.ibm.com/support/docview.wss?rs=180&uid=swg27004980#ver70>

Use Fix Pack 5 or later.

Follow these steps to upgrade WebSphere Application Server:

1. Ensure that all WebSphere Application Server processes are stopped. To stop WebSphere Application Server on the machine (Figure 1-26), go to **Start → All Programs → IBM WebSphere → Application Server <version> → Profiles → <profile_name> → Stop the server**.

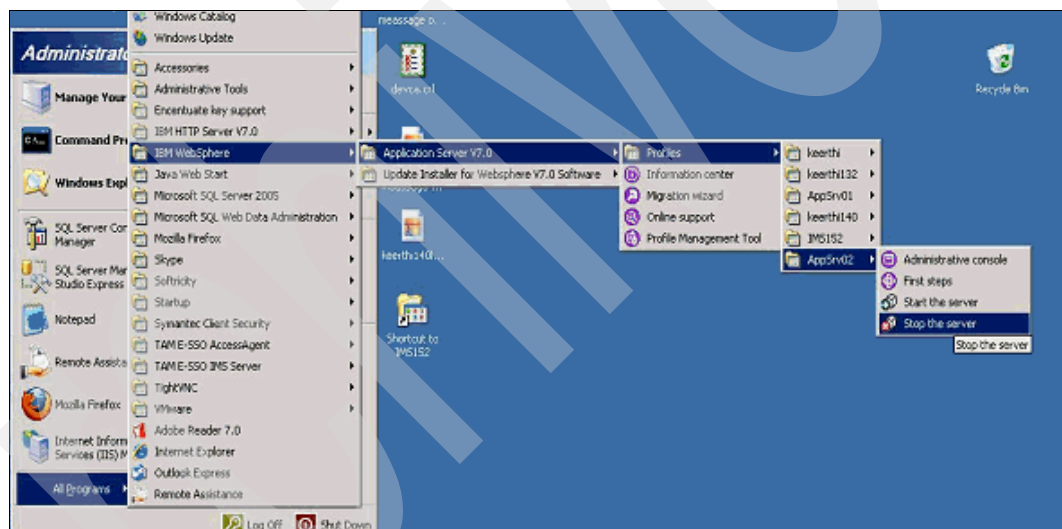


Figure 1-26 Stopping WebSphere Application Server

2. Copy the .pak file into a directory on the local system. This can be the standard directory (C:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance) or one of your choosing.

3. Run the update installer, either after installation or from the Start menu by clicking **All Programs** → **IBM WebSphere** → **Update Installer**. Figure 1-27 presents the interface for when the update installer is started. Click **Next** to proceed with the upgrading process.

Note: On a Windows 2008 server, we found that even though a user was logged in as the administrator, it was necessary to right-click and select **Run as Administrator** for the installs to work correctly.

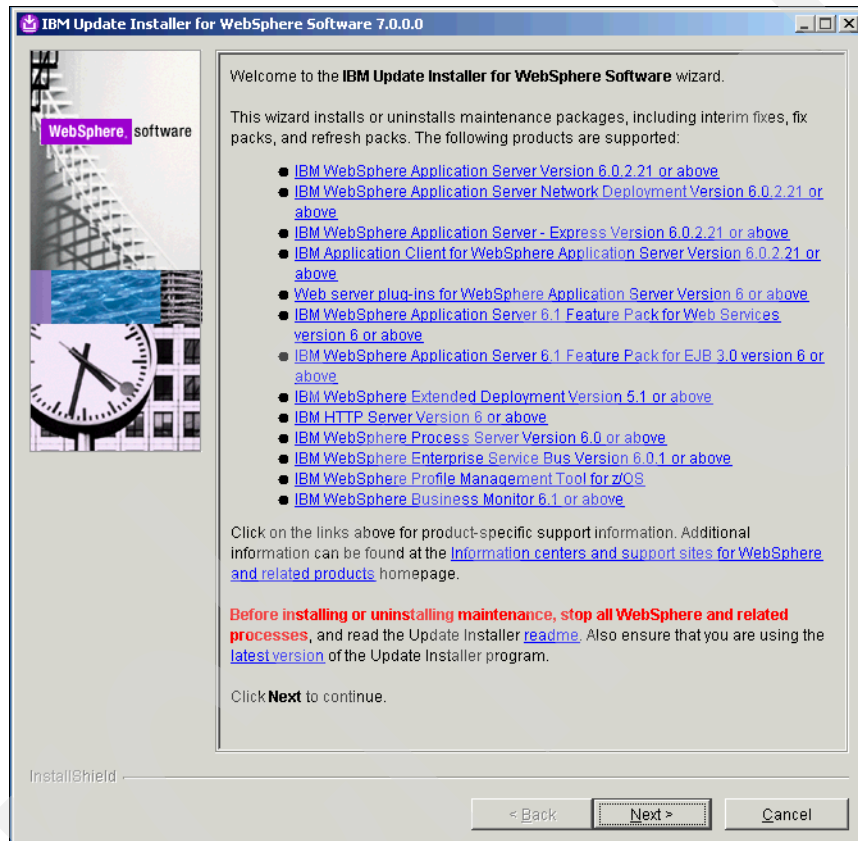


Figure 1-27 IBM Update Installer for WebSphere Software wizard

4. Select which product to update by entering the installation location of the product (Figure 1-28). Select the directory path of the app server for the WebSphere Application Server to update (for example, C:\Program File\IBM\WebSphere\AppServer). When finished, click **Next**.

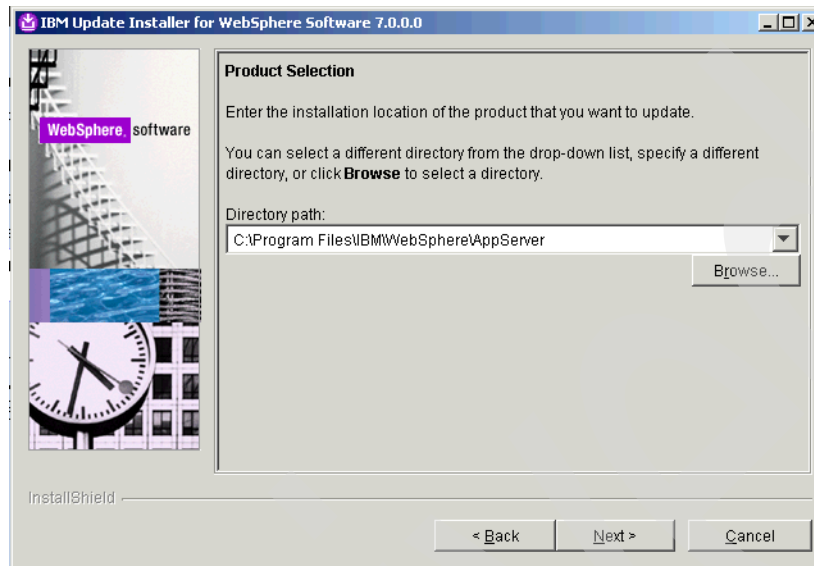


Figure 1-28 Specify installation location of product to be updated for WebSphere Application Server

5. Browse to or specify the location of the fix pack .pak files used in step 1 (Figure 1-29). Ensure that the specified directory path is where the WebSphere Application Server fix pack .pak files are copied into. When finished, click **Next**.

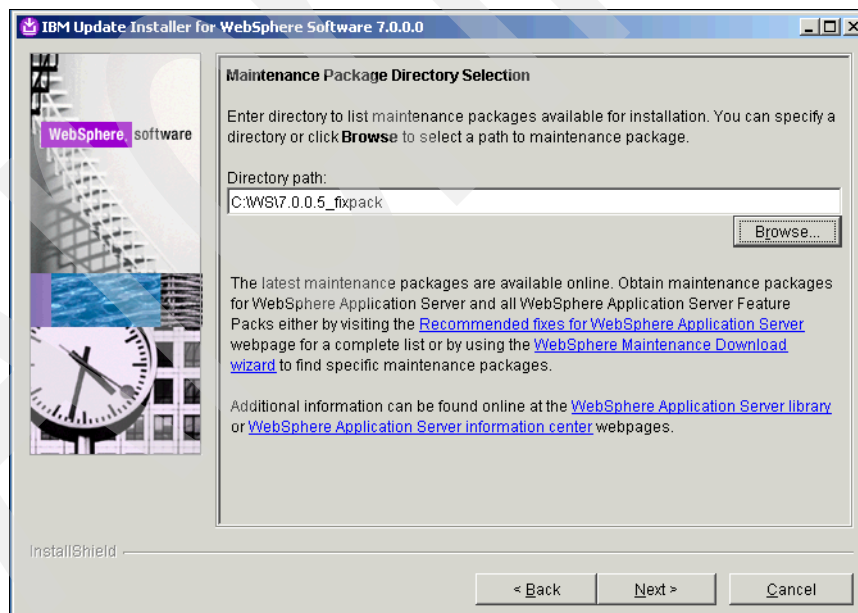


Figure 1-29 Maintenance package location for WebSphere Application Server fix packs

6. Select the check box for the maintenance fix pack packages to install that are relevant to WebSphere Application Server (Figure 1-30).

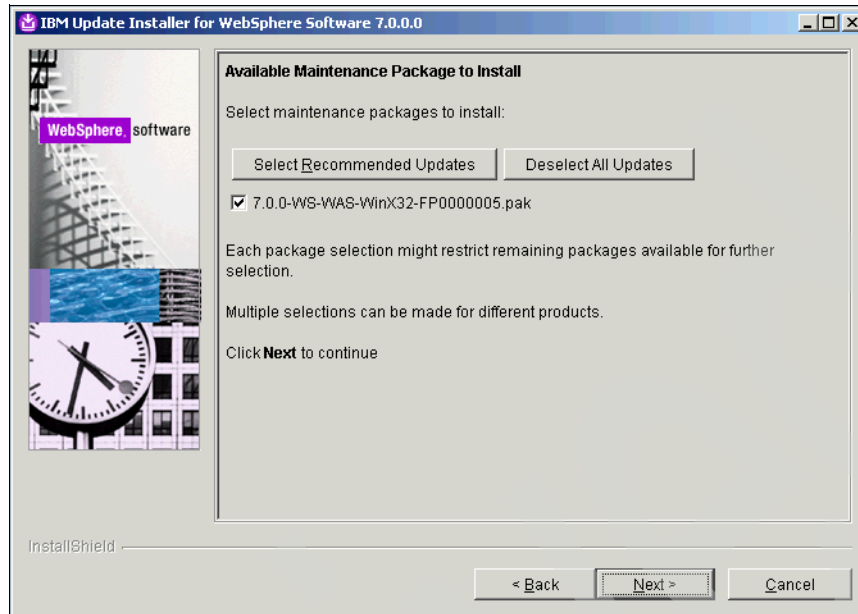


Figure 1-30 Select WebSphere Application Server Maintenance Packages to install

When finished, click **Next** to proceed to the Installation Summary page (Figure 1-31).

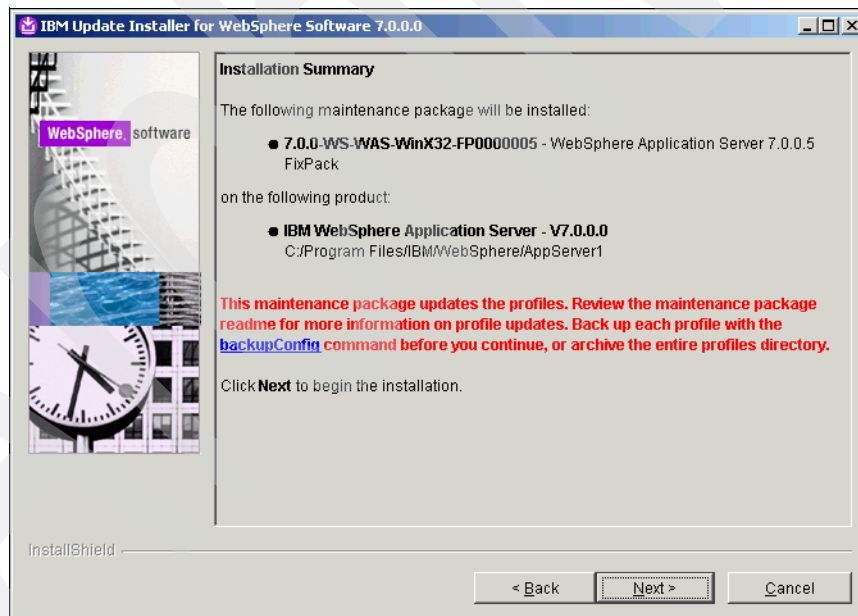


Figure 1-31 Installation Summary for updating WebSphere Application Server

7. Click **Next** to install the fix pack.

Note: Up to this part in the installation process, you can install IBM HTTP Server, and apply the relevant fix packs for IHS. However, do not install and configure the HTTP Server WebSphere Application Server plug-in yet. The IHS install, patches, configuration, and WebSphere Application Server plug-in install/config are covered later.

1.3 IMS Server

This section details the installation of the Tivoli Access Manager for Enterprise Single Sign-On IMS Server (called IMS from now on).

Before proceeding further into this section, ensure that the WebSphere Application Server has been started and is running.

1.3.1 Preparing WebSphere Application Server for Global Application Security

Enable application security before installing the IMS Server into WebSphere Application Server. You might recall that during the WebSphere Application Server installation, the administrative security was enabled.

First, Start WebSphere Application Server. To start WebSphere Application Server on the machine (Figure 1-32 on page 27), go to the Start menu and select **All Programs → IBM WebSphere → Application Server <version> → Profiles → <profile name> → Start the server**.

To enable application security:

1. Select **Start → All Programs → IBM WebSphere → Application Server <version> → Profiles → <profile name> → Administrative console**.
2. On the IBM Integrated Solutions Console (ISC) login page, enter your login credentials (the WebSphere Application Server administration account specified during the WebSphere Application Server install, such as wasadmin), and click **Log in**.
3. From the task list on the left side of the welcome page, click **Security**.
4. Click **Global security**.
5. On the Global security page, select **Enable application security** and click **Apply**.
6. In the Messages box at the top of the page, click **Save**.
7. Restart WebSphere Application Server.

You are now ready to install IMS.

1.3.2 Installing IMS

For installation of the Tivoli Access Manager for Enterprise Single Sign-On IMS Server, the steps are:

1. To begin the installation wizard for the Tivoli Access Manager for Enterprise Single Sign-On IMS Server, run the executable file from the Tivoli Access Manager for Enterprise Single Sign-On installation CD provided, for example, `imsinstaller_8.1.0.0.210.exe`. Figure 1-32 displays the initial startup interface when the Tivoli Access Manager for Enterprise Single Sign-On IMS Server installation begins. Select the language from the drop-down list and click **OK**.



Figure 1-32 Begin to install the IMS Server 8.1

2. Read the software license agreement details and select **I accept the terms in the license agreement** to continue the installation. Click **Next** to continue (Figure 1-33).

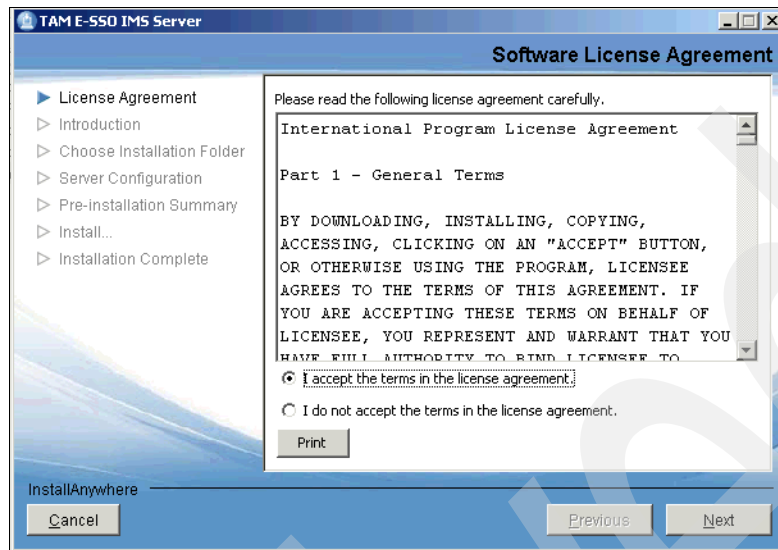


Figure 1-33 Software license agreement details

Click **Next** to proceed to the next page for this installation.

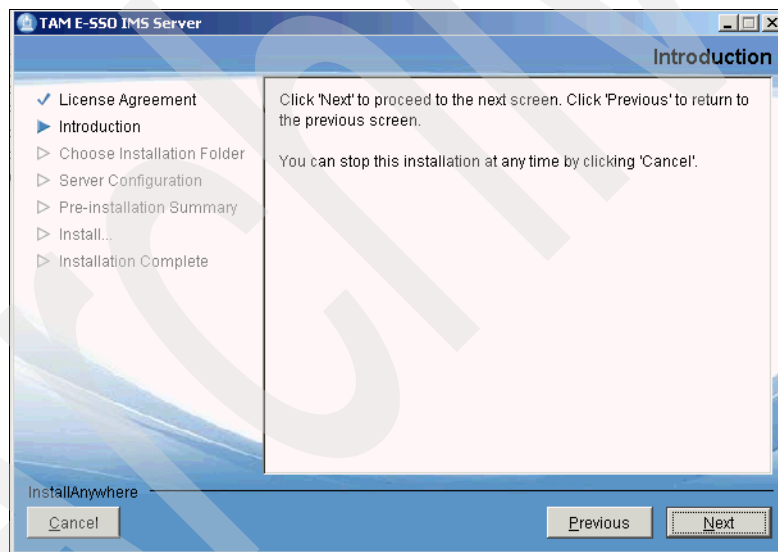


Figure 1-34 Introduction

3. Specify the destination folder for this installer (Figure 1-35). When finished, click **Next**.

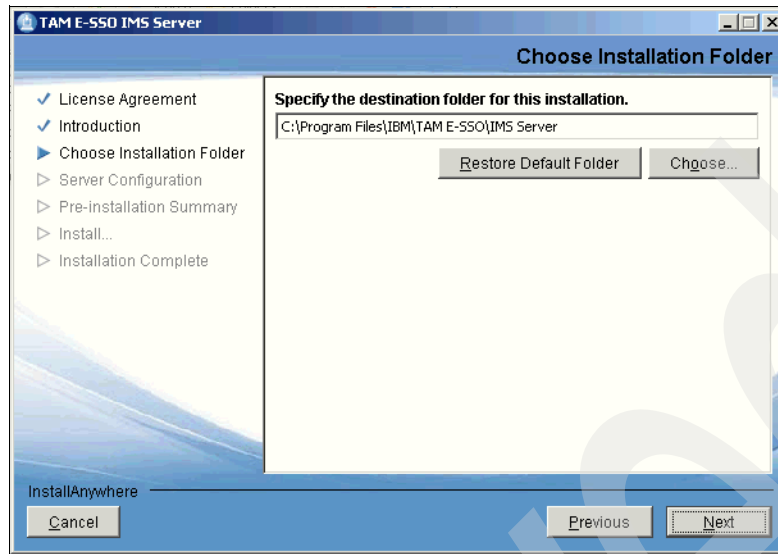


Figure 1-35 Installation destination for the IMS Server

4. Use the installer to deploy the Tivoli Access Manager for Enterprise Single Sign-On IMS Server to WebSphere Application Server (Figure 1-35).
5. The installer gives you the option to defer deployment of the IMS EAR file to WebSphere Application Server. This is on the Server Configuration page. If you choose to not install the application, you need to manually deploy it according to the instructions in the installation guide. Choose **Yes** if you want to install the application. Otherwise, choose **No**. In this example presented, we chose **Yes** (Figure 1-36). When finished, click **Next**.

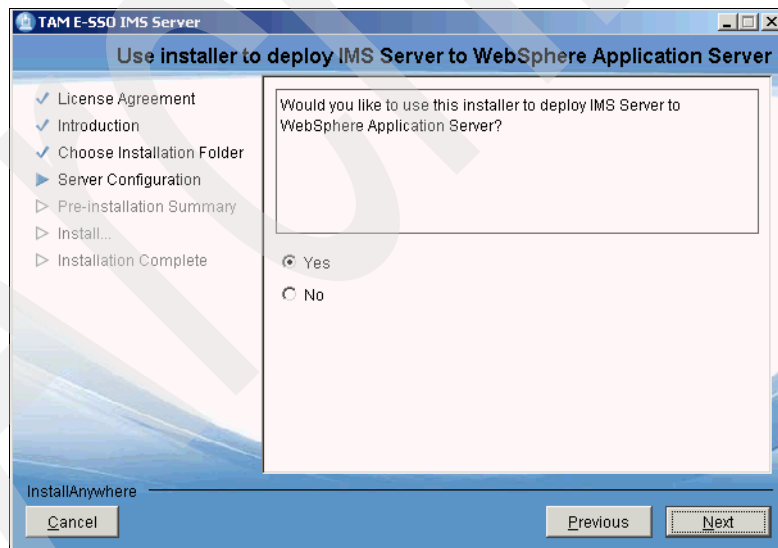


Figure 1-36 Deploy IMS Server to WebSphere Application Server

6. The WebSphere Security page for server configuration asks whether administrative security has been enabled (Figure 1-37). This was done during the WebSphere Application Server install. Note that this is *administrative* security, not application security. This is relevant to the settings made in step 3 in 1.2.1, “Installing WebSphere Application Server 7.0” on page 16. In this example, administration security was enabled in the WebSphere Application Server, hence, **Yes** is selected. Click **Next**.

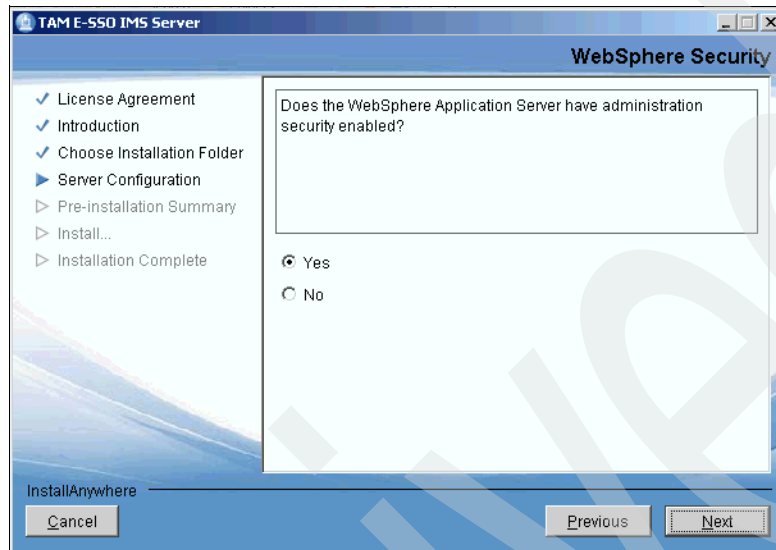


Figure 1-37 Define whether WebSphere Application Server has administration security enabled

7. The next page of the server configuration asks for the administrative user and password and the SSL key store files (Figure 1-38). The administrative user is the one specified during the WebSphere Application Server install in step 3 in 1.2.1, “Installing WebSphere Application Server 7.0” on page 16. For the two SSL trusted keystore files, specify it as the default trust.p12 and key.p12 files. When finished, click **Next**. By default they reside in C:\Program Files\IBM\WebSphere\AppServer\profiles\<profile>\config\cells\<cell>\nodes\<node>. The default password for the trust.p12 and key.p12 files is WebAS.

- Example for trust.p12 file:

C:\Program
Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\IMS81Node01Cell\nodes\IMS81Node01\trust.p12

- Example for key.p12 file:

C:\Program
Files\IBM\WebSphere\AppServer\profiles\AppSrv01\config\cells\IMS81Node01Cell\nodes\IMS81Node01\key.p12

The screenshot shows a window titled "TAM E-SSO IMS Server" with a sub-header "WebSphere Application Server administration security information". On the left is a navigation pane with a tree view containing: "License Agreement" (checked), "Introduction" (checked), "Choose Installation Folder" (checked), "Server Configuration" (selected with a blue arrow), "Pre-Installation Summary", "Install...", and "Installation Complete". The main area contains several input fields: "Administrative user name *" with the text "WASAdmin"; "Administrative password *" with masked characters "*****"; "SSL Trusted Java key store file *" with the path "AppSrv01\config\cells\IMS81Node01Cell\nodes\IMS81Node01\trust.p12" and buttons "Restore Default" and "Choose..."; "SSL Trusted key store password *" with masked characters "*****"; and "SSL Java key store file" with the path "AppSrv01\config\cells\IMS81Node01Cell\nodes\IMS81Node01\key.p12" and buttons "Restore Default" and "Choose...". At the bottom left is a button "Cancel" and at the bottom right are buttons "Previous" and "Next".

Figure 1-38 Administration security information

8. The next page asks for the SOAP port on WebSphere Application Server. Use the default port number, 8880. When finished, click **Next** to proceed with the IMS Server configuration (Figure 1-39). To get the SOAP number, go to <WAS install folder>/profiles/<profile name>/logs/AboutThisProfile.txt.

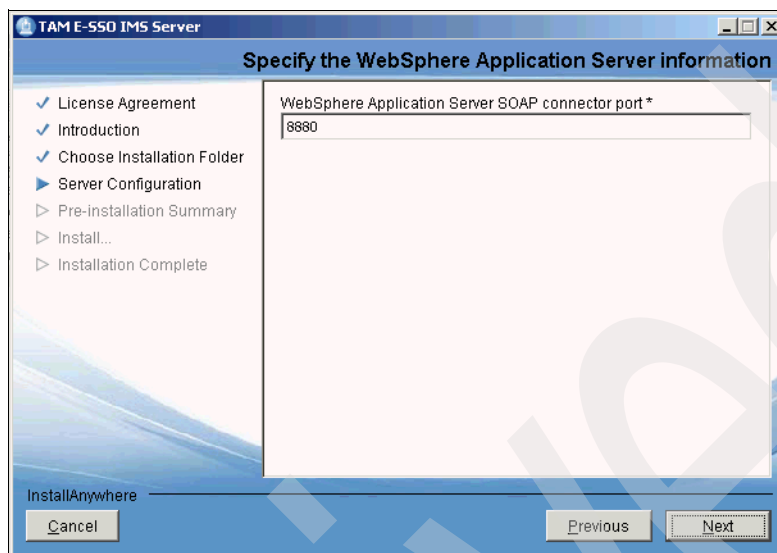


Figure 1-39 SOAP connector port on WebSphere Application Server

When finished, click **Next** to proceed to the Server Configuration page (Figure 1-40), which begins the process of configuring the IMS Server for the system.

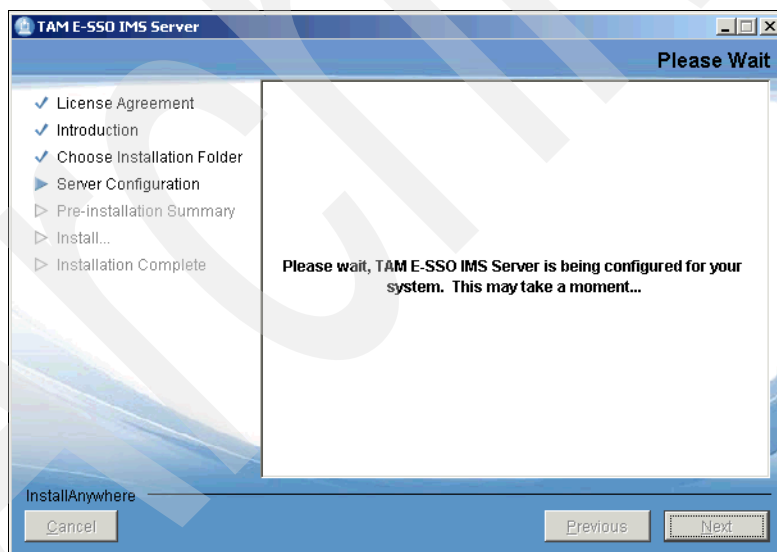


Figure 1-40 Complete IMS Server configuration step

This completes the server configuration steps.

9. When the server configuration step is completed, a pre-installation summary displays for review (Figure 1-41). Click **Install** to continue. This installs the IMS Server onto WebSphere Application Server and configures the base server settings.

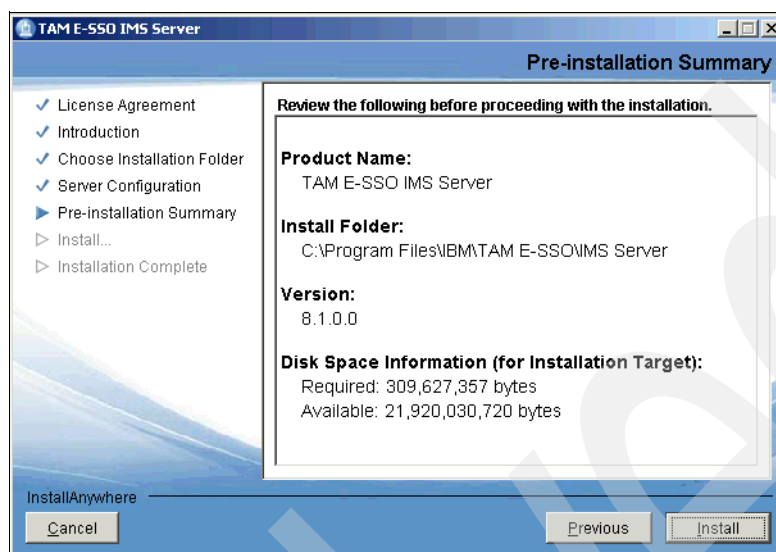


Figure 1-41 Pre-installation Summary of IMS Server

Note: Apply the latest Tivoli Access Manager for Enterprise Single Sign-On IMS fix pack to use Tivoli Access Manager for Enterprise Single Sign-On. Configure the HTTP Server first to front the IMS (next section). Then install the fix pack.

1.3.3 Verifying the IMS Server installation and deployment

After the installation of the IMS Server, check the Tivoli Access Manager for Enterprise Single Sign-On <installationdirectory>/TAM_E-SSO_IMS_Server_InstallLog.log file for critical errors that occurred during the IMS Server installation.

After deploying the IMS Server on the WebSphere Application Server, verify that the deployment was successful with the following steps:

1. Select **Start** → **All Programs** → **IBM WebSphere** → **Application Server v<version>** → **Profiles** → <profile name> → **Administrative console**.
2. On the ISC login page, enter your login credentials.
3. Click **Log in**.
4. Select **Applications** → **Application Types** → **WebSphere enterprise applications**.
5. Verify that **TAM E-SSO IMS** appears on the list of applications.

1.4 HTTP Server and WebSphere Application Server plug-in

After you install the IMS Server, configure the IBM HTTP Server to front the IMS Server. Then configure the IMS Server and modify your enterprise directory settings.

This section details the installation and configuration steps of the IBM HTTP Server and the IBM HTTP Server WebSphere Application Server plug-in.

1.4.1 Installing HTTP Server

If you are not going to run the IHS services by logging in as a local system account, then create a suitable account in the active directory (AD) for the IHS services to run under.

The steps to install the IBM HTTP Server are:

1. Start the launchpad from the installation CD. In the WebSphere Application Server launchpad (Figure 1-41 on page 33), select **IBM HTTP Server Installation** from the navigation list on the left. Click the **Launch the installation wizard for IBM HTTP Server** link to install IBM HTTP Server using the installation wizard. Click **Next** to go through the install (Figure 1-42).
2. Install IBM HTTP Server from the same launchpad used to install WebSphere Application Server (this also includes the WebSphere Application Server plug-in on later CD images).

Note: As with the WebSphere Application Server install, you can accept most defaults. The exceptions are highlighted in the following sections.

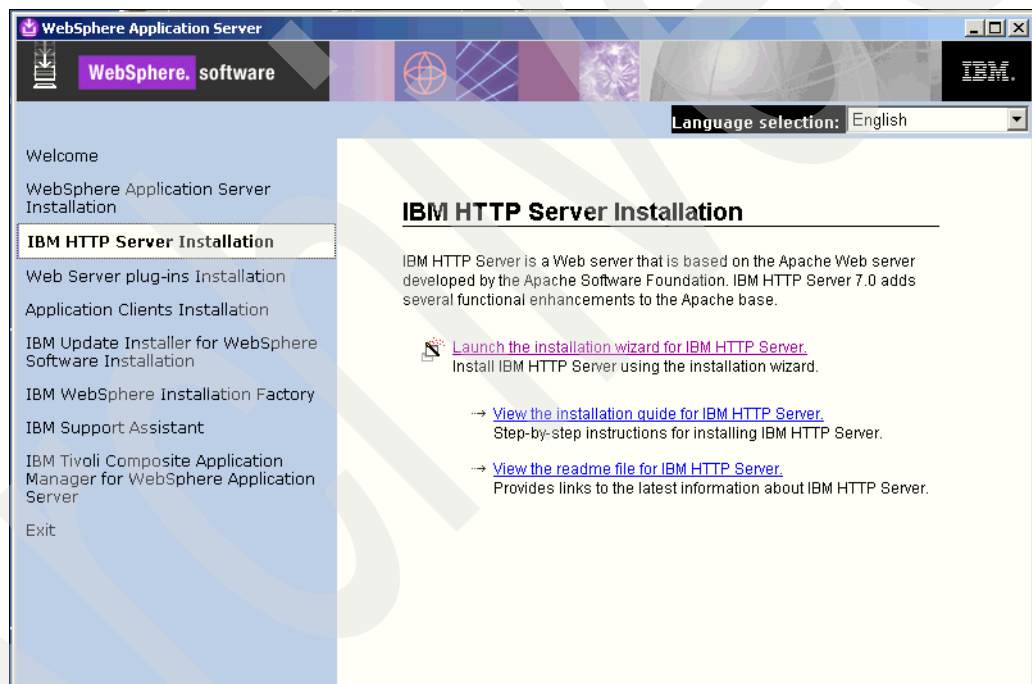


Figure 1-42 IBM HTTP Server Installation

3. Read the software license agreement details and select **I accept the terms in the license agreement** to continue the installation (Figure 1-43).

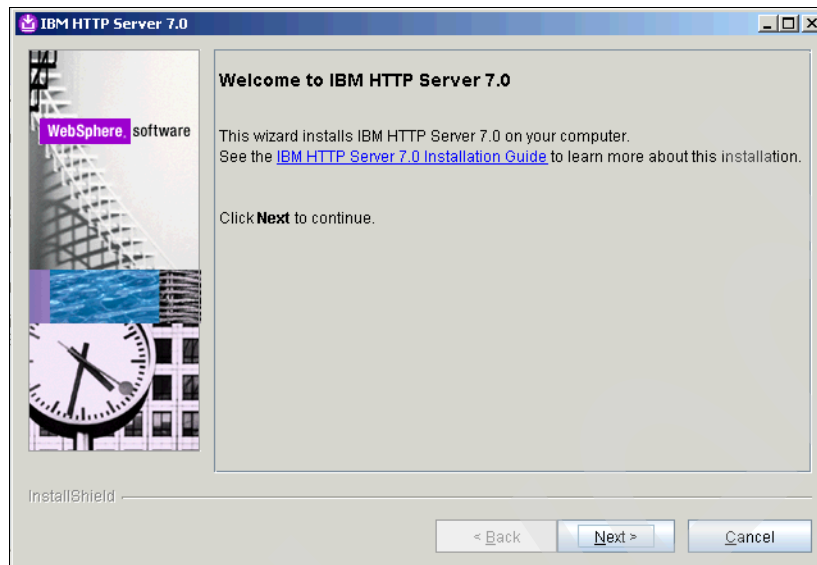


Figure 1-43 Installation wizard for IBM HTTP Server

4. Continue through the license agreement and then click **Next** to proceed with the system prerequisite check on the system (Figure 1-44).

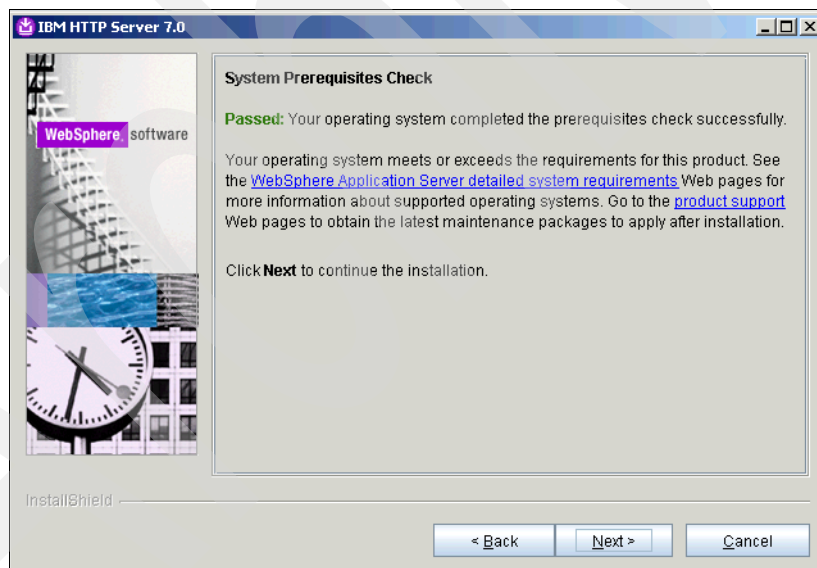


Figure 1-44 System Prerequisite Check for IBM HTTP Server

5. Enter the installation location for installation of the IBM HTTP Server (Figure 1-45). Note the install location, as you will need it when you apply a fix pack in later steps. Click **Next** to continue.

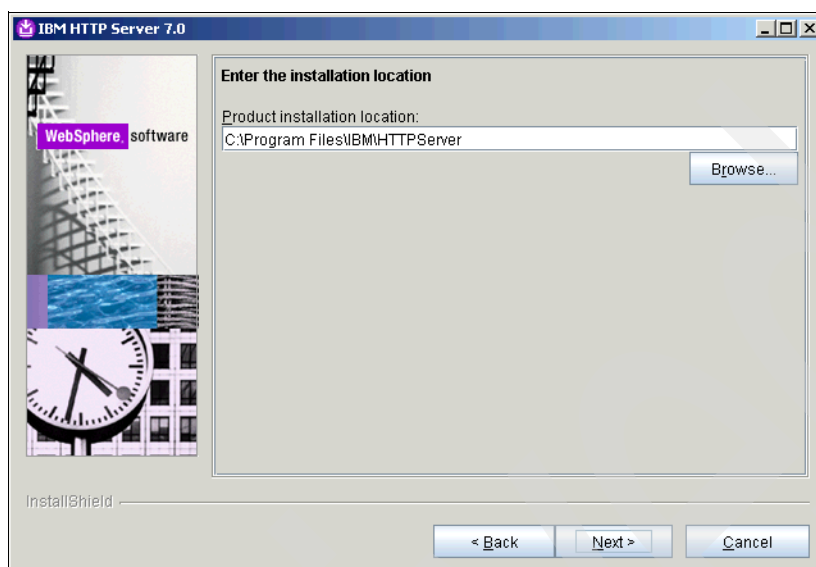


Figure 1-45 IHS installation location

6. Configure the port numbers for IBM HTTP Server Communication (Figure 1-46). Default port numbers will be provided. Use the default ports values, and make sure that no Windows applications (such as IIS) are running to use the same port number or can start before IHS. When finished, click **Next**.

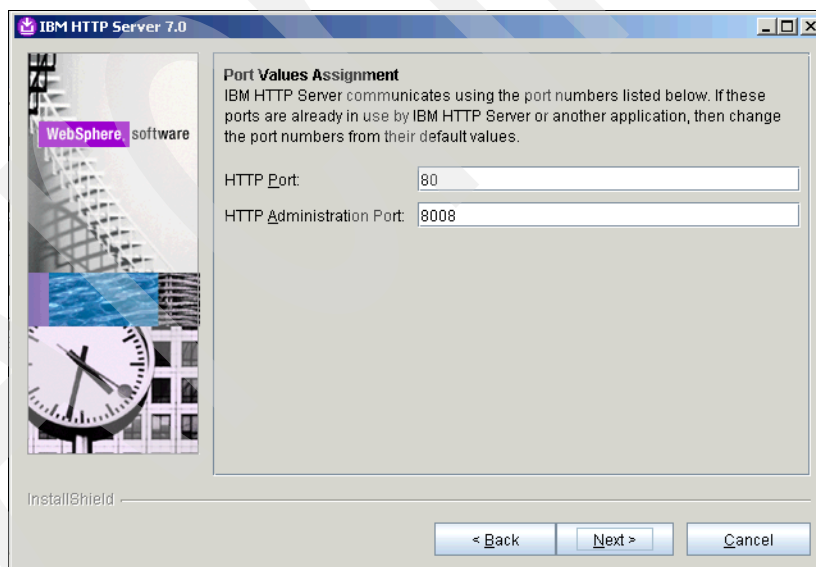


Figure 1-46 Port Value Assignment for IHS

7. Define how Windows starts IHS and the IHS Administrative process. Leave them as Windows services and use the local system account to start them. Click **Next** (Figure 1-47).

Note: This is the minimal administrative involvement option. IHS and the admin service come up when the box displays.

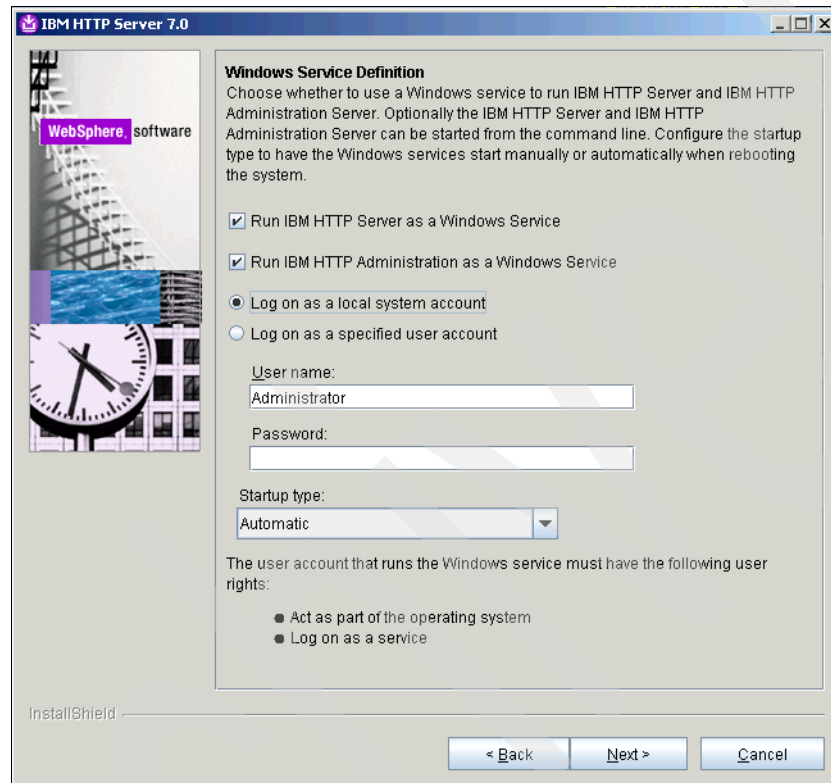


Figure 1-47 Windows Service Definition

This completes the configuration of IHS itself.

The next steps configure the integration between IHS and WebSphere Application Server:

1. Define the WebSphere Application Server account for administering IHS and the IHS plug-in for WebSphere Application Server to route the appropriate HTTP requests to the application server (Figure 1-48). Specify an account that can be used to administer IHS from WebSphere Application Server. This is a WebSphere Application Server account, not an operating system account. This is an account used to authenticate to IHS for management from WebSphere Application Server. The install process creates the account. When finished, click **Next**.

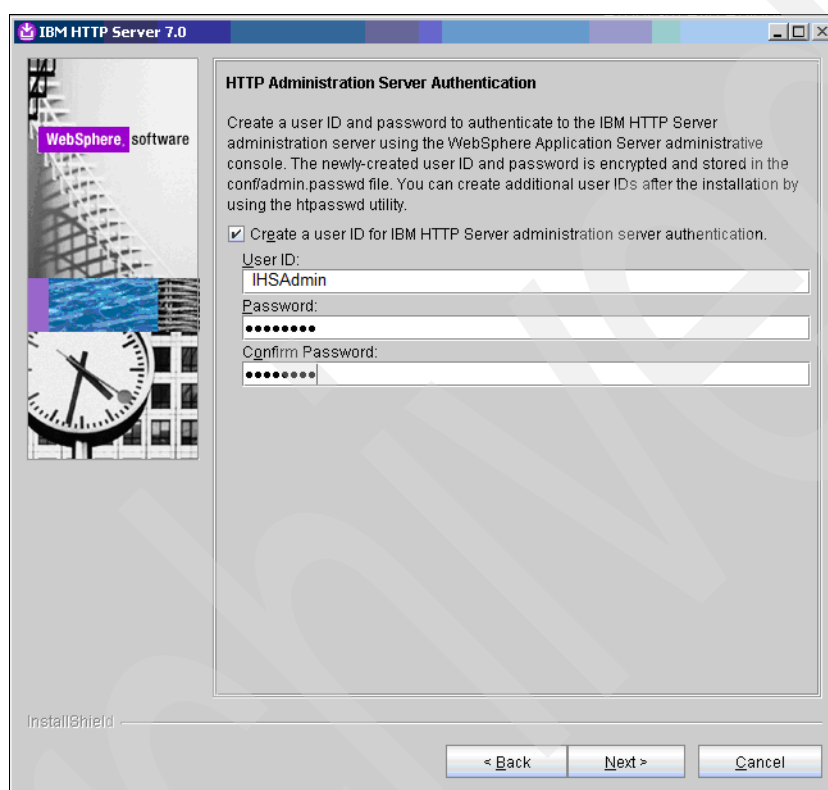


Figure 1-48 HTTP Administration Server Authentication account

The next step is setting the parameters is to generate the IHS WebSphere Application Server plug-in configuration.

2. Specify the web server definition (by default, webserver1) and the host name or IP address of the application server (WebSphere Application Server) (Figure 1-49). This sets the parameters to install the IHS plug-in for WebSphere Application Server and configure the plugin-cfg.xml file. When finished, click **Next**.

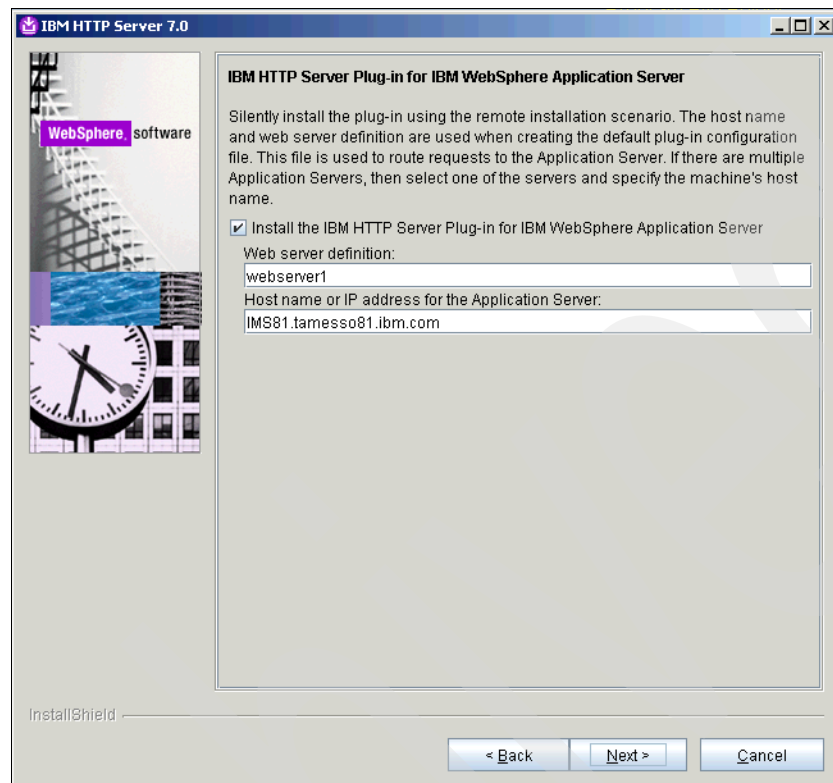


Figure 1-49 Define routing information for IHS plug-in

3. Review the installation summary details prior to installing the both IBM HTTP Server and IBM HTTP Server plug-in for IBM WebSphere Application Server (Figure 1-50).

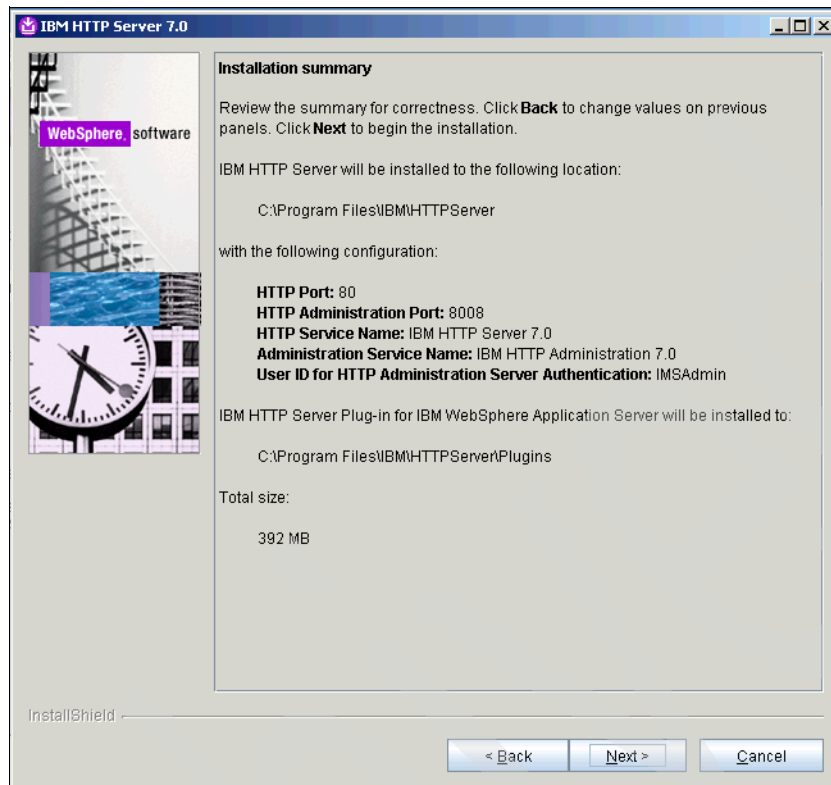


Figure 1-50 IHS and IHS plug-in installation summary

4. Click **Next** to start the install. When the installation completes and is successful (Figure 1-51), click **Finish**.

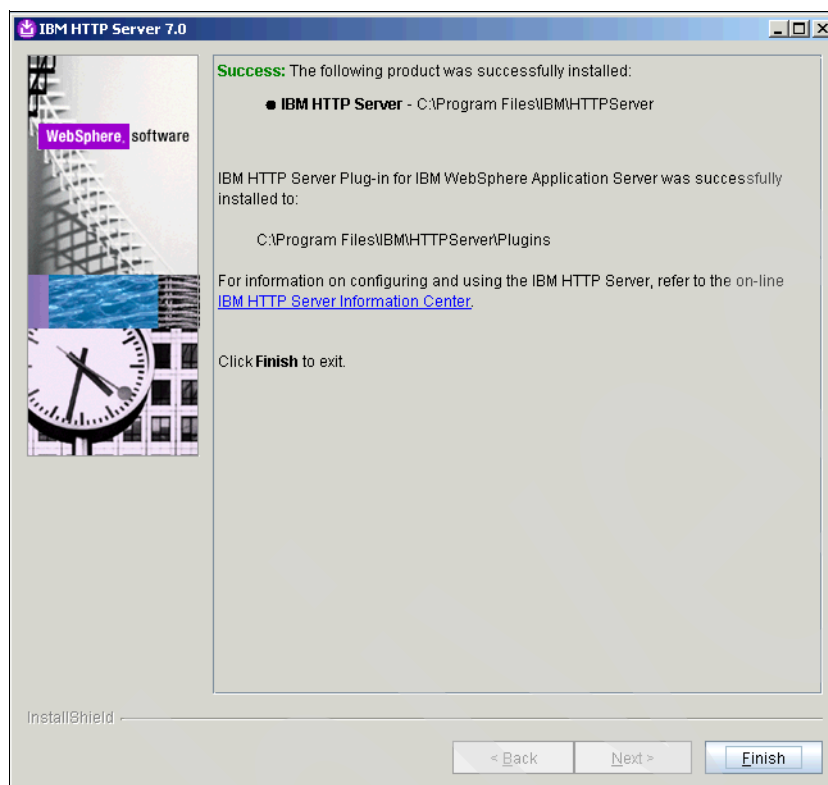


Figure 1-51 Successful installation of IHS and IHS plug-in for WebSphere Application Server

This completes the IHS and IHS plug-in for WebSphere Application Server installation.

In the following section are the steps for the IMS-required IHS configuration. You can also apply the latest IHS fix pack before or after the configuration. We do it after the configuration.

1.4.2 Configuring the IBM HTTP Server

Use this procedure to set up the IBM HTTP Server to work with the WebSphere Application Server. These steps are detailed in the first section of Chapter 5 of the *BM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309.

Before you begin, ensure that:

- ▶ You installed the WebSphere Application Server and IMS Server.
- ▶ The IBM HTTP Server and IBM HTTP Server Administration Server are running.
- ▶ The WebSphere Application Server is running.
- ▶ You have an administrator user name and password for the IBM HTTP Server.
- ▶ You disabled Microsoft Internet Information Services (IIS) if your system is running on Windows 2000 or later.

If IIS is active, port 80 and 443 are locked and the IBM HTTP Server configuration might fail.

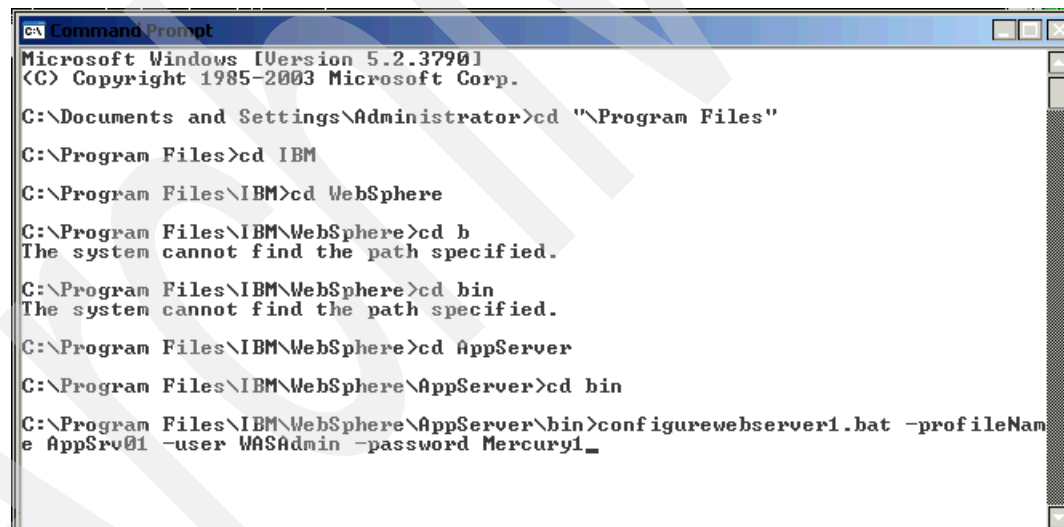
Take the following steps to configure the IHS:

1. Select **Start** → **All Programs** → **IBM WebSphere** → **Application Server v<version>** → **Profiles** → **<profile name>** → **Administrative console**.
2. On the IBM Integrated Solutions Console login page, enter your login credentials.
3. Click **Log in**.
4. Set up the WebSphere Application Server environment to work with the IBM HTTP Server plug-in and configure remote administration for IHS. This done so that the web server can be managed from within the ISC.

During the steps of the IHS installation and configuration in previous sections a Windows batch file (configure<web server name>.bat) to configure the web server was created. The default batchfile is called configurewebserver1.bat.

The <web server name> part of the configure<web server name>.bat file is specified during IBM HTTP Server installation. Copy this file from the <IHS install directory>\Plugins\bin to <WAS install directory>\bin. For example, copy C:\Program Files\IBM\IBMHTTPServer\Plugins\bin\configurewebserver1.bat to C:\Program Files\IBM\WebSphere\AppServer\bin.

5. Run configure<web server name>.bat from the command prompt. In the WebSphere Application Server bin directory, run the batch file, passing it arguments of the profile name, WebSphere Application Server administration user, and password. Figure 1-52 presents an example of executing the batch file to configure a created web server to be managed within the ISC.



```
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>cd "\Program Files"
C:\Program Files>cd IBM
C:\Program Files\IBM>cd WebSphere
C:\Program Files\IBM\WebSphere>cd b
The system cannot find the path specified.
C:\Program Files\IBM\WebSphere>cd bin
The system cannot find the path specified.
C:\Program Files\IBM\WebSphere>cd AppServer
C:\Program Files\IBM\WebSphere\AppServer>cd bin
C:\Program Files\IBM\WebSphere\AppServer\bin>configurewebserver1.bat -profileName AppSrv01 -user WASAdmin -password Mercury1_
```

Figure 1-52 Configure the web server to WebSphere Application Server as a profile

Note: If the script fails, edit the soap.client.props file in the <WAS profile>\properties directory (for example, C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\properties) and increase the value for the com.ibm.SOAP.requestTimeout property to 6000.

6. Wait until you see the Configuration save is complete message and exit the command prompt when it is finished.

7. Grant remote server management rights to the WebSphere Application Server administrator:
 - a. Log in to the WebSphere Application Server ISC using the WebSphere Application Server administrative account to set remote administration.
 - b. Navigate to **Servers** → **Server Types** → **Web servers** → **<server>** → **Remote Web server management**, specify the SOAP port, and enter the credentials that you set when provisioning an administrator for IBM HTTP Server (Figure 1-53).
 - c. Select **Use SSL** if you want to use the HTTPS secure protocol. If you do not select Use SSL, the default protocol is HTTP, which is not secure. When finished, click **OK**.
 - d. Save the configuration when prompted by clicking **Save** in the Messages box.

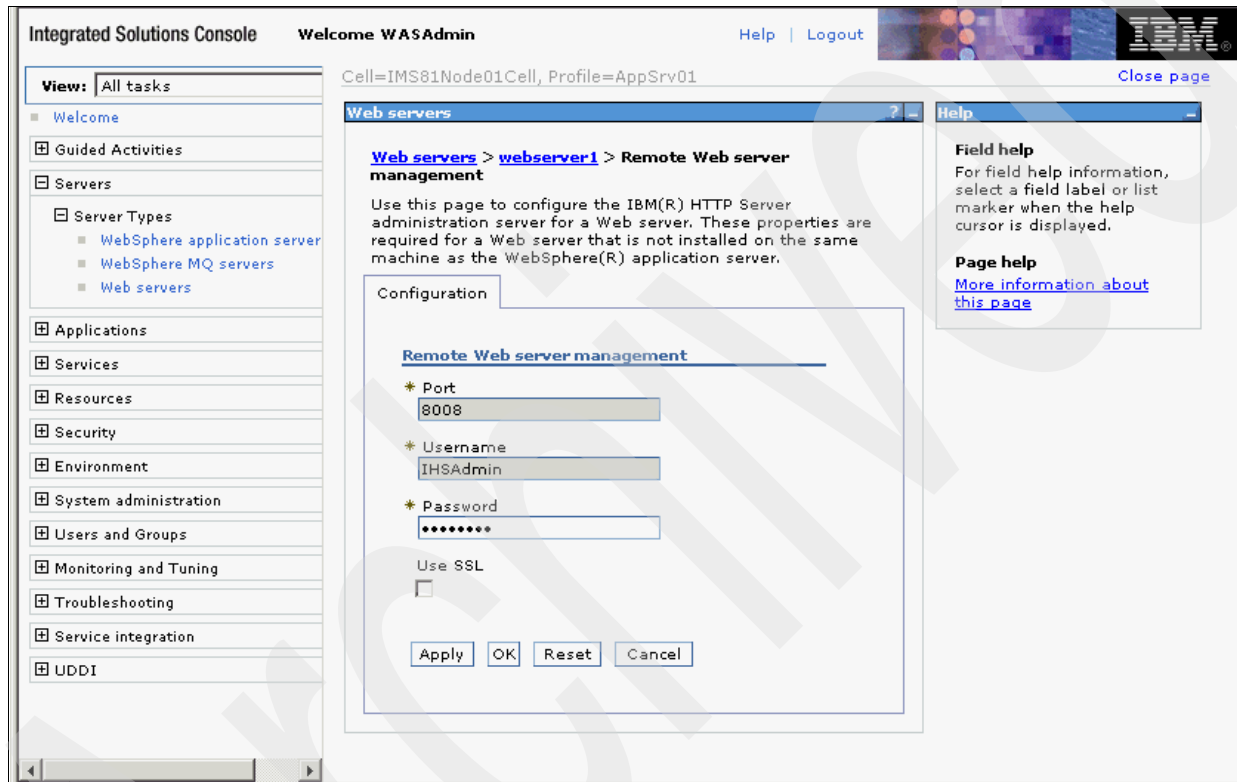


Figure 1-53 Specify port and user credentials for remote web server configuration

8. Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore.

From the Web servers list, click **<server>** → **Plug-in properties** (on the right of the page). There is nothing to change here, but you need to click **Copy to Web server key store directory** to synchronize the WebSphere Application Server keystore with IHS so that the HTTP plug-in will work (Figure 1-54).

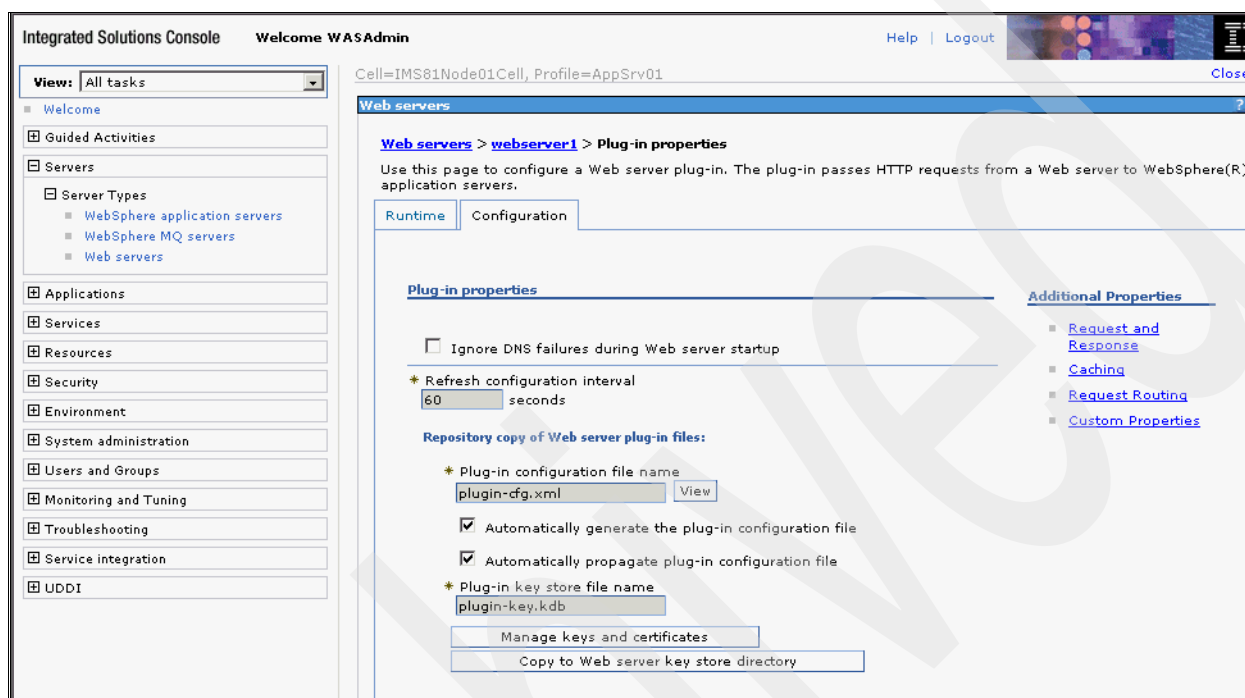


Figure 1-54 Synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore

9. Click **OK** to complete this configuration (Figure 1-55).

Figure 1-55 Complete WebSphere Application Server configuration file changes

10. Click **Save** in the Messages box at the top of the page to save the changes to the WebSphere Application Server configuration files (Figure 1-56).

Figure 1-56 Saving WebSphere Application Server configuration file changes

11. Enable the Secure Sockets Layer (SSL) on IBM HTTP Server. This is for the AccessAgent to IMS Server (via IHS) communication and should be encrypted. To achieve this, manually add the SSL Apache directive to the HIS http.conf file. This can be done manually by locating the file on the OS, editing it to add the required entries, saving it, and restarting IHS.

Another option is to use the WebSphere Application Server ISC to edit the file. The steps are:

- a. Log on to the ISC.
- b. From the task list on the left side select **Servers** → **Server Types** → **Web servers**.
- c. Select the web server link (for example, webserver1).
- d. Under Additional Properties (on the right of the page), click **Configuration File**.
- e. Add the following to the end of the configuration file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
#Listen [::]:443
<VirtualHost *:443>
SSLEnable
SSLProtocolDisable SSLv2
SSLServerCert <alias of the IBM HTTP Server SSL certificate>
</VirtualHost>
KeyFile "<absolute path of the plugin-key.kdb file>"
SSLDisable
```

To help you understand the configuration information that is required to be added, consider the following lists for details:

- The alias of the default SSL certificate is *default*.
- The default location of the plugin-key.kdb file is C:\Program Files\IBM\HTTPServer\Plugins\config\webserver1.
- The KeyFile file is in Servers\Server Types\Web Server\<servername>\Plug-in Properties\<Web server copy of Web server pluginfiles>\<absolute path of the plugin keystore file>.

Example 1-1 shows an example of the content that is added to the configuration file.

Example 1-1 Configuration file example

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
#Listen [::]:443
<VirtualHost *:443>
SSLEnable
SSLProtocolDisable SSLv2
SSLServerCert default
</VirtualHost>
KeyFile "C:\Program
Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb"
SSLDisable
```

Figure 1-57 shows how the configuration file changes look when using the WebSphere Application Server ISC.

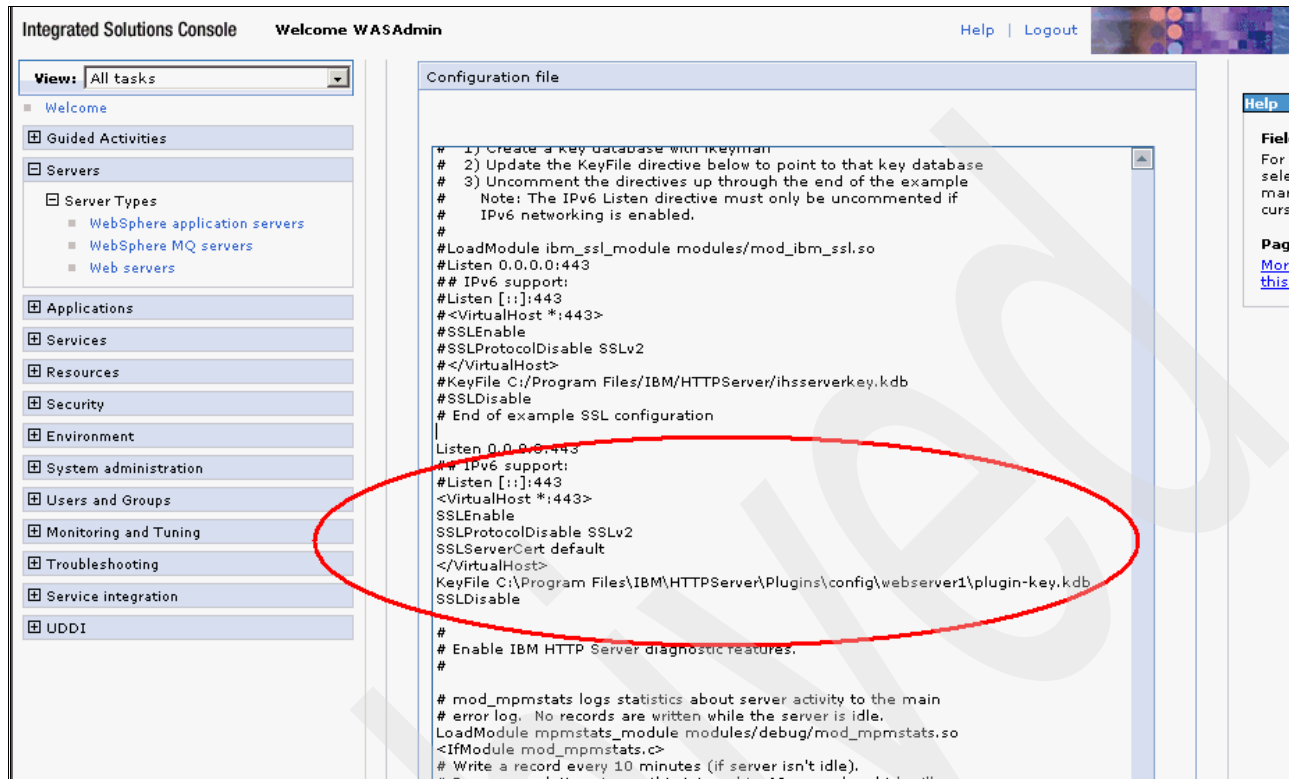


Figure 1-57 Configuration file changes made in the Integration Solutions Console

Note: When performing this change to the configuration file, note to the user that in the configuration file, there exists an example SSL configuration approximately half way in the file that has been commented out on purpose. Do not be mix up this commented-out example with your new SSL configuration entry.

12. When finished, click **Apply** and then **OK**.
13. Select **General Properties** → **Apply**. Click **Save** in the Messages box at the top of the page.
14. Stop and start the IBM HTTP Server from the IBM Integrated Solutions Console.
15. From the left side menu panel, select **Servers** → **Server Types** → **Web servers**.
16. Select the check box beside the web server link (for example, webserver1).
17. Click **Stop**.
18. Select the check box beside the web server link again.
19. Click **Start**.

This completes the IHS installation steps.

1.4.3 Applying HTTP Server fix pack

Apply the IHS patch using the IBM Update Installer as per the WebSphere Application Server patch application in 1.2.3, “Upgrading WebSphere Application Server” on page 22. The only difference is the location of IHS, C:\Program Files\IBM\HTTPServer.

1.5 IMS configuration

This section describes the IMS-post installation steps to configure the IMS Server that you installed earlier. Before proceeding to the IMS configuration, follow the IMS pre-configuration steps in this section.

1.5.1 Applying the IMS fix pack

At the time of writing, the Tivoli Access Manager for Enterprise Single Sign-On 8.1 fix pack 1 (8.1.0.1) was available. The fix pack is shipped as an IBM Update Installer .pak file, 8.1.0-TIV-TAMESS0-IMS-FP00001.pak.

The installation instructions are included with the fix pack.

Note that:

- ▶ You can install the IMS FP1 before or after configuring IMS. There are specific scenarios in which it should be applied before IMS configuration. See the Release Notes for details.
- ▶ You must use Update Installer 7.0.0.1+ to update IMS Server, so apply the latest Update Installer FP. It makes sense to do this when you apply the WebSphere Application Server 7.0 FP.

1.5.2 Creating IMS administrator in Active Directory

An IMS administration account is required. You can use any user account, but it needs to be a member of the local administrators group. Figure 1-58 shows the creation of the IMS administration account user named IMSAdmin.

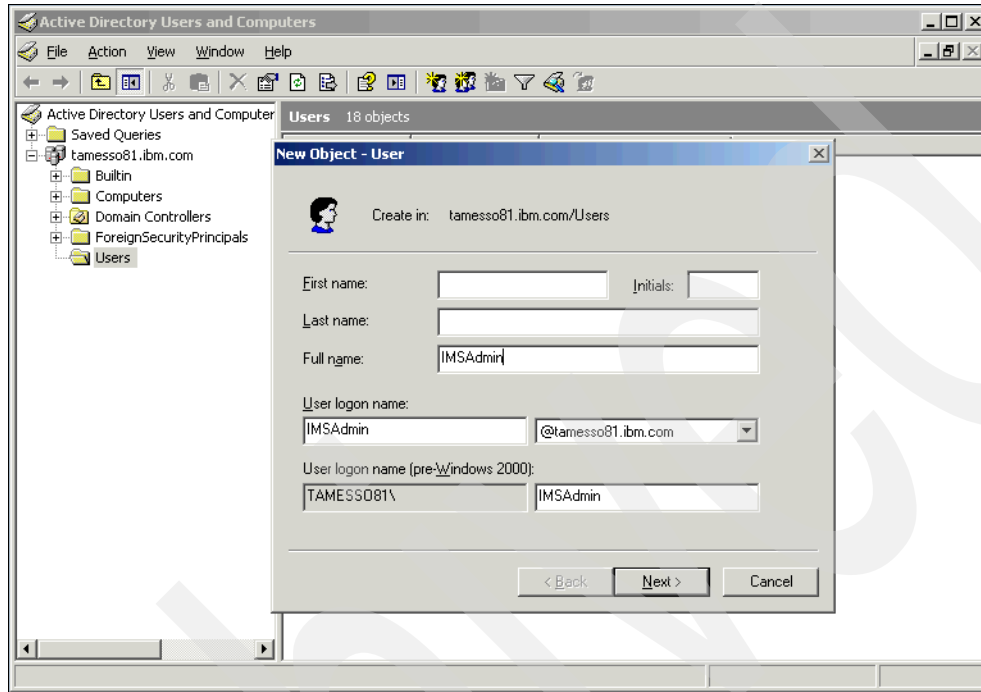


Figure 1-58 Creating an IMS administration account in Windows Active Directory

1.5.3 Configuration of the IMS Server

Before beginning to configure the IMS Server, ensure that the following tasks are complete:

- ▶ Install the IMS Server and the IBM HTTP Server, then complete the IMS-required IHS configuration steps.
- ▶ Check the Tivoli Access Manager for Enterprise Single Sign-On *<installation directory>/TAM_E-SSO_IMS_Server_InstallLog.log* file for critical errors that occurred during the IMS Server installation (if not done as described in 1.3.3, “Verifying the IMS Server installation and deployment” on page 33).
- ▶ Set up the database that you want to use as the IMS Server database.
- ▶ During the IMS Server configuration steps, choose whether you want to use your own database schema or create the new schema with the configuration wizard. If you chose to use own database schema, create the schema before you start the IMS Server configuration. Also, ensure that you set up your IMS Server database.
- ▶ See the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, for the setup instructions.

The steps for configuring the IMS Server are:

1. Connect to the IMS Server using one of the following:
 - If you are using the default port, access `https://<IMS IHS hostname>/ims`.
 - If you are not using the default port, access `https://<IMS IHS hostname:IHS SSL port>/ims`.

An example of the URL is:

`https://computerXYZ.us.ibm.com:1234/ims`

This confirms that the HTTP Server is running, the WebSphere Application Server plug-in is configured correctly, IMS is running on WebSphere Application Server, and (if the https URL is used) the HTTPS is configured correctly on IHS.

If everything is configured correctly you will see the Tivoli Access Manager for Enterprise Single Sign-On Configuration Wizard Import Configuration page (Figure 1-59).

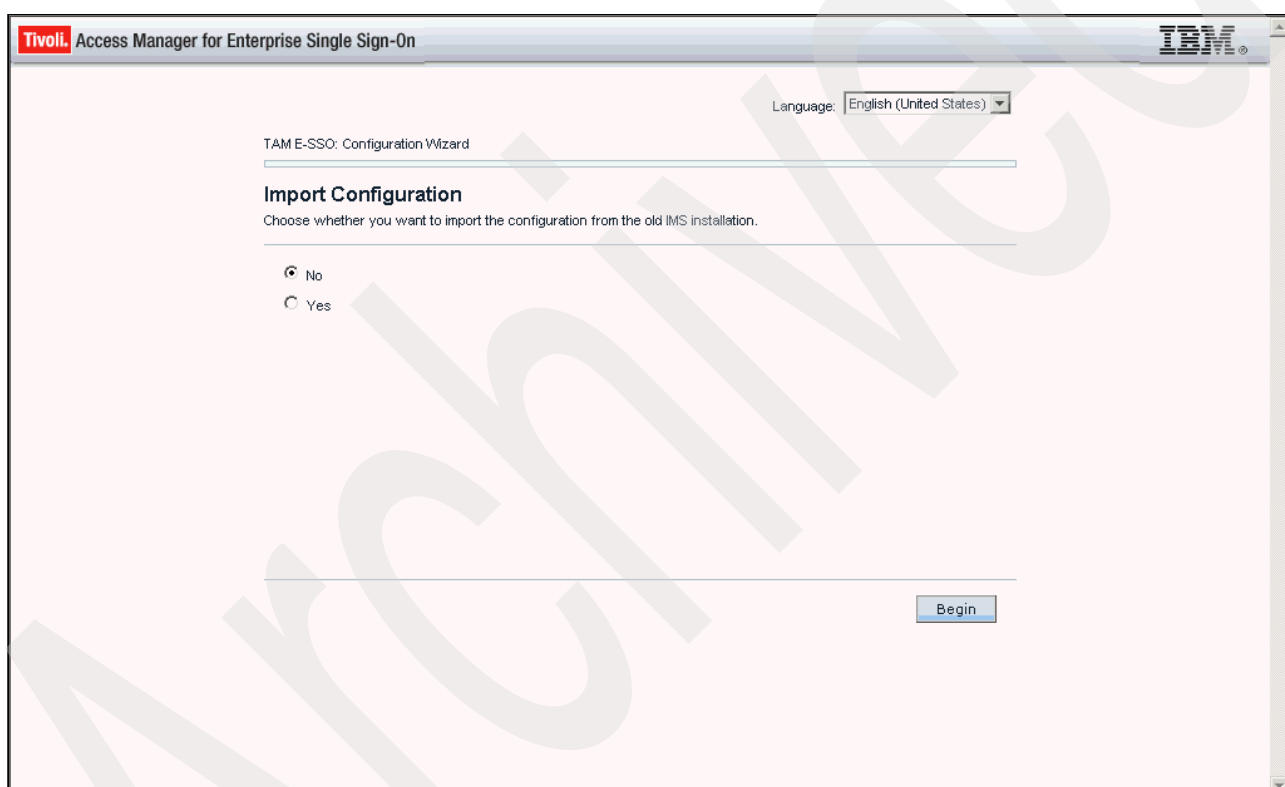


Figure 1-59 Configuration Wizard Import Configuration

2. Select No, and click **Begin** to start the configuration.

3. On the Enter data source information page (Figure 1-60), leave all values as they are. These are the names that will be given to the JDBC provider and data source definitions in WebSphere Application Server, and changing them can cause problems with IMS. When finished, click **Next** to continue.

Tivoli Access Manager for Enterprise Single Sign-On

Language: English (United States)

TAM E-SSO: Configuration Wizard

Enter data source information

Set the configuration values of a data source.

JDBC provider name:
TAM E-SSO JDBC Provider

Data source name:
TAM E-SSO IMS Server Data Source

JNDI name:
jdbc/ims

JAAS - J2C authentication data alias:
imsauthdata

Cancel Back Next

Figure 1-60 Data source information

4. When choosing to create an IMS Server database schema (Figure 1-61), do one of the following actions:
 - a. Select the **Create IMS Server database schema** check box. This tells the Configuration wizard to build the database schema and initial content.
 - b. If you de-select this item, you need to manually create the database after the configuration. To use your own schema, see Appendix D in the *BM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, G111-9309, for further information about creating database schema. In the example presented in this guide, this option has been checked.

Click **Next** to continue.

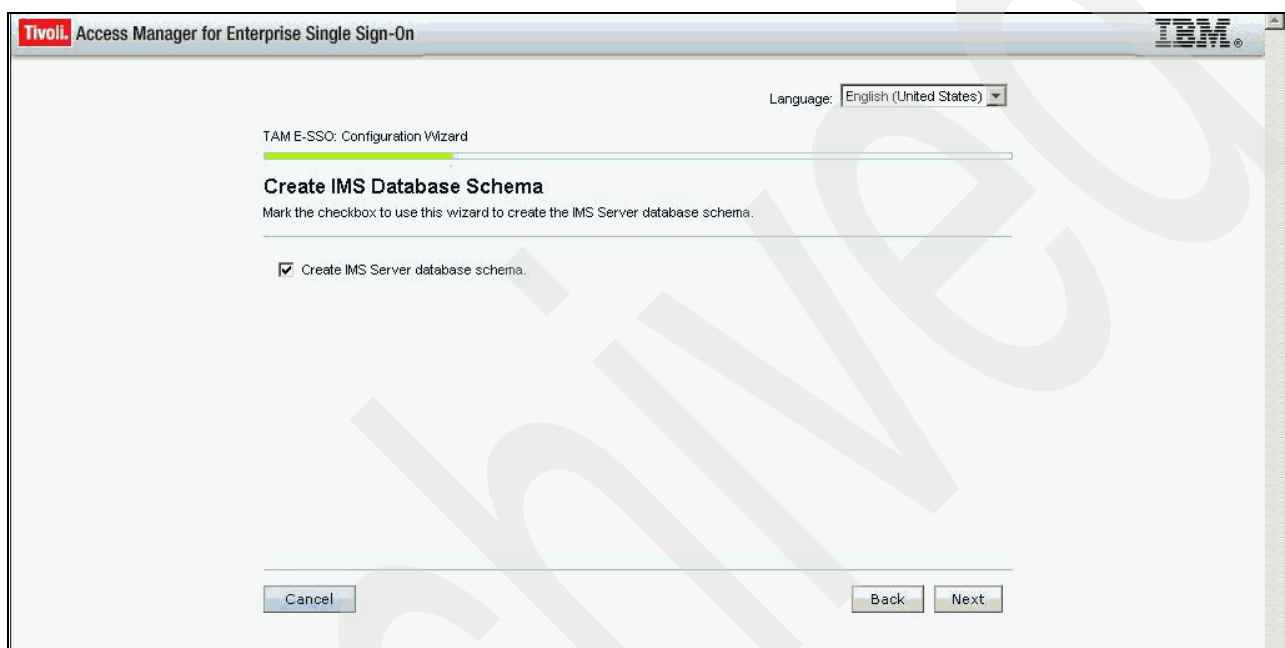


Figure 1-61 Create IMS Database Schema

5. On the Choose Database Type page (Figure 1-62), select the type of database server that you installed earlier and click **Next** to continue.

The screenshot shows the 'TAM E-SSO: Configuration Wizard' window. At the top, the title bar reads 'Tivoli. Access Manager for Enterprise Single Sign-On'. Below the title bar, there is a language dropdown menu set to 'English (United States)'. The main content area is titled 'Choose Database Type' and includes the instruction 'Choose the database type the IMS Server will use.' Below this, there are three radio button options: 'DB2 Server' (which is selected), 'Microsoft SQL Server', and 'Oracle Server'. At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next'.

Figure 1-62 Database Type for IMS Server

6. On the Database Configuration - *<database type>* page, specify the necessary information about the database type. Before proceeding, check any prerequisites for applying the database type during this configuration step. Appendix A, "Database type configuration for IMS Server" on page 203, provides detailed information about configuration for DB2 and Microsoft SQL server for the IMS Server. When you have chosen the database type, click **Next** to continue.

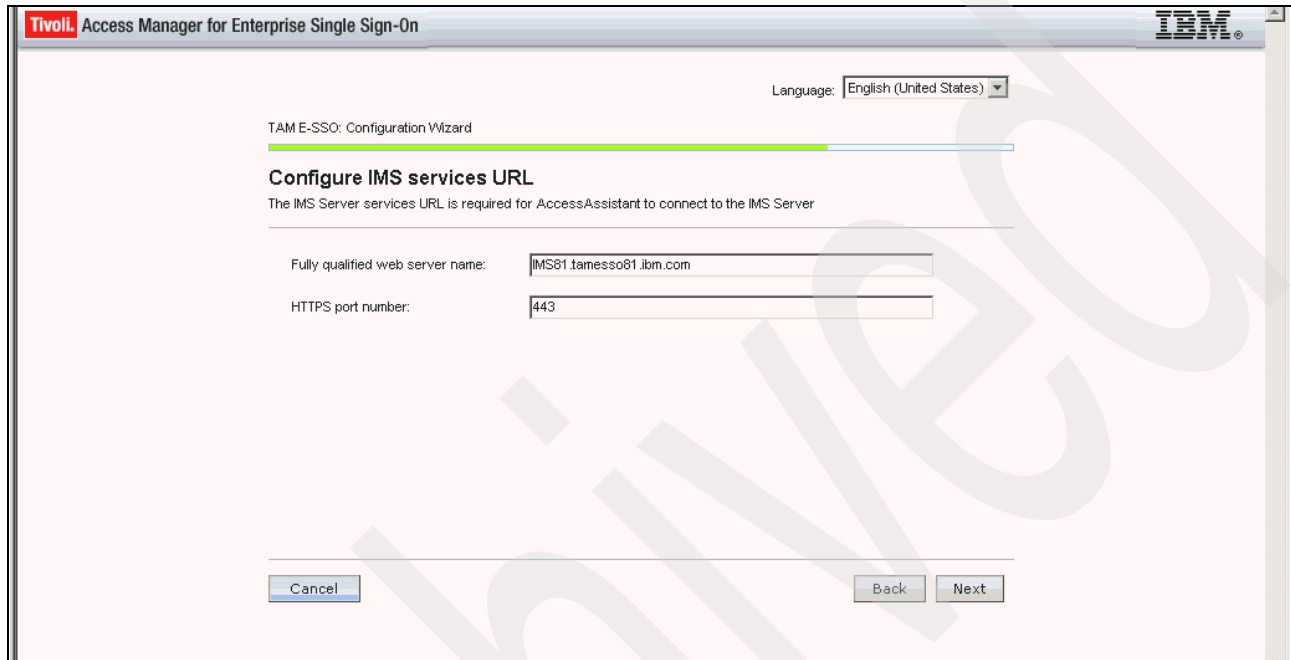
7. On the Provide Root CA Details page (Figure 1-63), leave the default values (the password is WebAS) if you have not changed the root CA used to sign the SSL certificate used by IHS. The option is to specify the necessary information. When finished, click **Next** to continue.

Note: The root CA must be the same CA that signs the SSL certificate. There the root CA is used to sign the IMS Server CA.

The screenshot shows the 'Provide Root CA Details' page of the Tivoli Access Manager for Enterprise Single Sign-On configuration wizard. The page has a title bar with 'Tivoli. Access Manager for Enterprise Single Sign-On' and the IBM logo. A language dropdown menu is set to 'English (United States)'. Below the title bar, a progress bar indicates the current step. The main heading is 'Provide Root CA Details', followed by a sub-heading: 'Enter the keystore name, password, and certificate alias of the root CA that will be used to sign the IMS Server intermediate CA.' There are three input fields: 'Keystore name:' with the value 'NodeDefaultRootStore', 'Keystore password:' with masked characters '*****', and 'Root CA alias name:' with the value 'root'. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

Figure 1-63 Root CA Details

8. On the Configure IMS services URL page (Figure 1-64), specify the IBM HTTP Server name and port number value. The IBM HTTP Server name is the full-qualified web server name of the IBM HTTP Server that interfaces with the WebSphere Application Server. The port number value is the HTTPS communication port number. The IBM HTTP Server host name must match the CN attribute of the SSL certificate used by IBM HTTP Server. You can connect to the SSL port in a web browser to check this. When finished, click **Next** to continue.



Tivoli Access Manager for Enterprise Single Sign-On

Language: English (United States)

TAM E-SSO: Configuration Wizard

Configure IMS services URL

The IMS Server services URL is required for AccessAssistant to connect to the IMS Server

Fully qualified web server name:

HTTPS port number:

Figure 1-64 Configure IMS Services URL

9. On the Confirm settings page (Figure 1-65), review and verify that the setting information entered looks correct and click **Save**.

Tivoli Access Manager for Enterprise Single Sign-On

Language: English (United States)

TAM E-SSO: Configuration Wizard

Confirm settings

The following settings will be applied. Confirm the settings before proceeding to the next step. If the settings are correct, click Save.

- ✓ Data source name:
 - TAM E-SSO IMS Server Data Source
- ✓ JNDI name:
 - jdbc/ims
- ✓ Provide Root CA Details
 - Keystore name: NodeDefaultRootStore
 - Root CA alias name: root

Cancel Back Save

Figure 1-65 Confirm settings

The page is redisplayed with a progress bar showing the installation progress (Figure 1-66). At completion a Data Source and Certificate Store Setup Complete page is displayed.

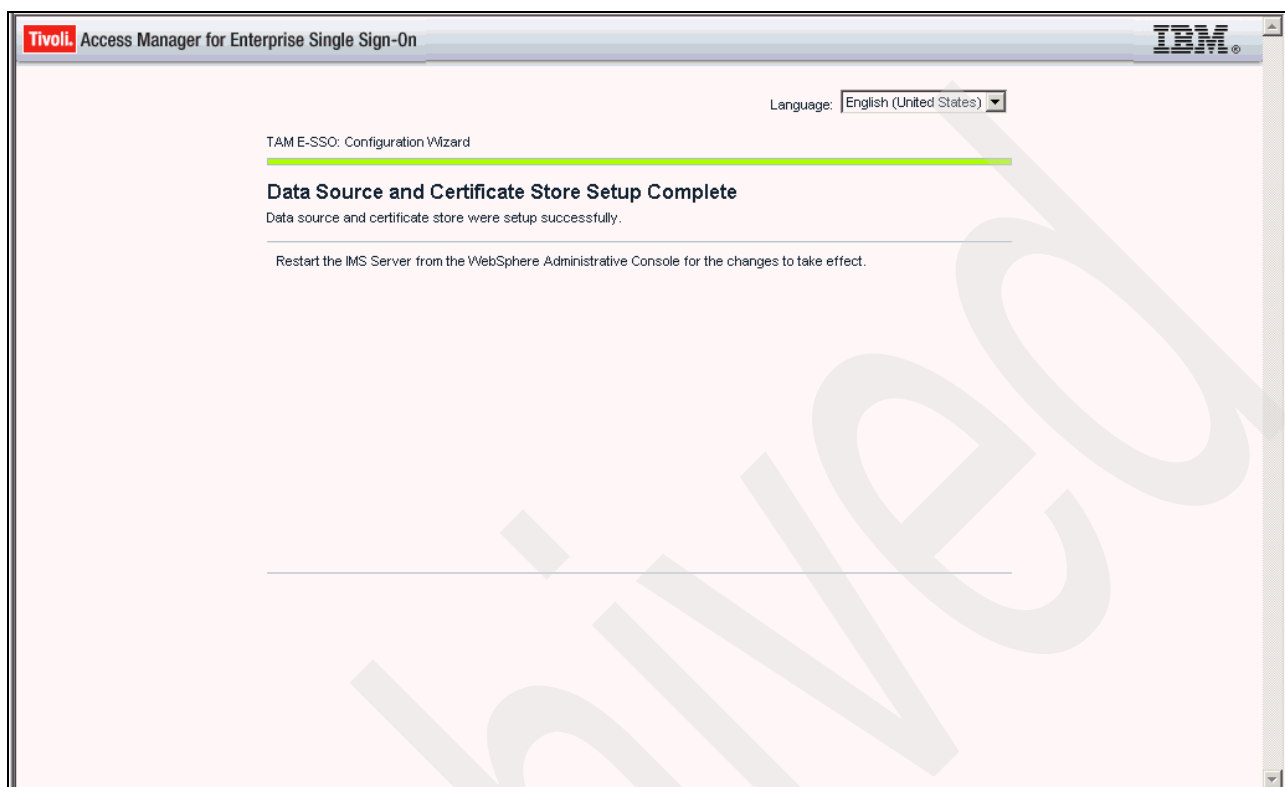


Figure 1-66 IMS configuration process

10. Restart the IMS Server application from within the IBM Integrated Solutions Console:

- a. Select **Start** → **All Programs** → **IBM WebSphere** → **Application Server** <version> → **Profiles** → <profile name> → **Administrative console**.
- b. Log in to WebSphere Application Server ISC with WebSphere Application Server administration user credentials.
- c. From the task list on the left side of the page, select **Applications** → **Application Types** → **WebSphere Enterprise Applications**.
- d. Select the check box beside the **Tivoli Access Manager for Enterprise Single Sign-On IMS** application.
- e. Click **Stop**.
- f. Select the check box beside the **Tivoli Access Manager for Enterprise Single Sign-On IMS** application.
- g. Click **Start**.

This concludes the IMS basic configuration.

1.5.4 Provisioning IMS administrator and defining enterprise directory

The next step is to provision an IMS administrator and create an enterprise directory connection.

These steps are mentioned in Chapter 5 of the *Tivoli Access Manager for Enterprise Single Sign-On 8.1 Install Guide* and are covered in detail in Chapter 3 of the *Tivoli Access Manager for Enterprise Single Sign-On 8.1 Setup Guide*.

1. To start the process, access the Tivoli Access Manager for Enterprise Single Sign-On Web Interface (Figure 1-67) via the URL `https://<IMS IHS Server>/ims`.

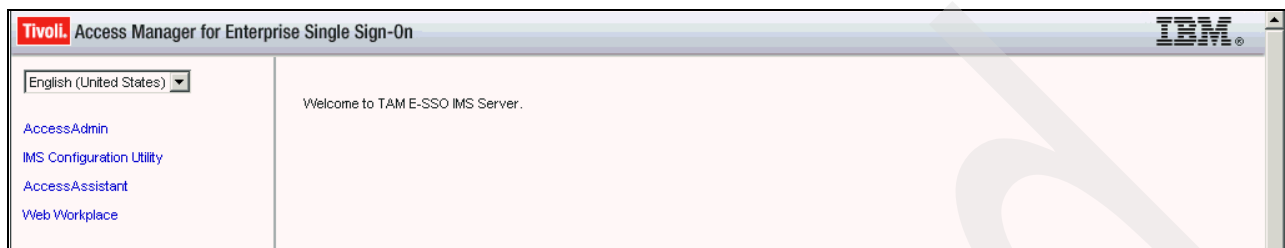


Figure 1-67 IMS web interface

2. Select the **IMS Configuration Utility** link.

The WebSphere Application Server Administrator needs to log on to the application, and as we have enabled global application security in WebSphere Application Server, our wasadmin account is used to log in on the Log on page (Figure 1-68).

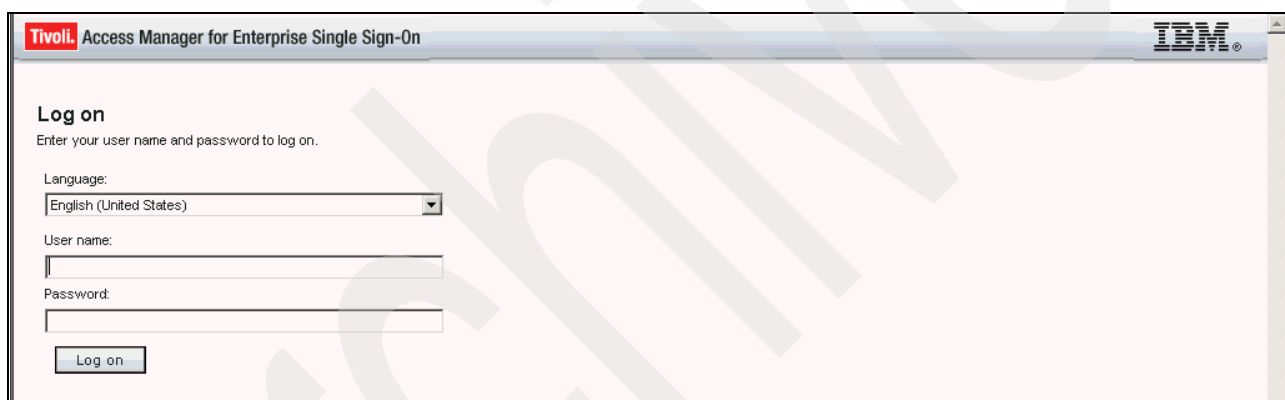


Figure 1-68 iMS configuration utility

The opening page for the IMS Configuration Utility is the Welcome page (Figure 1-69).



Figure 1-69 Welcome page of IMS configuration utility

3. Click the **Setup assistant** link. The setup assistant configures the Enterprise Directory (the Enterprise Directory Setup Wizard) and the initial IMS Administrator (Provision an IMS Server Administrator). The first few pages cover the Enterprise Directory setup.
4. On the Enterprise Directory Setup page (Figure 1-70), select **Active Directory**. A generic LDAP can be used, such as Tivoli Directory Server. This might be appropriate for certain demo environments.

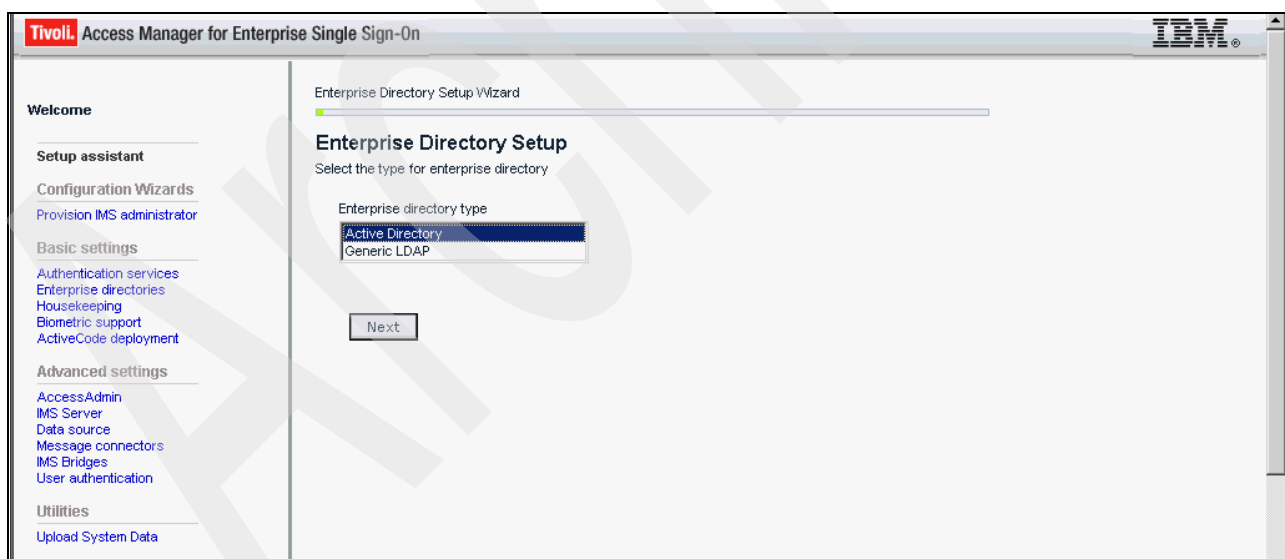


Figure 1-70 Enterprise Directory Setup

5. Click **Next** to continue to the Edit domain page (Figure 1-71). Specify the Windows AD domain (DNS domain name) and a lookup user ID/password for the Enterprise Directory. When finished, click **Next** to continue.

The screenshot shows the 'Edit domain' page in the Tivoli Access Manager for Enterprise Single Sign-On interface. The page title is 'Configure Active Directory connection'. The left sidebar contains a 'Welcome' section and a 'Setup assistant' section with links to 'Configuration Wizards' (Provision IMS administrator), 'Basic settings' (Authentication services, Enterprise directories, Housekeeping, Biometric support, ActiveCode deployment), 'Advanced settings' (AccessAdmin, IMS Server, Data source, Message connectors, IMS Bridges, User authentication), and 'Utilities' (Upload System Data). The main content area is titled 'Edit domain' and includes the instruction 'Edit the configured domain : tamesso81.ibm.com'. It contains three input fields: 'DNS domain name' with the value 'tamesso81.ibm.com', 'Lookup user name' with the value 'tamesso81.ibm.com\MSAdmin', and 'Lookup password' with masked characters. At the bottom of the form are 'Back' and 'Next' buttons.

Figure 1-71 Edit domain for Active Directory configuration

This is the user that IMS will look up in AD. This involves an initial AD lookup to determine the AD schema in use. Also, when a new user registers, it will look up AD to verify that the user exists.

For our deployment, we used the IMSAdmin account created above, which will be the Tivoli Access Manager for Enterprise Single Sign-On administrator in our case, though it can be any local user. Do not use an ordinary user account used to log into the domain, but you might want to make it different from the administrator account that you will use for policy and user administration (that is, one user account as the Tivoli Access Manager for Enterprise Single Sign-On user to look up AD and one Tivoli Access Manager for Enterprise Single Sign-On user account for administrative purposes).

- On the Password synchronization page (Figure 1-72), decide whether you want password synchronization between the Tivoli Access Manager for Enterprise Single Sign-On and AD for all users registered against this AD domain. With this option checked, the Active Directory password is enabled to be used as the Tivoli Access Manager for Enterprise Single Sign-On password. Users can then use their Active Directory credential information to log in to Tivoli Access Manager for Enterprise Single Sign-On. When finished, click **Next** to continue.

The screenshot shows the 'Configure Active Directory connection' step of the setup wizard. The left sidebar contains a 'Welcome' section and a 'Setup assistant' section with links to 'Configuration Wizards' (Provision IMS administrator) and 'Basic settings' (Authentication services, Enterprise directories, Housekeeping, Biometric support, ActiveCode deployment). The main content area is titled 'Password synchronization' and includes a progress bar. Below the title, it states: 'This option enables the Active Directory password to be used as the TAM E-SSO password. Users can then use their Active Directory credentials to log on to TAM E-SSO software.' There is a checkbox labeled 'Use Active Directory password as the TAM E-SSO password' which is currently unchecked. At the bottom of the main area are 'Back' and 'Next' buttons.

Figure 1-72 Password synchronization between users

- On the Choose credentials page (Figure 1-73), define the IMS Administrator to provision.

The screenshot shows the 'Provision an IMS Server Administrator' step of the setup wizard. The left sidebar is similar to the previous screen, but the 'Provision IMS administrator' link under 'Configuration Wizards' is highlighted. The main content area is titled 'Choose credentials' and includes a progress bar. Below the title, it states: 'Provide credentials of a valid domain user to be provisioned as an IMS Administrator.' There are three input fields: 'User name:' with the value 'IMSAdmin', 'Password:' with masked characters, and 'Domain:' with a dropdown menu showing 'tamesso81.ibm.com'. Below these fields is a checkbox labeled 'I will assign the Administrator later' which is unchecked. At the bottom of the main area are 'Back' and 'Next' buttons.

Figure 1-73 Define credentials to be provisioned as an IMS Administrator

- Specify the user to be used as the initial IMS Server administrator. In our case we re-used the AD lookup account from earlier. When finished, click **Next** to proceed to the Summary page (Figure 1-74).

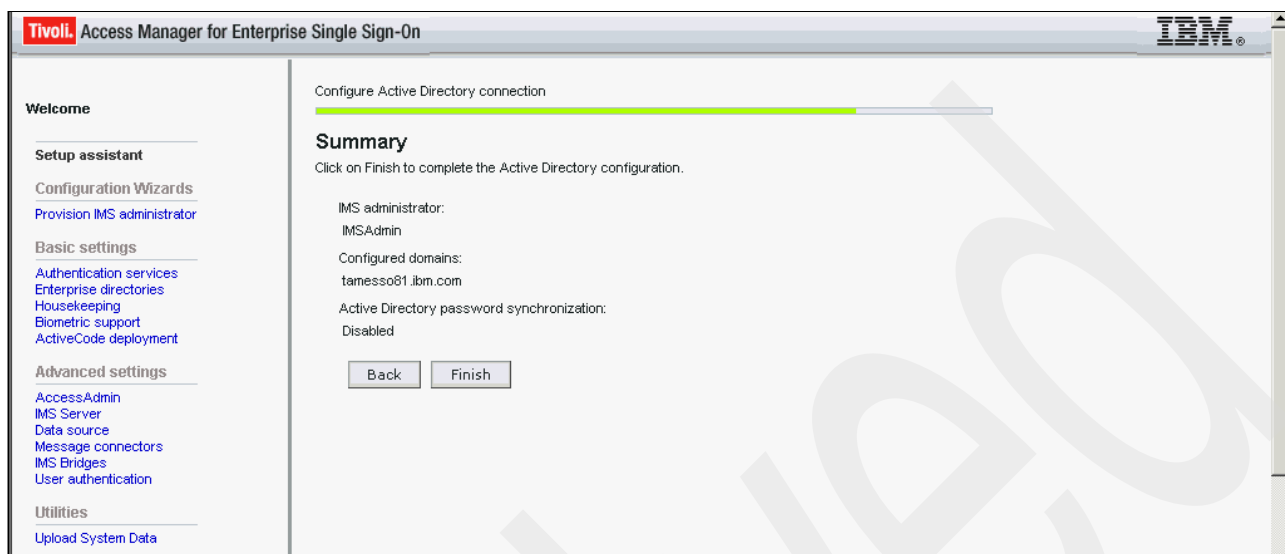


Figure 1-74 Summary for configuring Active Directory connection

- Verify the settings and click **Finish** to complete. After the configuration is completed and successfully, a finished message and configuration results are displayed to confirm the status (Figure 1-75).

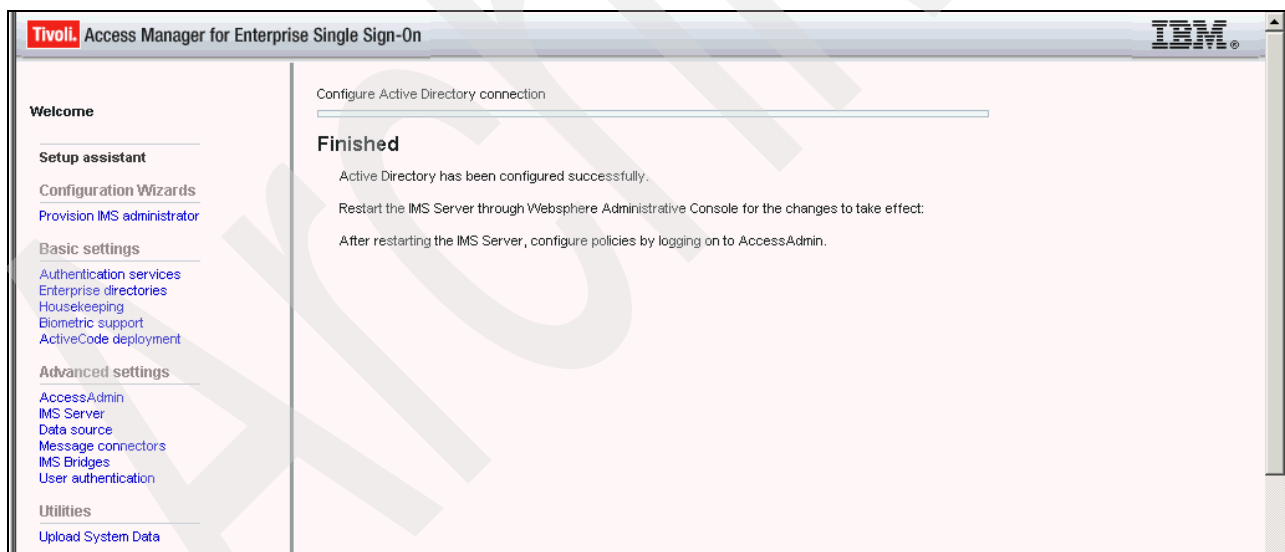


Figure 1-75 Active Directory configured successfully

- Restart the IMS application from within the WebSphere Application Server ISC. Then go to the access admin at <https://<IHS server>/admin> and log in using your Tivoli Access Manager for Enterprise Single Sign-On administrator account that you specified above.

Proceed to define user and machine policy templates using the setup wizard, but this is not covered in this document. See the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Policies Definition Guide*, SC23-9694, for information about the policies that can be set for this product.

1.6 AccessAgent and AccessStudio

The Tivoli Access Manager for Enterprise Single Sign-On AccessAgent and Tivoli Access Manager for Enterprise Single Sign-On AccessStudio installation is reasonably straightforward. The Access Studio requires an AccessAgent to be installed (so it can communicate with the IMS Server). The AccessAgent requires a configuration file to be edited prior to running the installer.

1.6.1 Preparing to install AccessAgent

Before installing AccessAgent, you must understand the preinstallation tasks and certain key concepts. See the “AccessAgent preinstallation tasks and information” section in the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309.

The AccessAgent install is controlled by settings in the SetupHlp.ini file (Figure 1-76), found in the Config directory under the Access Agent install image.

Edit this file in an editor and set the ImsServerName argument to the full host name of the IMS Server. This is the host name of the IHS server and should match the full host name in the HTTP Server SSL CA cert.



Figure 1-76 AccessAgent installation and upgrade options defined in SetHlp.ini

You might want to check the ImsSecurePortDefault, ImsDownloadPortDefault, and ImsDownloadProtocolDefault settings. If you have configured IMS and IHS correctly, the values already there should be correct. Save and exit.

1.6.2 Installing AccessAgent

The steps to install the AccessAgent are straightforward. For more details on installation steps, refer to the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, for information.

1. Run the installer in the AccessAgent directory. You can install AccessAgent using either of following methods:

- Using setup.exe
 - i. Start setup.exe.
 - ii. Go to the Select a language step.

Note: If the language for the installation is different from the Windows operating system language, certain messages might appear in English or the operating system language.

- Using AccessAgent.msi.

Double-click **AccessAgent.msi**. The installation program installs the English version without prompting you to select a language.

2. Select a language from the list and click **OK**.
3. Click **Next** to display the license agreement.
4. Select **I accept the terms in the license agreement**.
5. Click **Next** to display the Install AccessAgent dialog.
6. Click **Browse** to select another folder. Click **Next** to continue the installation.
7. Click **Yes** to restart the computer immediately or **No** to restart it later.

Important: You must restart the computer before you can sign up or log on to the Wallet. After the computer restarts, the AccessAgent window appears. The contents vary according to your organization's settings.

For Microsoft Windows Vista, enable "Interactive logon: Do not require CTRL+ALT+DEL" in the Active Directory. AccessAgent automatically enables this security option during installation unless other group policy enforcements prevent it from doing so. If the setting is not enabled, press Ctrl+Alt+Delete to invoke the AccessAgent logon page.

Note: If there is a problem connecting to the IMS Server, you might be prompted to enter the IMS Server host name and port again. If this continues to be a problem, you must diagnose the connection problems (see Appendix B, "Diagnosing installation problems" on page 207). You can bypass the step to define the IMS Server, but you are better off resolving the connection issue before continuing.

1.6.3 Installing AccessStudio

The AccessStudio installation is straightforward. Run setup.exe in the AccessStudio directory and follow the prompts. For more details about the installation steps, see the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309.

1.7 Conclusion

In this chapter we provided detailed instructions about installation, including figures and information discovered during a number of installations that are not documented elsewhere in the standard installation guides for the Tivoli Access Manager for Enterprise Single Sign-on Version 8.1 product.

The contents presented here focused on providing a thorough and comprehensive set of installation and configuration steps for the various product components for setting up a Tivoli Access Manager for Enterprise Single Sign-on environment for a single server install.

In the next chapter we take a closer look at how to install and configure Tivoli Access Manager for Enterprise Single Sign-on in a cluster environment.

Archived

Installation and configuration in a clustered environment

In this chapter we introduce the installation of Tivoli Access Manager for Enterprise Single Sign-On 8.1 in a clustered IBM WebSphere Application Server environment. This section supplements the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, and *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Setup Guide*, GC23-9692. Do not use this chapter in isolation. Check the relevant guides in the Tivoli Access Manager for Enterprise Single Sign-On Information Center as you perform the install.

Figure 2-1 shows a typical architecture diagram of WebSphere Application Server and Tivoli Access Manager for Enterprise Single Sign-On components in a clustered environment.

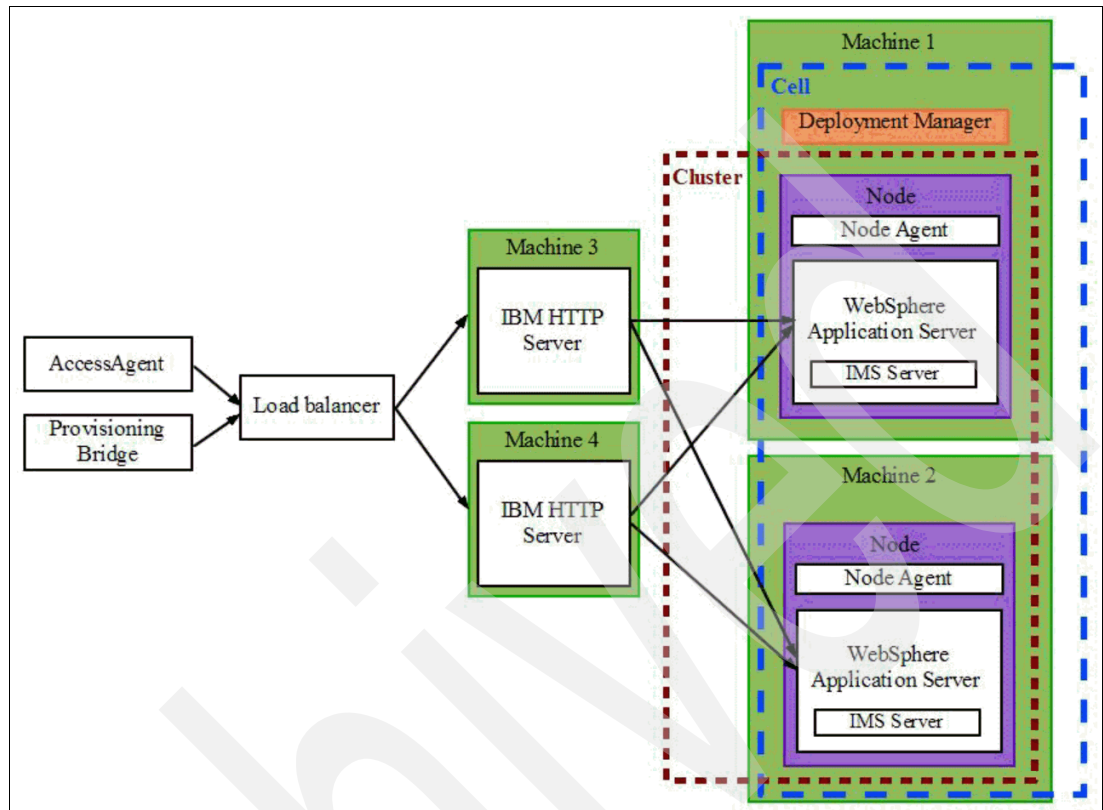


Figure 2-1 Clustered solution architecture

For the Tivoli Access Manager for Enterprise Single Sign-On 8.1 deployment (as documented in this chapter), we set up a single node WebSphere Application Server cluster with a single HTTP server without any load balancer. We use IBM DB2 for the IMS database. At a later point, you can add new cluster members as needed.

2.1 Database installation and configuration

Tivoli Access Manager for Enterprise Single Sign-On supports various versions of IBM DB2, Microsoft SQL Server, and Oracle databases. This section walks you through the installation of the IBM DB2 database.

2.1.1 Installing IBM DB2 Workgroup Server Version 9.7

To install IBM DB2 Workgroup Server Version 9.7, follow the steps below:

1. Start the DB2 Setup launchpad wizard provided on the installation CD (Figure 2-2).



Figure 2-2 Welcome to DB2 Version 9.7

2. Click **Install New** to launch the DB2 Setup wizard (Figure 2-3).



Figure 2-3 Install a Product

3. Click **Next** to begin the process of installing the DB2 Server (Figure 2-4).

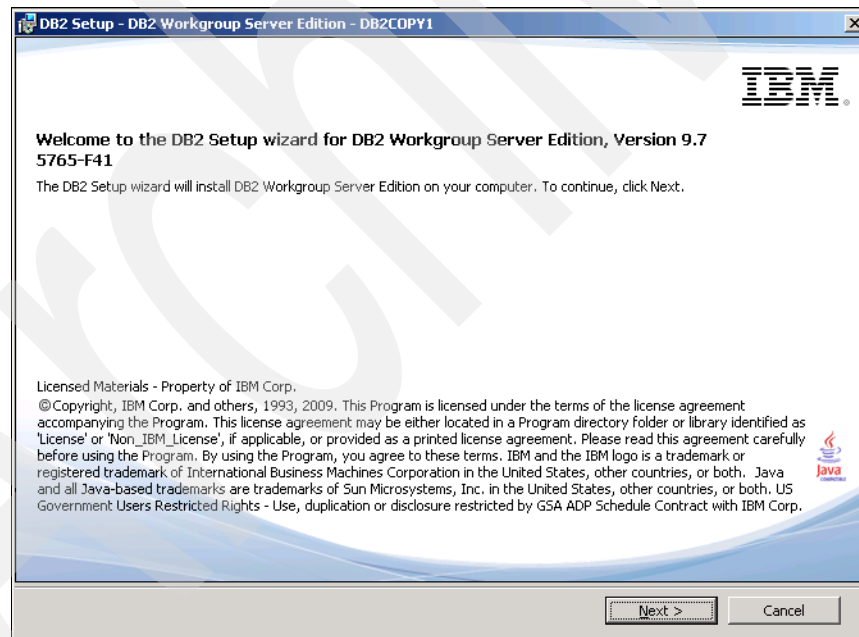


Figure 2-4 Welcome to the DB2 Setup wizard

4. Accept the license agreement and click **Next** (Figure 2-5).

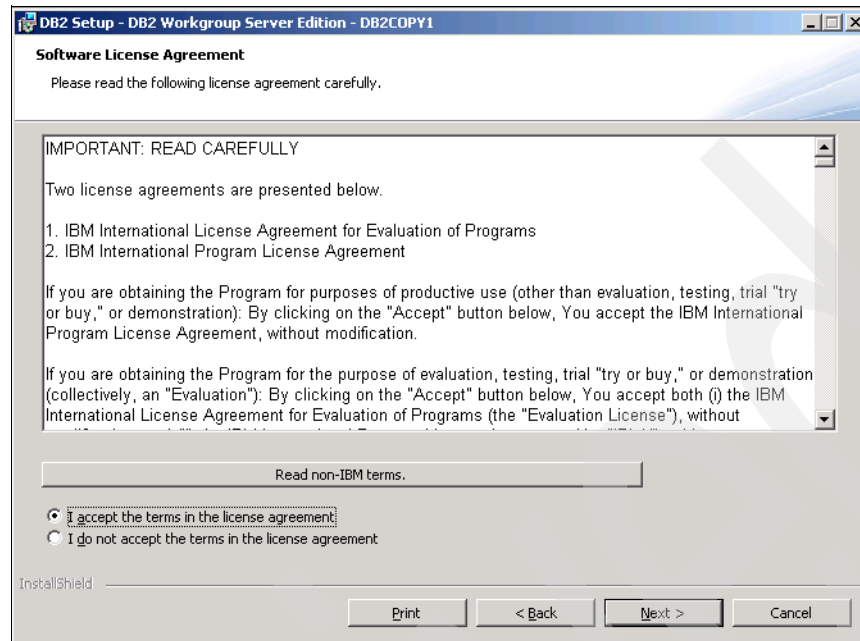


Figure 2-5 Software License Agreement

5. On the next page, you see three options for the installation type. Select the installation type that best suits your environment's needs. Click **Next** to continue the installation (Figure 2-6).

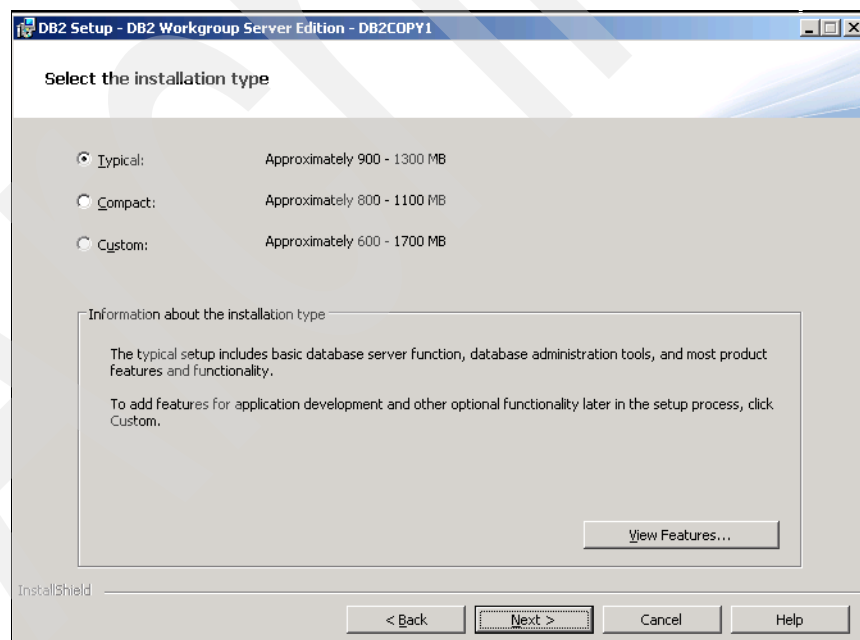


Figure 2-6 Select the installation type

6. On the Select the installation, response file creation, or both page, you can accordingly install DB2 on the computer or save the settings to a response file, or both, as necessary. Click **Next** to continue (Figure 2-7).

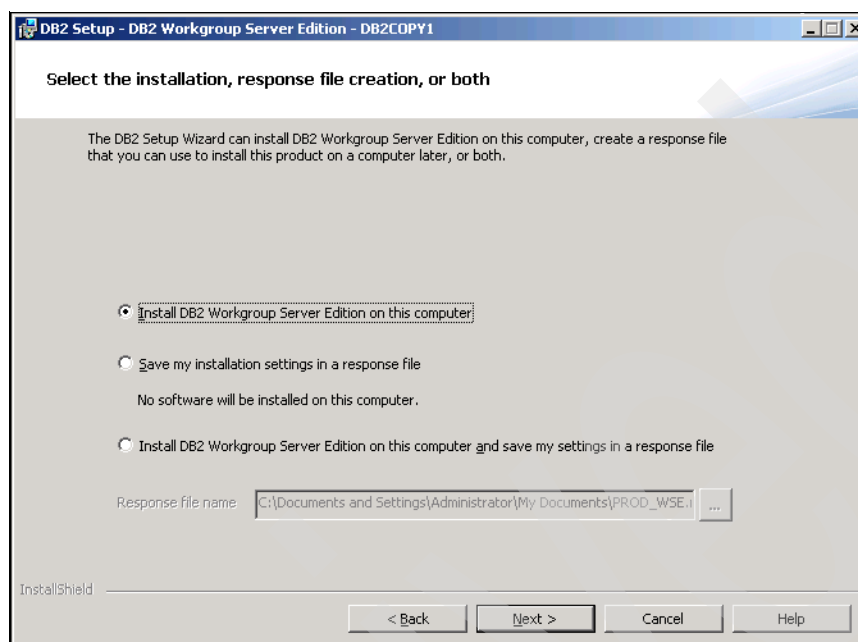


Figure 2-7 Select the installation, response file creation, or both

7. Select the installation location (Figure 2-8). Click **Change** to select a different folder. Click **Next**.

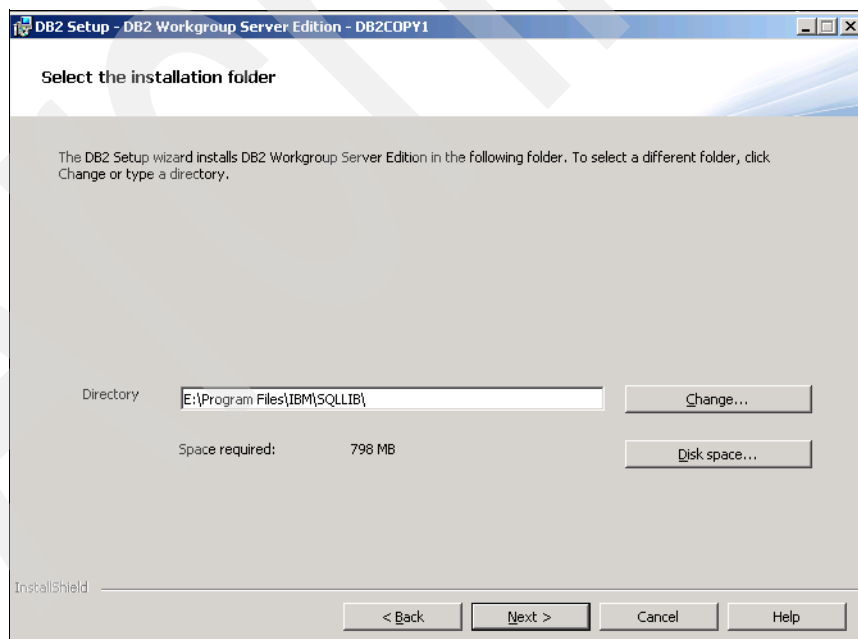


Figure 2-8 Select the installation folder

8. Define a DB2 administrator account and specify a password (Figure 2-9). When finished, click **Next**.

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. Specify the required user information for the DAS.

It is highly recommended that you use a local user or domain user account instead of the LocalSystem account. Further details are available by clicking Help.

☒ Local user or Domain user account

☐ LocalSystem account

☒ Use the same account for the remaining DB2 services

InstallShield

< Back Next > Cancel Help

Figure 2-9 Set user information for the DB2 Administration Server

9. On the Configure DB2 instances page (Figure 2-10), you are presented with the default DB2 instance, You do not have to specify additional configuration options for the default instance. Click **Next** to continue.

Configure DB2 instances

The following instances will be created during installation. You can customize the configurations by clicking on the Configure button.

DB2 Instances:

DB2

Configure...

Instance description

The default instance, DB2, stores application data.

InstallShield

< Back Next > Cancel Help

Figure 2-10 Configure DB2 instances

10. You do not need to prepare the DB2 tools catalog (Figure 2-11). Click **Next** to continue.

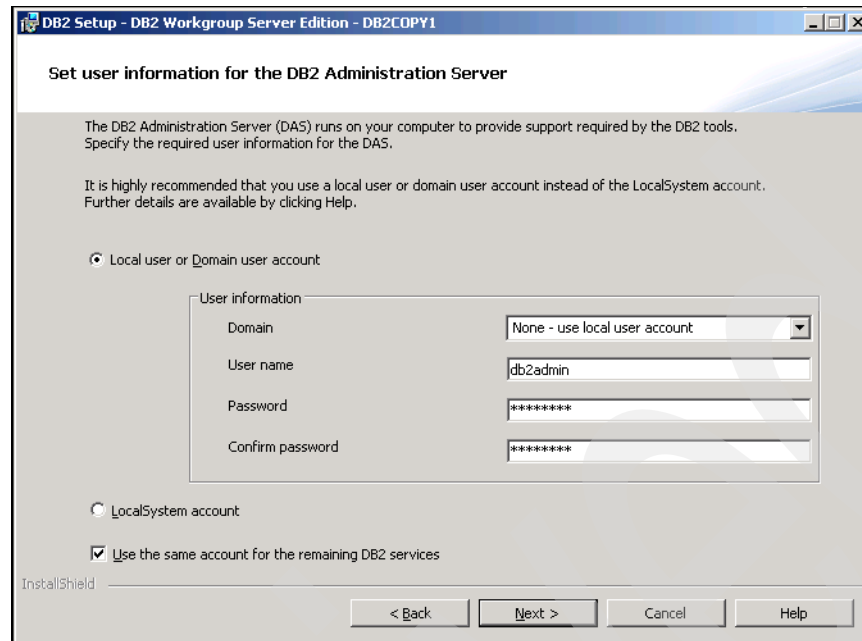


Figure 2-11 Prepare the DB2 tools catalog

11. On the Set up notifications page (Figure 2-12), uncheck the "Set up your DB2 server to send notifications" selection. Click **Next** to continue.

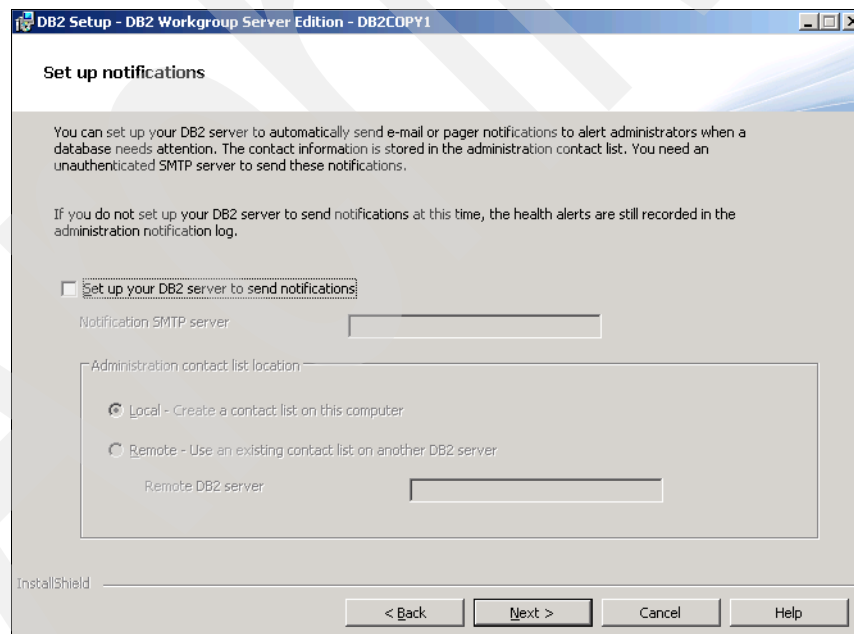


Figure 2-12 Set up notifications

12. Enable operating system security for the database server and accept the defaults (Figure 2-13). When finished, click **Next** to continue.

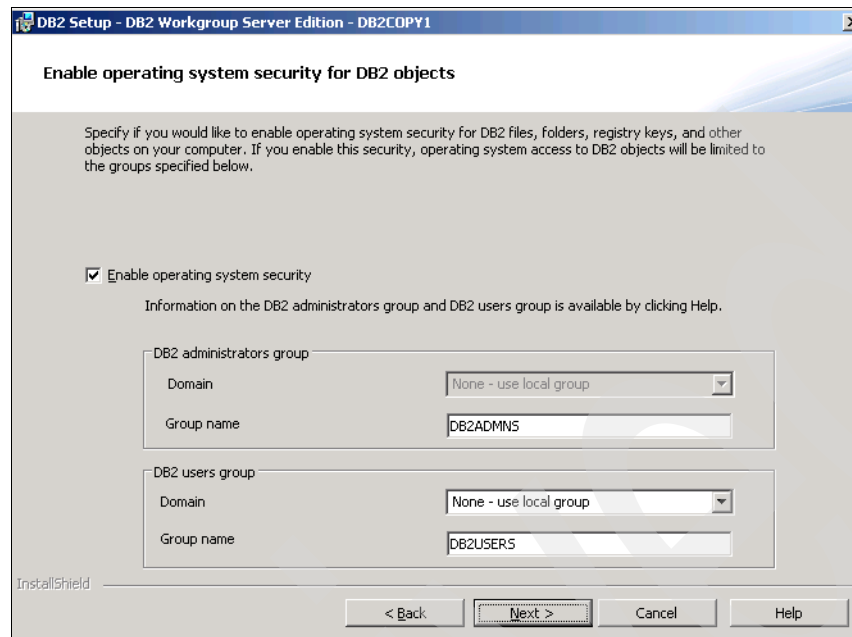


Figure 2-13 Enable operating system security for DB2 objects

13. Verify the settings on the Start copying files page and click **Install** (Figure 2-14).

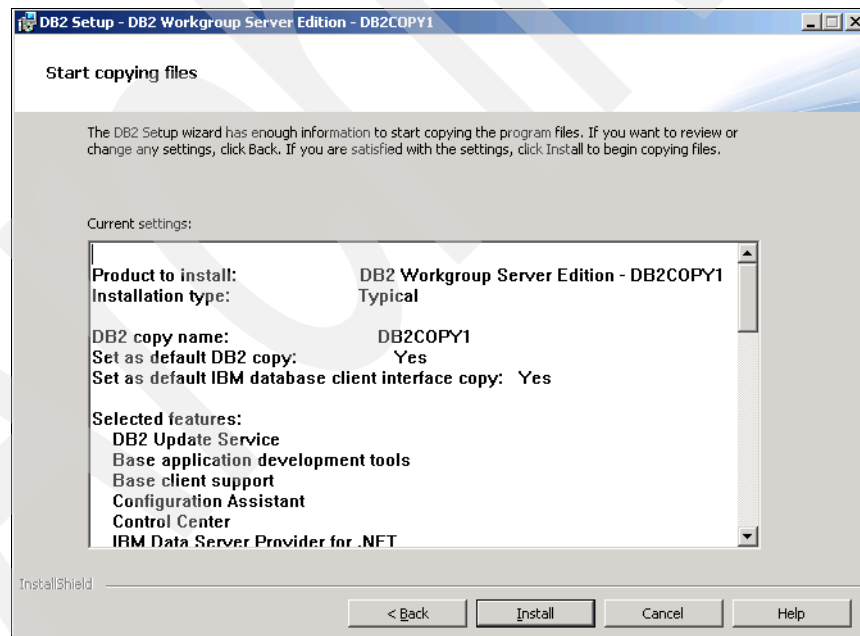


Figure 2-14 Start copying files

14. Wait for the installation to complete (Figure 2-15).

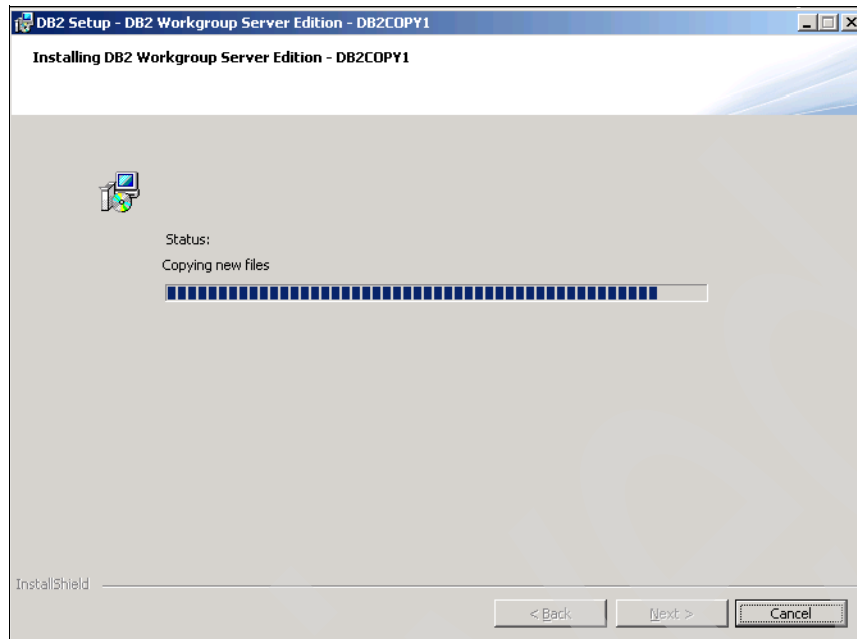


Figure 2-15 Installing DB2 Workgroup Server Edition - DB2COPY1

15. The Setup is complete page displays on completion of the install (Figure 2-16). Note the port number. This is 50000 by default. Click **Next** to complete the install and exit the installer.

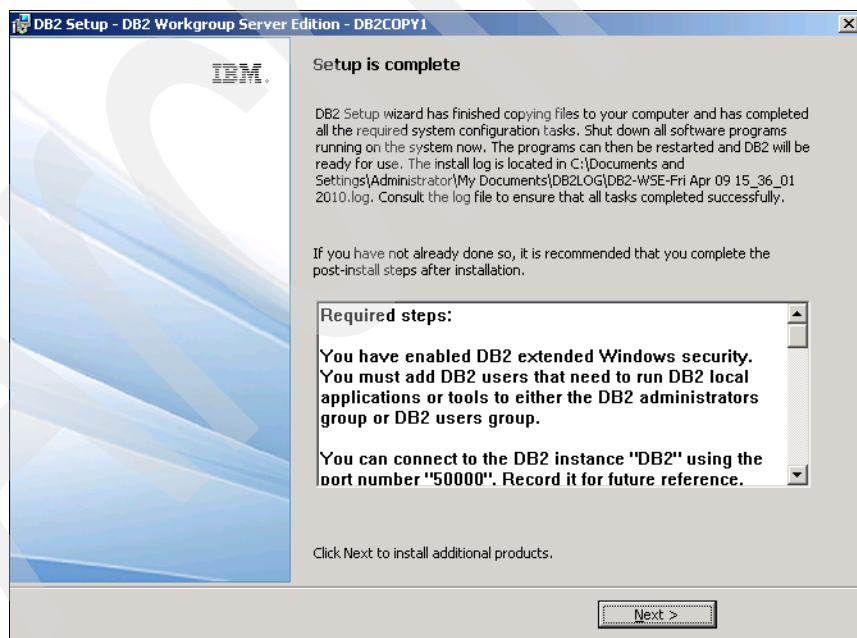


Figure 2-16 Setup is complete

2.1.2 Configuring DB2

To configure DB2 follow the steps below:

1. Create the IMS database using either the DB2 Control center or by entering the appropriate commands.
2. Configure DB2 via the Control Center:
 - a. In the Control Center, click the **Create New Database** link to start the Create Database wizard (Figure 2-17).
 - b. Enter a name for the database (such as IMSDB), specify an alias (such as IMSDB), and specify a path for the database (such as E:\).
 - c. Ensure that the default buffer pool and table space page size are set to 8 K. Click **Next** to continue.

Create Database Wizard

1. Name
2. Storage
3. Region
4. Summary

Specify a name for your new database

This wizard helps you create and tailor a new database. To create a basic database, type a new name, select a drive, and click Finish. If you want to tailor the database to your requirements, click Next to continue. [Task Overview.](#)

Database name:

Default path: ...

Alias:

Comment:

☐ Restrict access to system catalogs

☒ Let DB2 manage my storage (automatic storage)

☐ I want to manage my storage manually

Default bufferpool and table space page size:

Next > Finish Cancel

Figure 2-17 Specify a name for your new database

3. Verify that Use the database path as a storage path is checked (Figure 2-18) and click **Next** to continue.

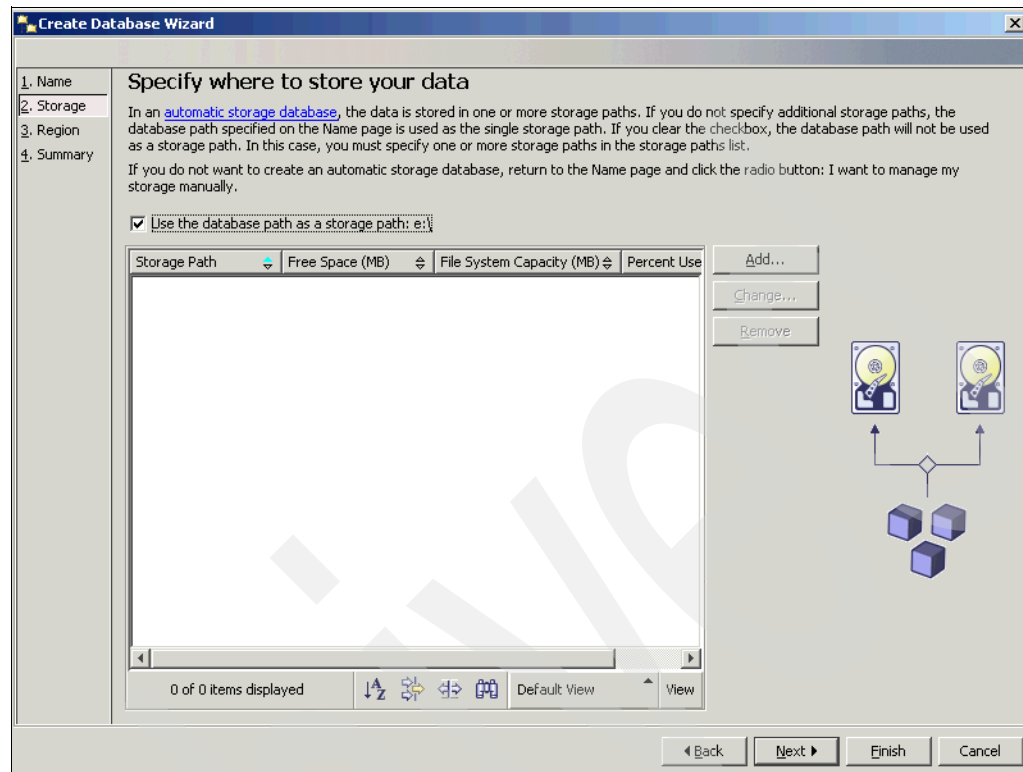


Figure 2-18 Specify where to store your data

4. Ensure that System is selected for the collating sequence and UTF-8 for the code set (Figure 2-19). Select the country/region and territory (for example, default for Country/Region) and US for territory. Select the code-set as UTF-8 and click **Next**.

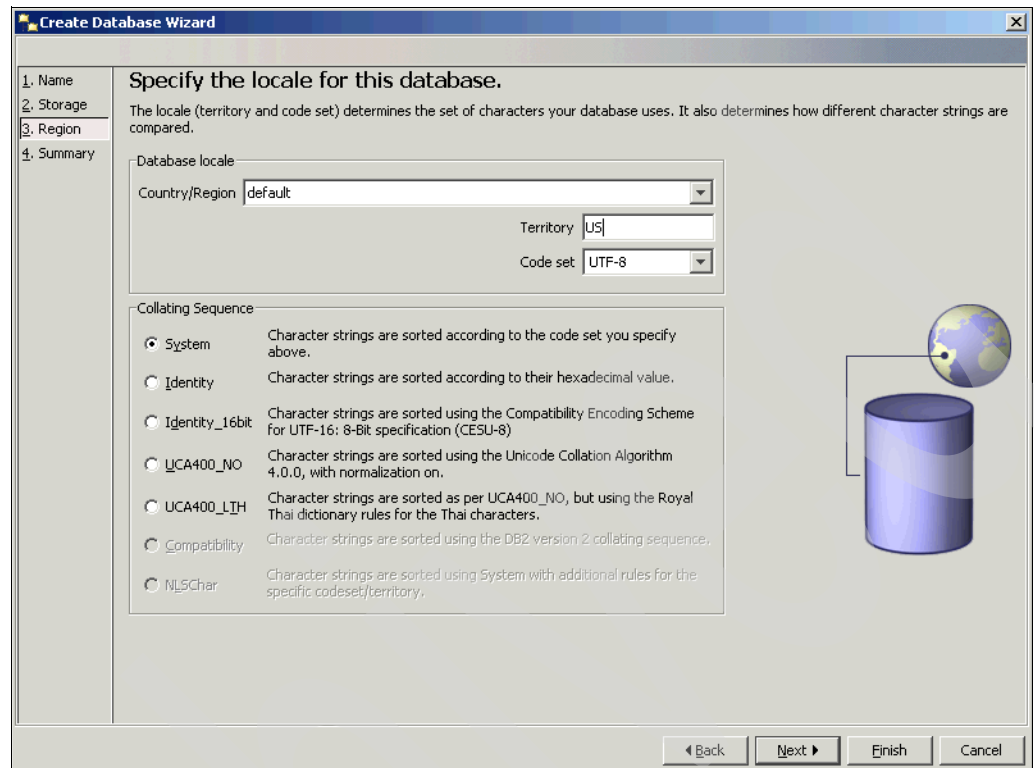


Figure 2-19 Specify the locale for this database

5. Review the options for creating the database (Figure 2-20) and click **Finish** to create the database.

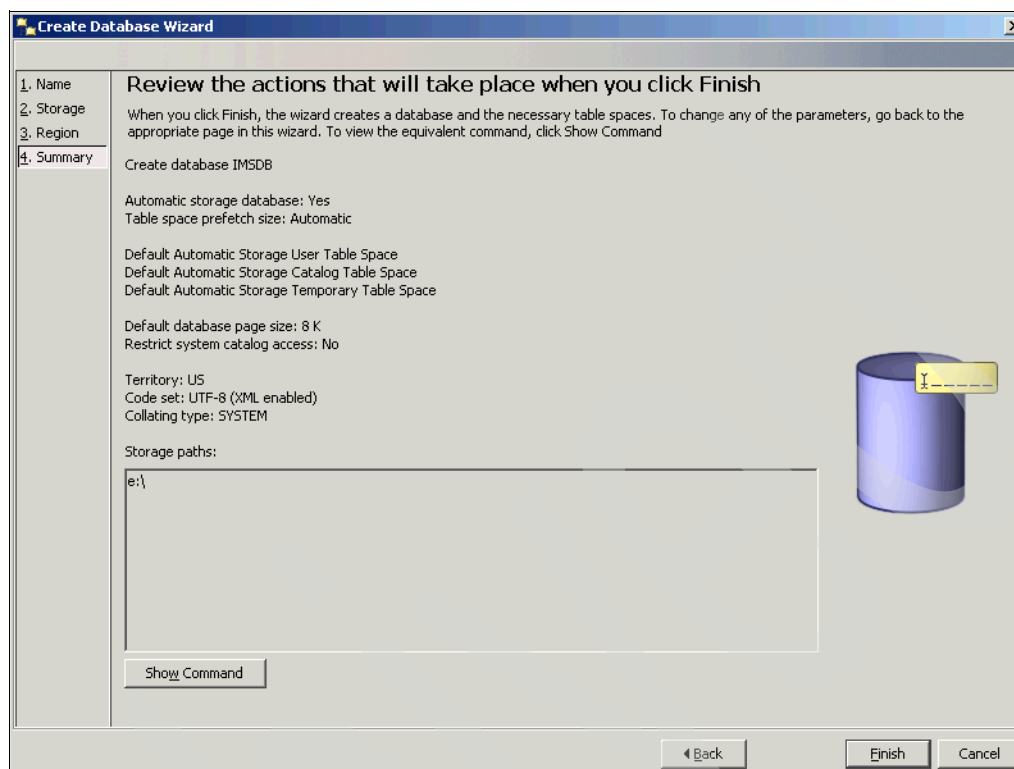


Figure 2-20 Review the actions that will take place when you click Finish

2.2 WebSphere Application Server Network Deployment

This section details the installation of IBM WebSphere Application Server Network Deployment.

Before starting the installation, ensure that the installation user has the following permissions:

- Act as part of the operating system
- Log on as a service

Note: The part number for the IBM WebSphere Application Server Network Deployment V7.0 for Windows on x86-32 bit installation package is C1G2GML. The part number for the IBM HTTP Server, HTTP plug-in, and Update Installer for IBM WebSphere Application Server Network Deployment V7.0 Windows x86-32 bit installation package is C1G2HML.

To install:

1. Run `launchpad.exe` (Figure 2-21). Click **Launch the installation wizard for WebSphere Application Server Network Deployment** to install IBM WebSphere using the installation wizard.

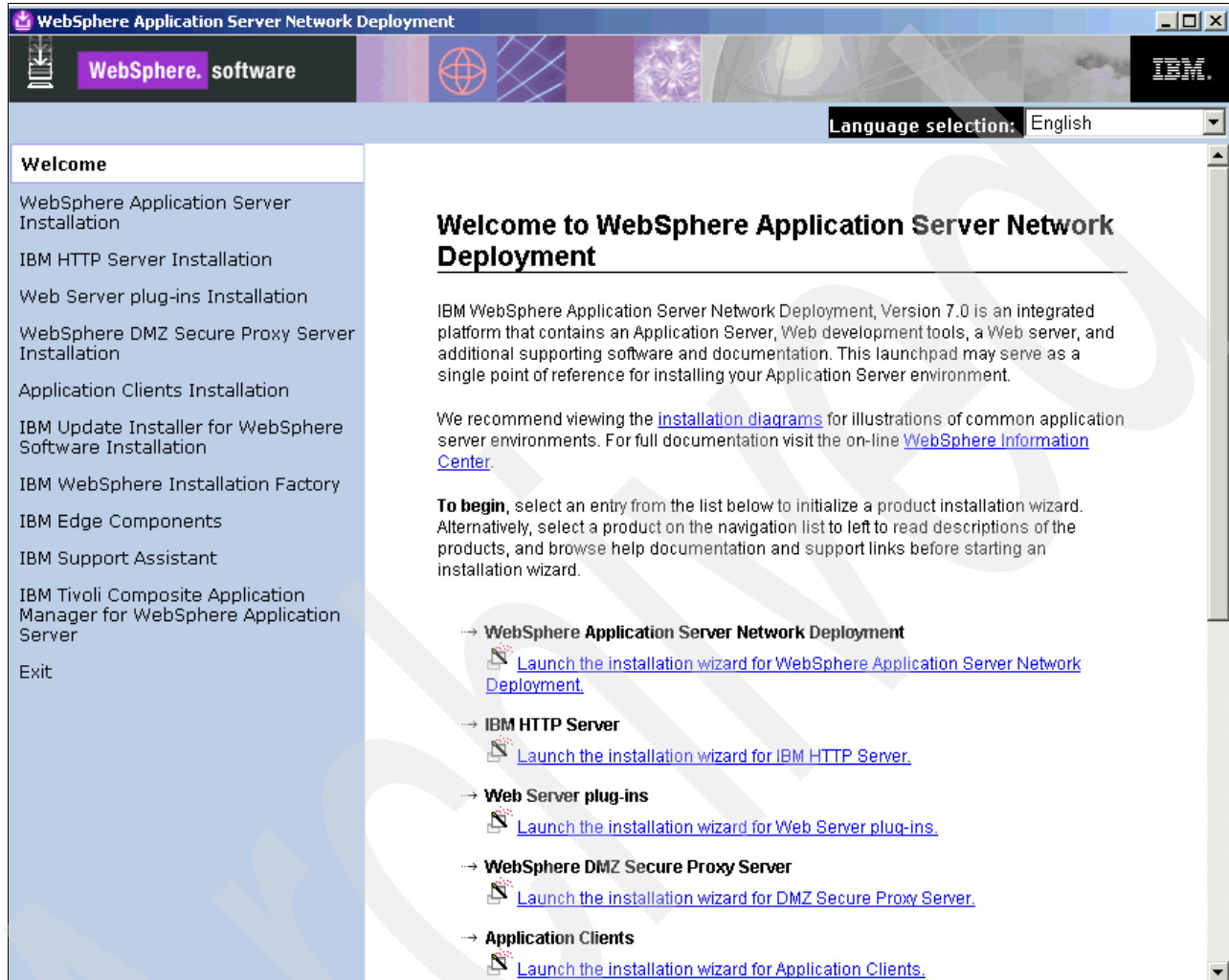


Figure 2-21 Welcome to WebSphere Application Server Network Deployment

Click **Next** to continue on the Welcome to the IBM WebSphere Application Server Network Deployment Installation wizard page (Figure 2-22).

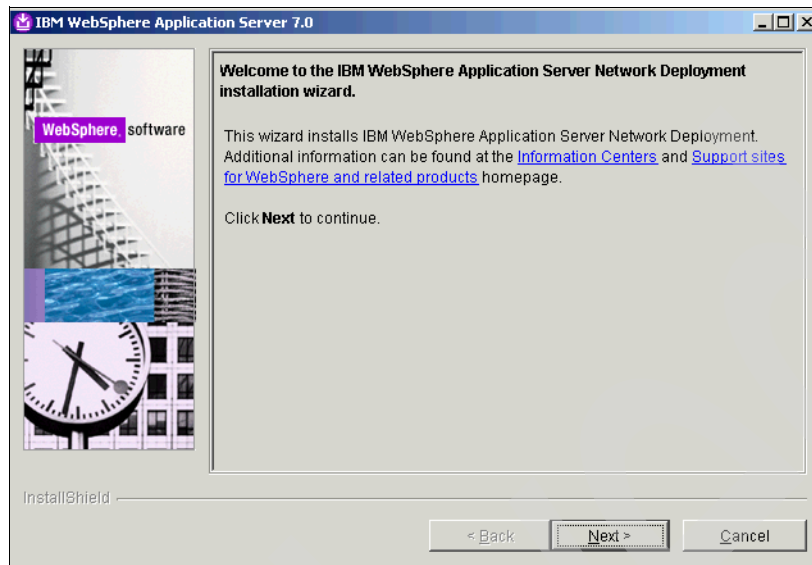


Figure 2-22 Welcome

2. On the Software License Agreement page (Figure 2-23), accept the IBM and non-IBM terms for the license agreement and click **Next**.

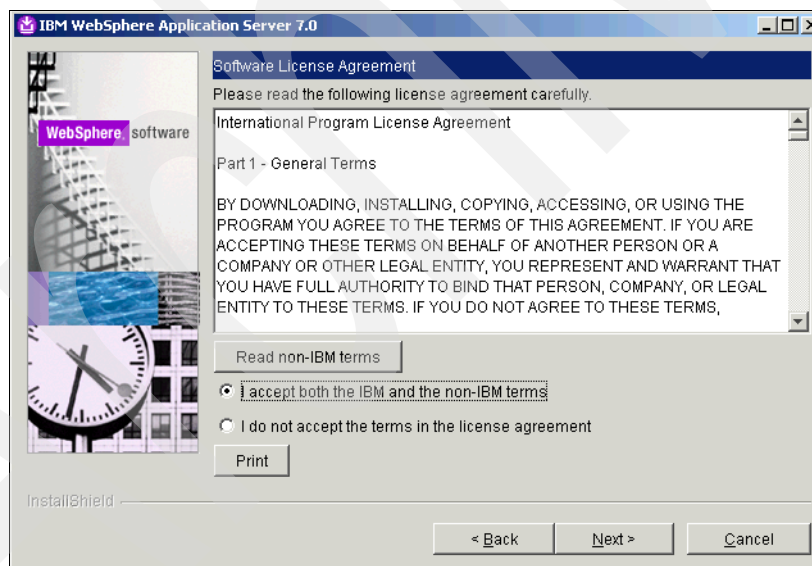


Figure 2-23 Software License Agreement

3. On the system Prerequisites Check page (Figure 2-24), click **Next** when you see the message that your operating system completed the prerequisites check successfully.

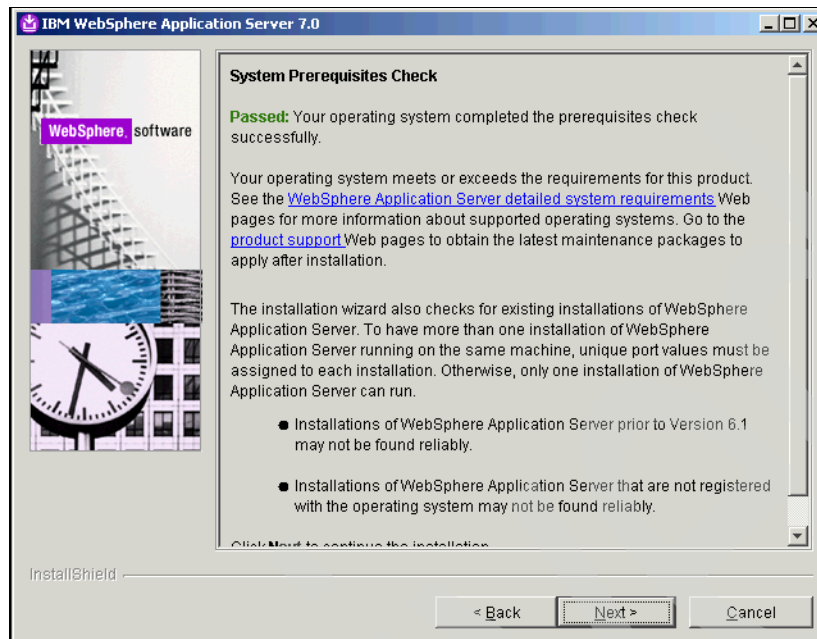


Figure 2-24 System Prerequisites Check

4. From the Optional Features Installation page (Figure 2-25), we do not install any of the sample applications/language packs. Click **Next** to continue.

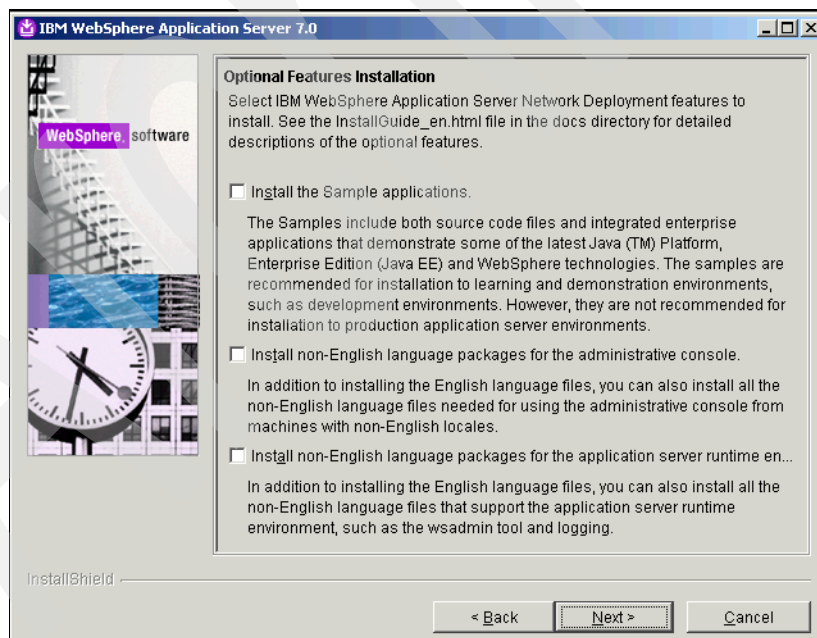


Figure 2-25 Optional Features Installation

5. Accept the default installation directory or modify it as needed (Figure 2-26), and click **Next**.

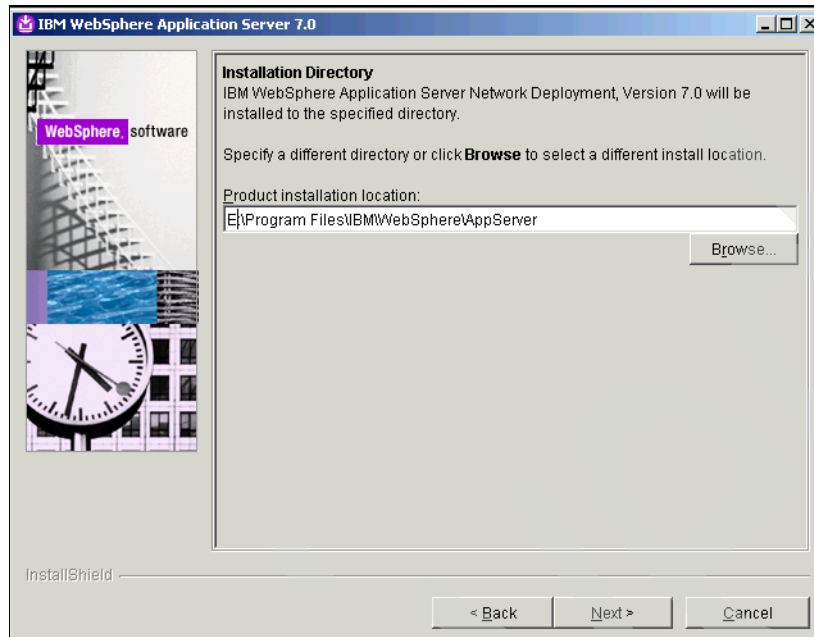


Figure 2-26 Installation Directory

6. On the WebSphere Application Server Environments page (Figure 2-27), select **None** from the list of environments. We configure a profile later in the deployment. Click **Next** to continue.

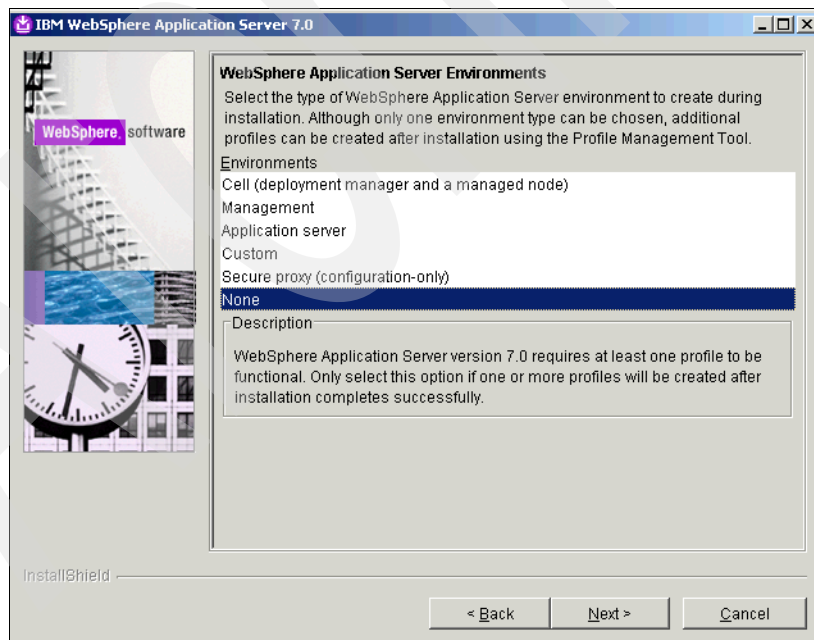


Figure 2-27 WebSphere Application Server Environments

7. A warning message displays (Figure 2-28). Ignore this message for the moment and click **Yes** to continue.

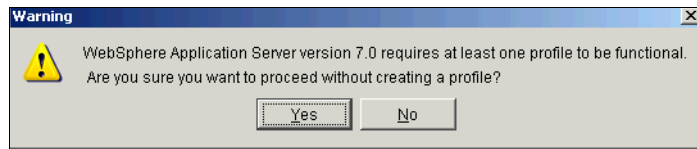


Figure 2-28 Warning

8. Select the Create a repository for Centralized Installation Managers check box (Figure 2-29).

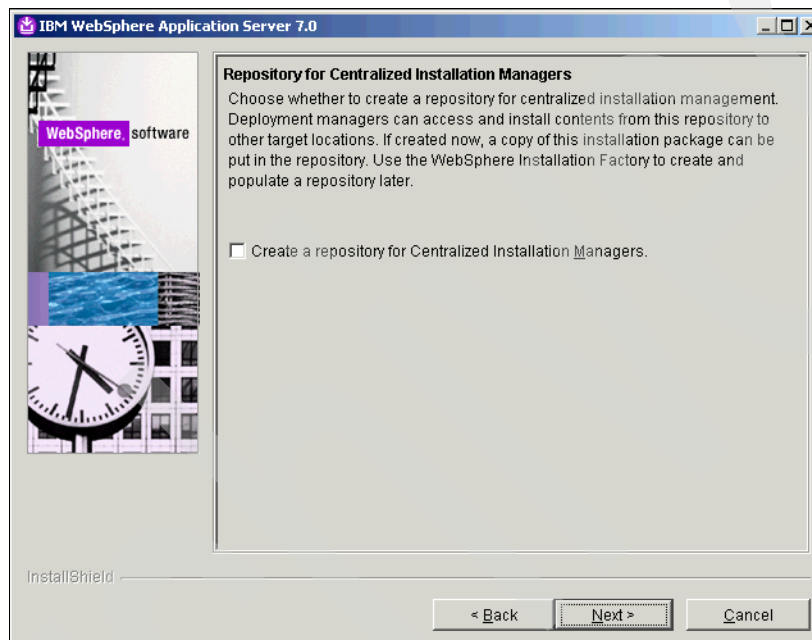


Figure 2-29 Repository for Centralized Installation Managers

9. You are then prompted for the directory path of the repository (Figure 2-30). Modify the directory path (if necessary) and click **Next** to continue.

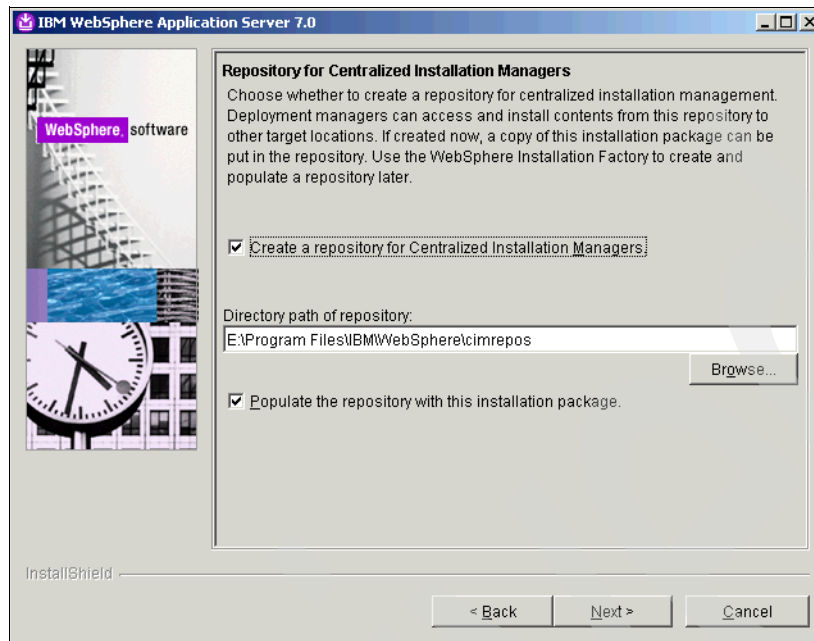


Figure 2-30 Repository for Centralized Installation Managers

10. On the Installation Summary page, review the installation (Figure 2-31) and click **Next**.

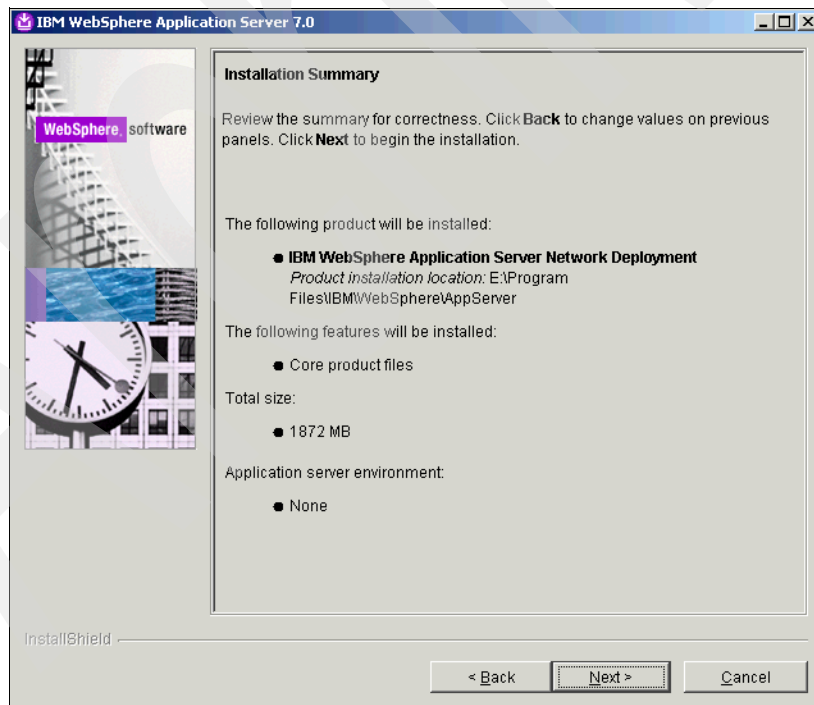


Figure 2-31 Installation Summary

11. On the Installation Results page, when you see the success message (Figure 2-32), uncheck **Create a new WebSphere Application Server Profile using the Profile Management Tool** and click **Finish** to complete the installation.

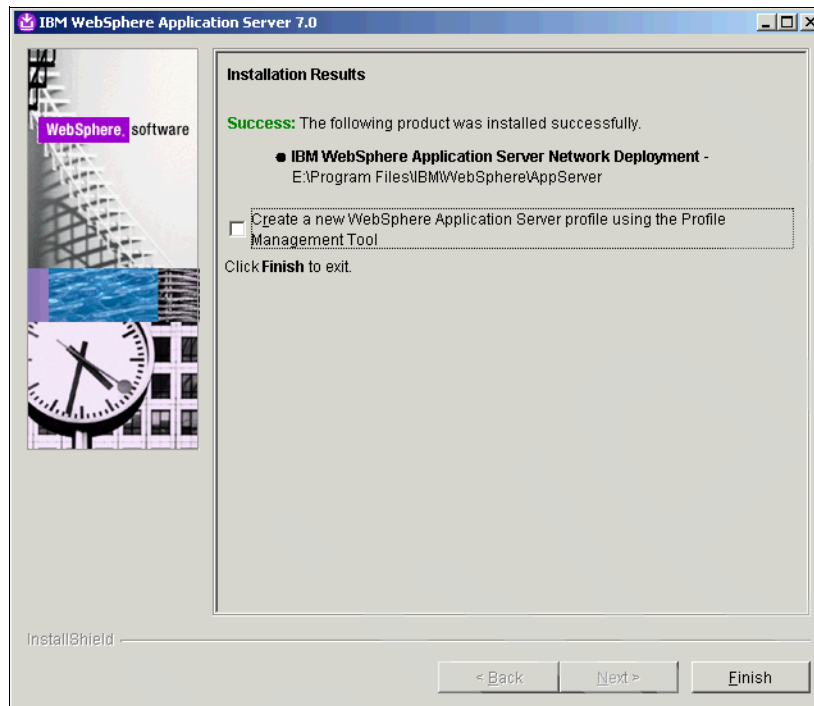


Figure 2-32 Installation Results

2.2.1 WebSphere Update Installer

The Update Installer is needed to install the HTTP Server, WebSphere Application Server fix packs, and the IMS fix packs. The update installer software is available with the WebSphere Application Server installation V7.0. Because we need to install a later version of the Update Installer (V 7.0.0.7 or later), you need to obtain the software installation package from the IBM support site and run the installation setup as shown in the following steps:

1. Run `install.exe` to start the Installation wizard for the update installer (Figure 2-33). Click **Next** to continue with the installation.

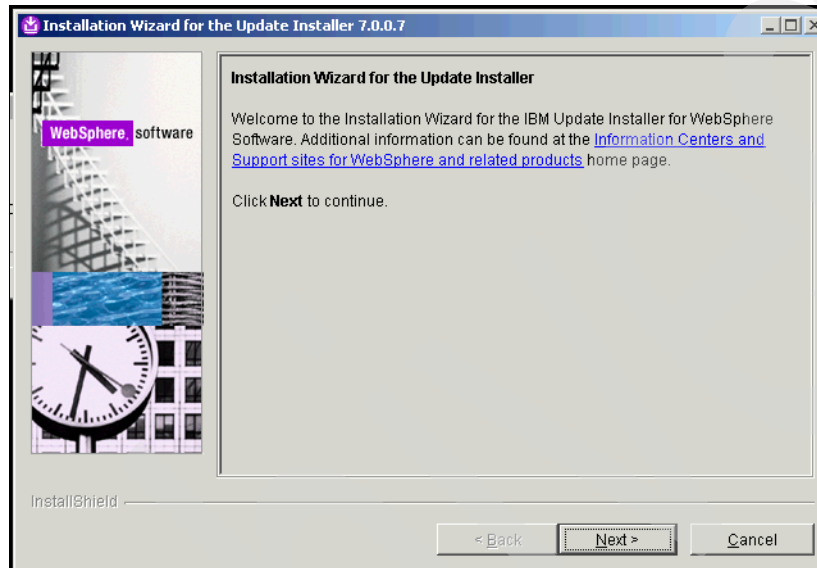


Figure 2-33 Installation Wizard for the Update Installer

2. From the Software License Agreement page (Figure 2-34), accept the IBM and non-IBM terms and click **Next**.

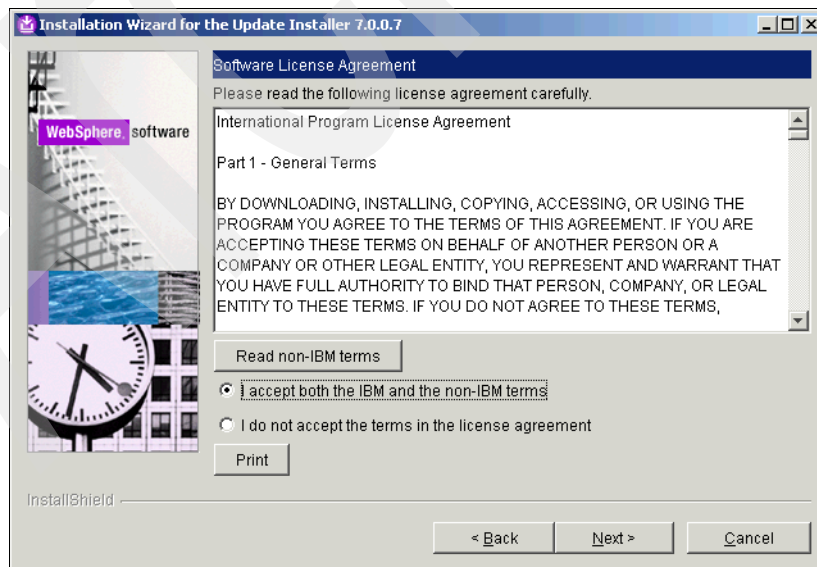


Figure 2-34 Software License Agreement

3. Click **Next** when you get the passed status on the System Prerequisite Check page (Figure 2-35).

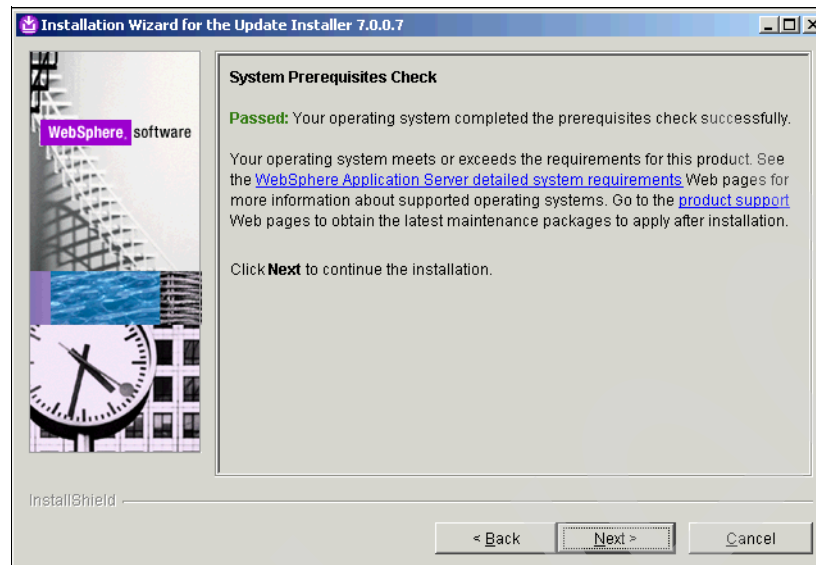


Figure 2-35 System Prerequisites Check

4. Change the directory location if necessary and click **Next**. You can create a start menu icon by clicking the check box.
5. On the Installation Summary page (Figure 2-36), click **Next** to continue.

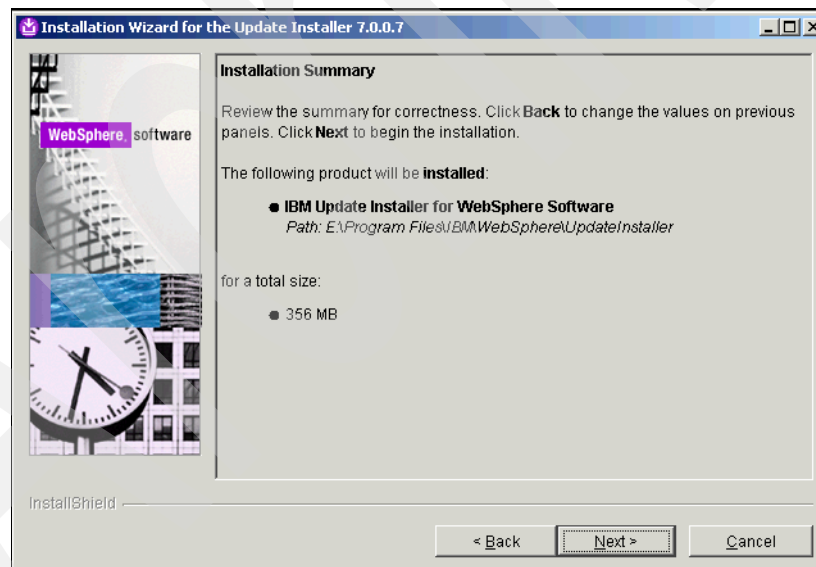


Figure 2-36 Installation Summary

6. Click **Finish** to complete the installation (Figure 2-37).

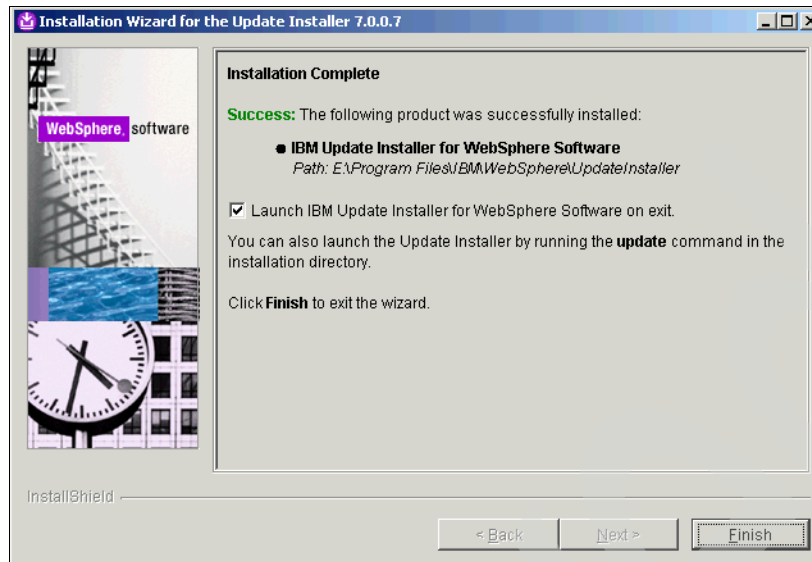


Figure 2-37 Installation Complete

The IBM Update Installer (V7.0.0.7) has been successfully installed.

2.2.2 WebSphere fix pack

For the purpose of this installation, the WebSphere Application Server fix packs can be copied to any standard directory on the local system. For this WebSphere deployment, we copy all the updates and fix packs to the Update Installer maintenance directory (for example, E:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance).

1. Run `update.bat` (from the E:\Program Files\IBM\WebSphere\UpdateInstaller directory) to start the IBM Update Installer for WebSphere Software wizard (Figure 2-38). Click **Next** to proceed with the upgrade process.

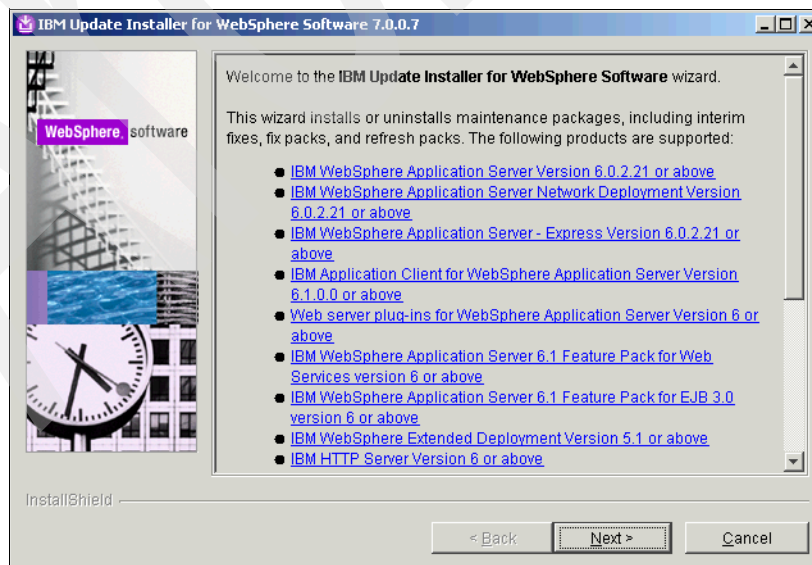


Figure 2-38 Welcome to the IBM Update Installer for WebSphere Software wizard

2. Select **WebSphere\AppServer** from the drop-down menu (Figure 2-39) and click **Next** to continue.

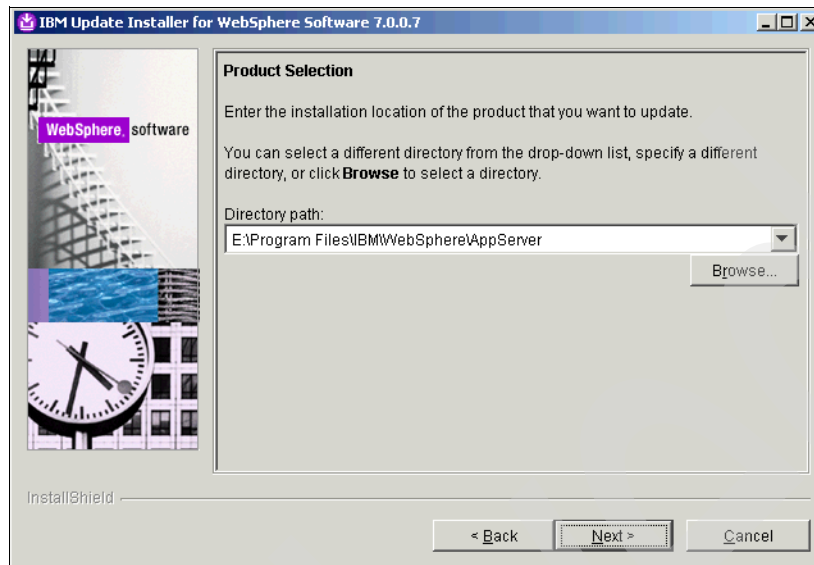


Figure 2-39 Product Selection

3. Select **Install maintenance package** (Figure 2-40) and click **Next** to continue.

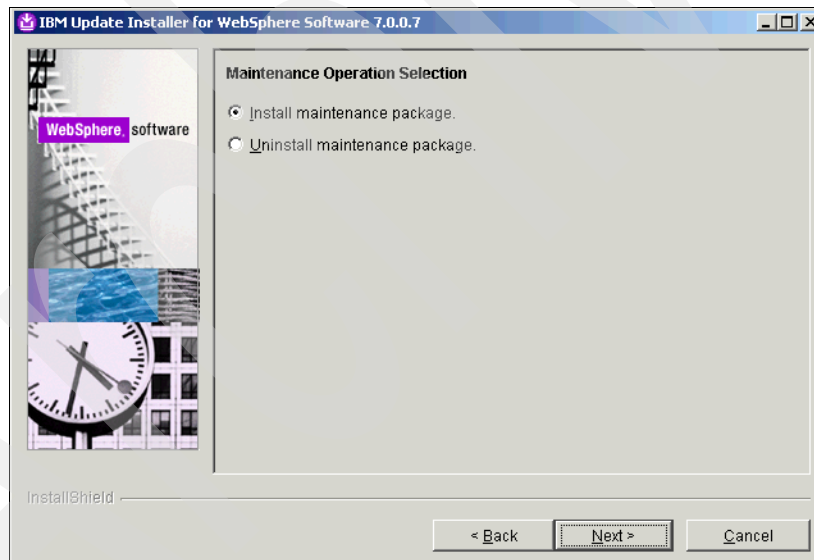


Figure 2-40 Maintenance Operation Selection

4. Browse to and specify the location of the fix pack (Figure 2-41). (This is the directory to which you copied the maintenance packages. For this example, it is E:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance). When finished, click **Next**.

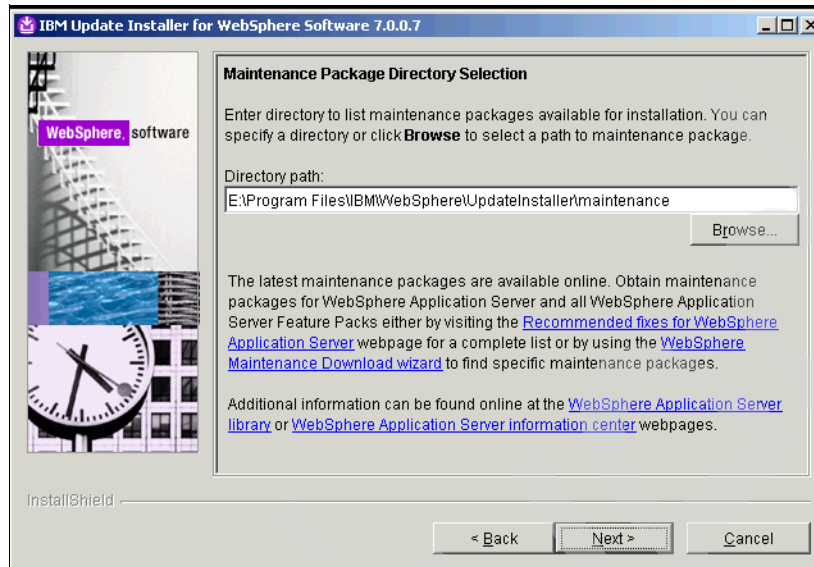


Figure 2-41 Maintenance Package Directory Selection

5. On the Available Maintenance Package to Install page (Figure 2-42), accept the WAS-WinX32-FP0000007.pak and click **Next**.

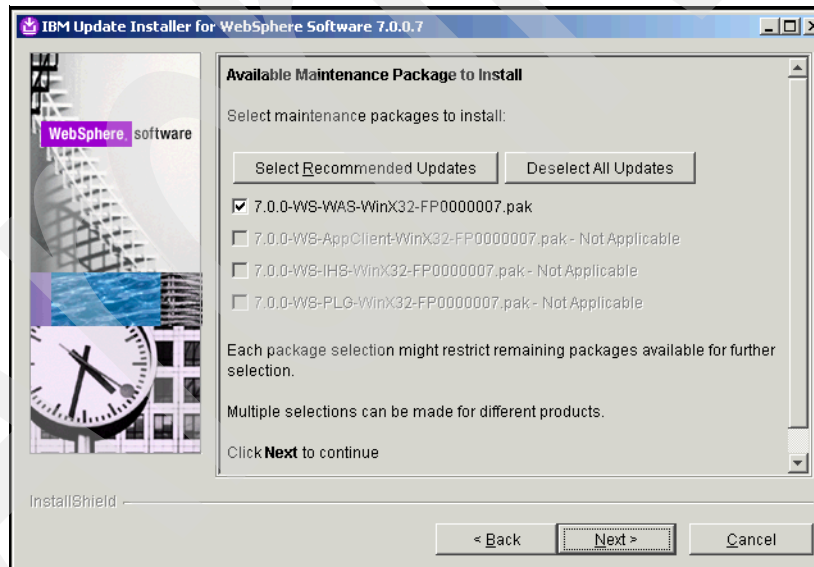


Figure 2-42 Available Maintenance Package to Install

Click **Next** on the Installation Summary page (Figure 2-43) and wait for the installation to complete.

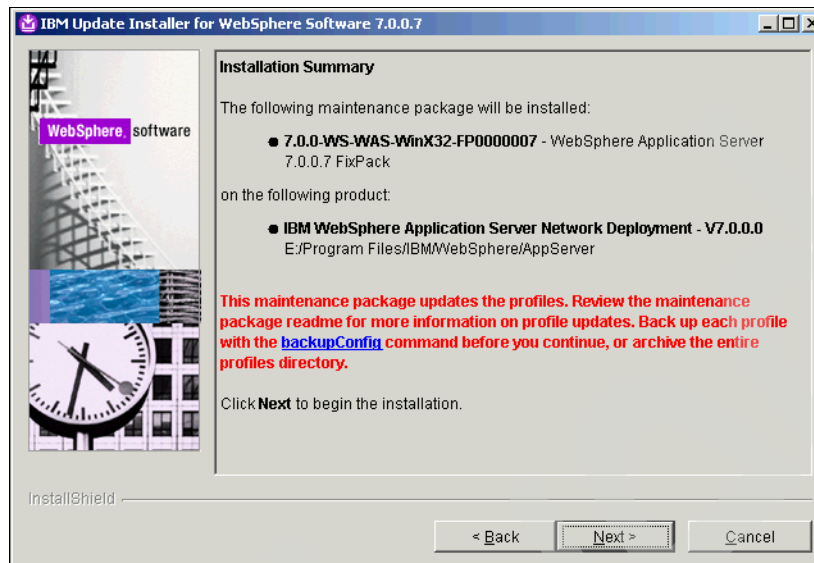


Figure 2-43 Installation Summary

6. When the success message is displayed on the Installation Complete page (Figure 2-44), click **Finish** to exit the wizard.

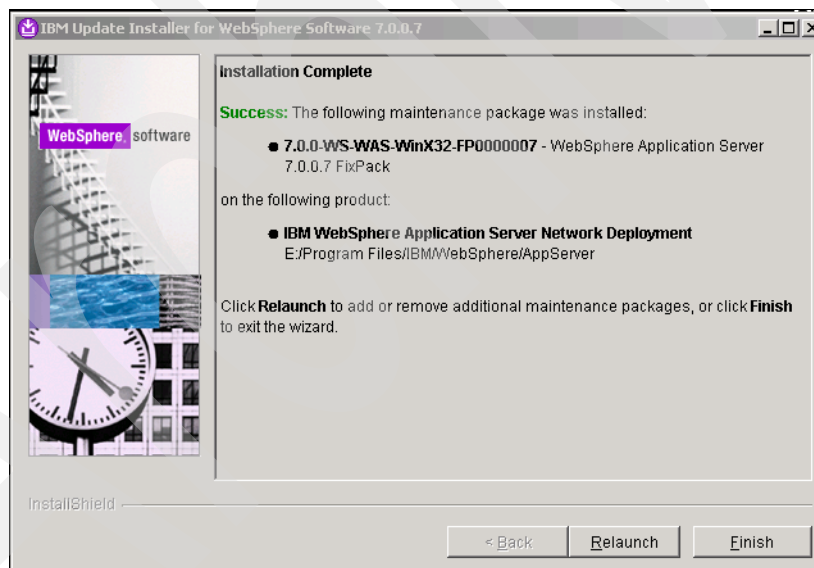


Figure 2-44 Installation Complete

Note: You will need to repeat the above installation steps on all servers/nodes to be added to the WebSphere Application Server cluster that will host the IMS Server.

Creating WebSphere profiles

In this section we create a Deployment Manager and a custom profile using the WebSphere Profile Management Tool.

Creating a Deployment Manager profile

To do this follow the steps below.

1. Launch the WebSphere Profile Management Tool from the appropriate program group. Click **Start** → **All Programs** → **IBM WebSphere** → **Application Server Network Deployment V7.0** → **Profile Management Tool** (Figure 2-45).

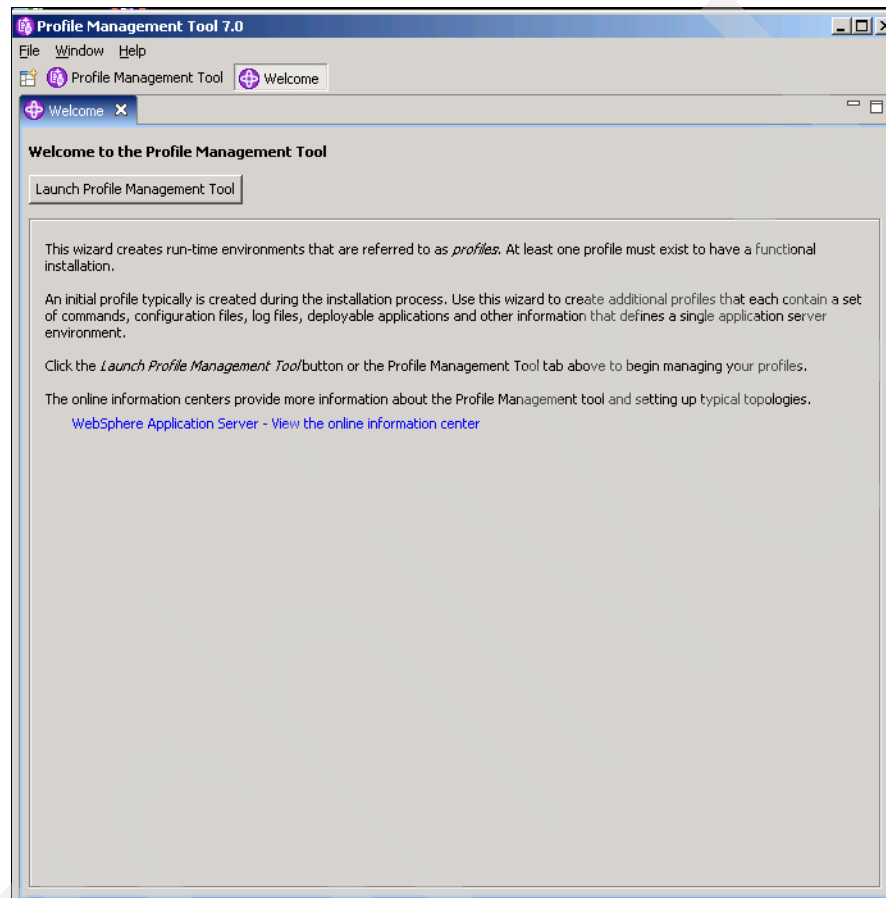


Figure 2-45 Welcome to the Profile Management Tool

2. Click **Create** to create a new profile (Figure 2-46).

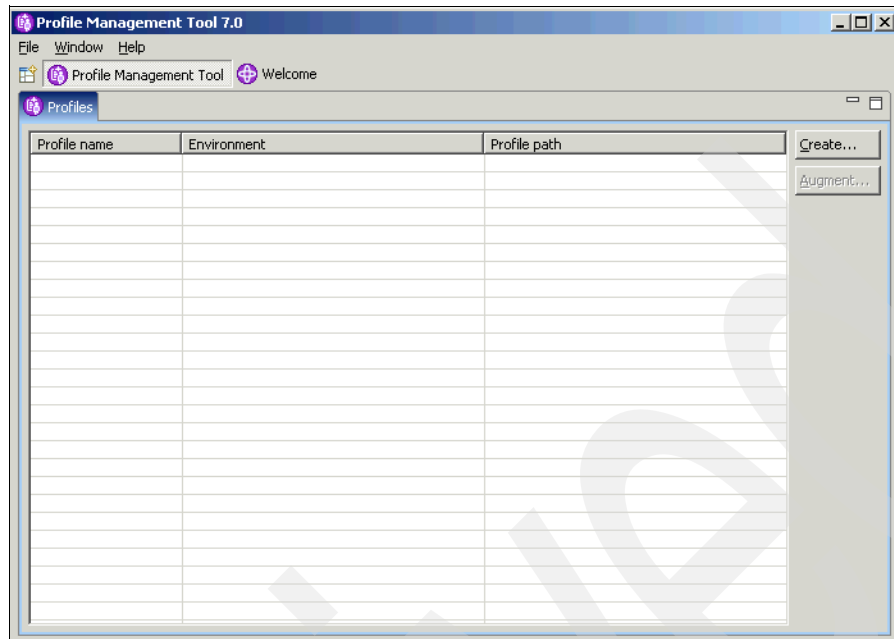


Figure 2-46 Profile Management Tool 7.0 - Profiles tab

3. For the type of WebSphere Application Server environments, select **Management** and click **Next** (Figure 2-47).

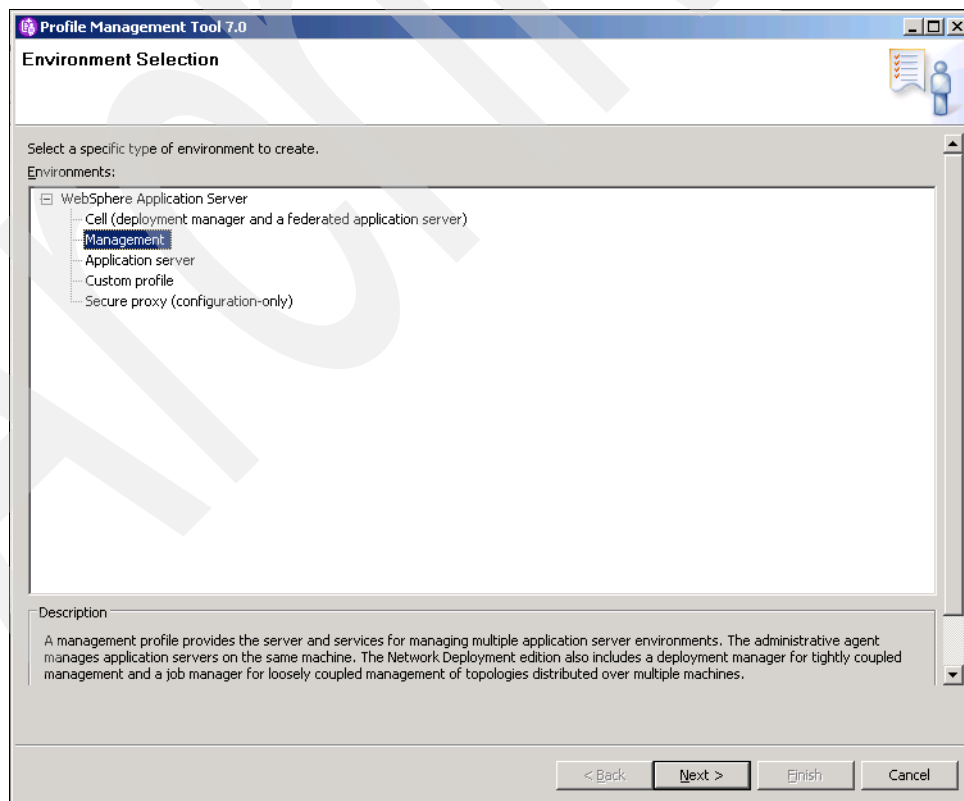


Figure 2-47 Environment Selection

4. On the Server Type Selection page (Figure 2-48), select **Deployment manager** and click **Next**.

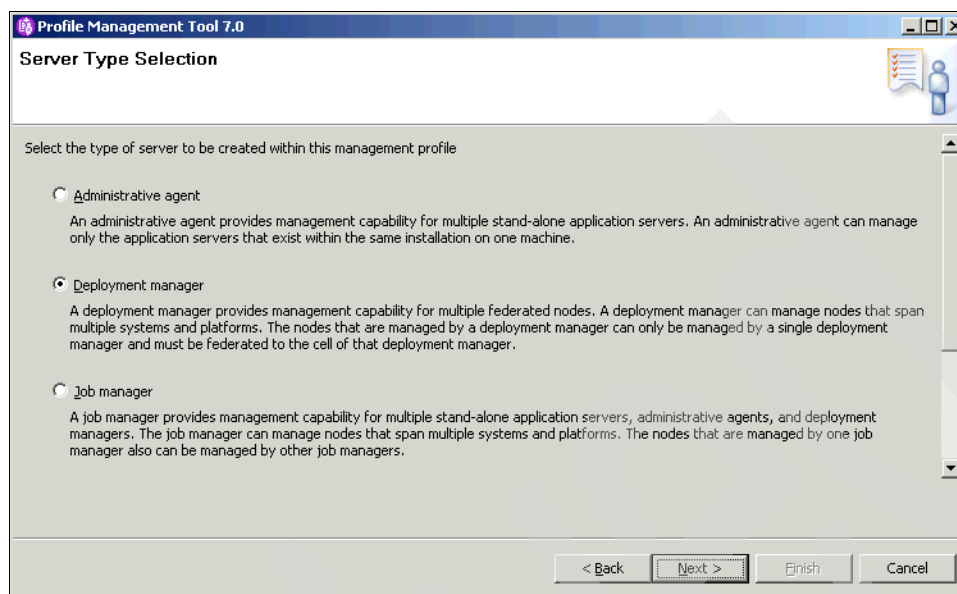


Figure 2-48 Sever Type Selection

5. Select **Typical Profile Creation** (Figure 2-49) and click **Next**.

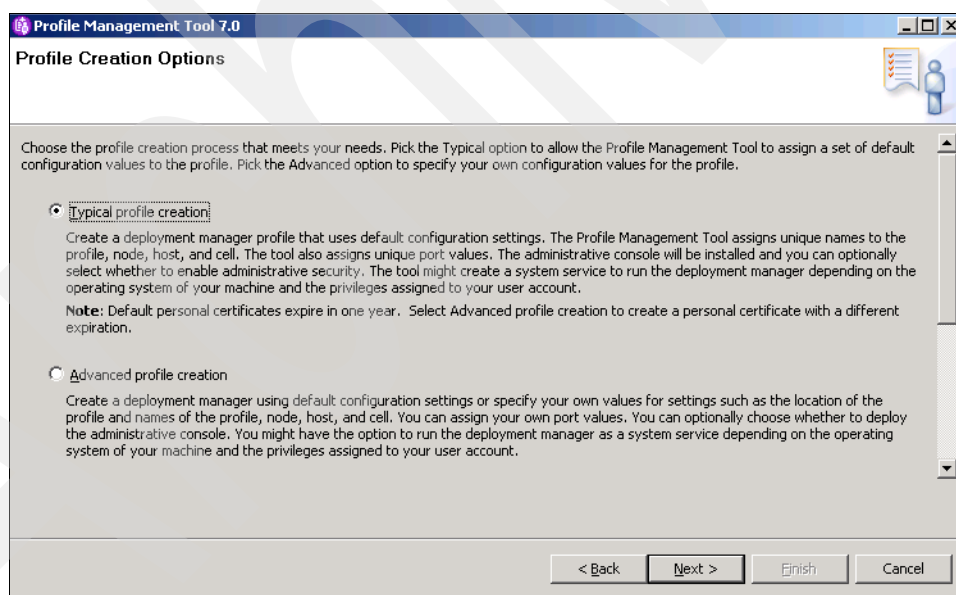


Figure 2-49 Profile Creation Options

- On the Enable Administrative Security page (Figure 2-50), click the **Enable administrative security** check box to enable administrative security. Enter a user name (of your preference) for the WebSphere Application Server administrator to be created (for example, wasadmin), and specify an appropriate password for the user. Re-enter the password for confirmation and click **Next**.

The screenshot shows the 'Administrative Security' window of the Profile Management Tool 7.0. It contains a checkbox labeled 'Enable administrative security' which is checked. Below it are text fields for 'User name' (containing 'wasadmin'), 'Password' (masked with dots), and 'Confirm password' (also masked with dots). A link 'View the online information center' is present. At the bottom are buttons for '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 2-50 Administrative Security

- Review the profile creation details and click **Create** (Figure 2-51).

The screenshot shows the 'Profile Creation Summary' window of the Profile Management Tool 7.0. It displays a summary of the configuration: 'Application server environment to create: Management', 'Server type: Deployment manager', 'Location: E:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01', 'Disk space required: 30 MB', 'Profile name: Dmgr01', 'Make this profile the default: True', 'Cell name: demoCell01', 'Node name: demoCellManager01', 'Host name: demo.tamesso.com', 'Deploy the administrative console (recommended): True', and 'Enable administrative security (recommended): True'. At the bottom are buttons for '< Back', 'Create', 'Finish', and 'Cancel'.

Figure 2-51 Profile Creation Summary

Wait for the profile creation to complete (Figure 2-52).

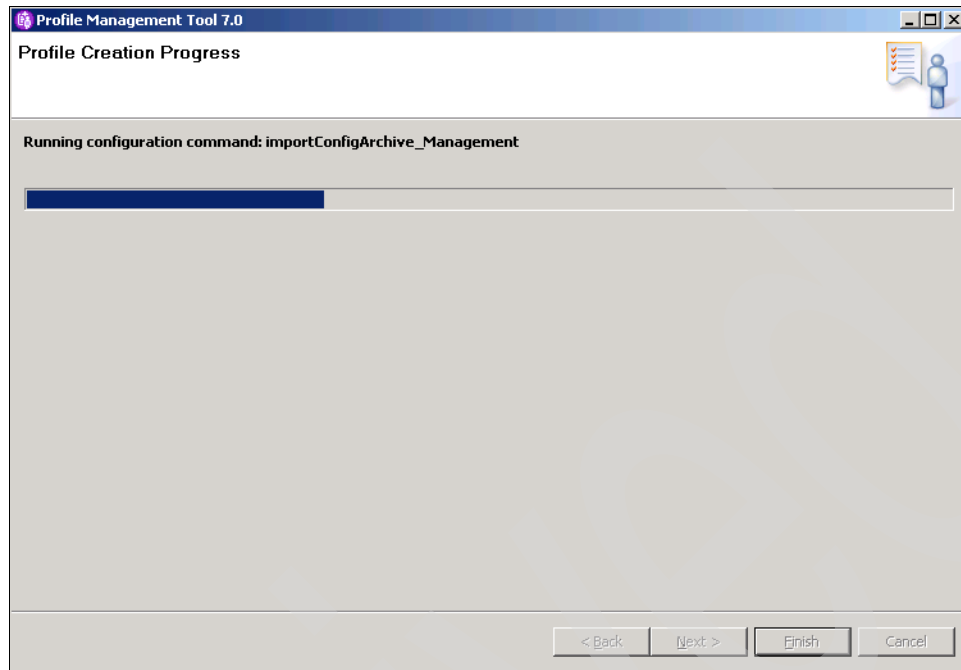


Figure 2-52 Profile Creation Progress

8. When the Profile Creation Complete page displays (Figure 2-53), select the **Launch the First steps console** check box and click **Finish** to display the First Steps page.

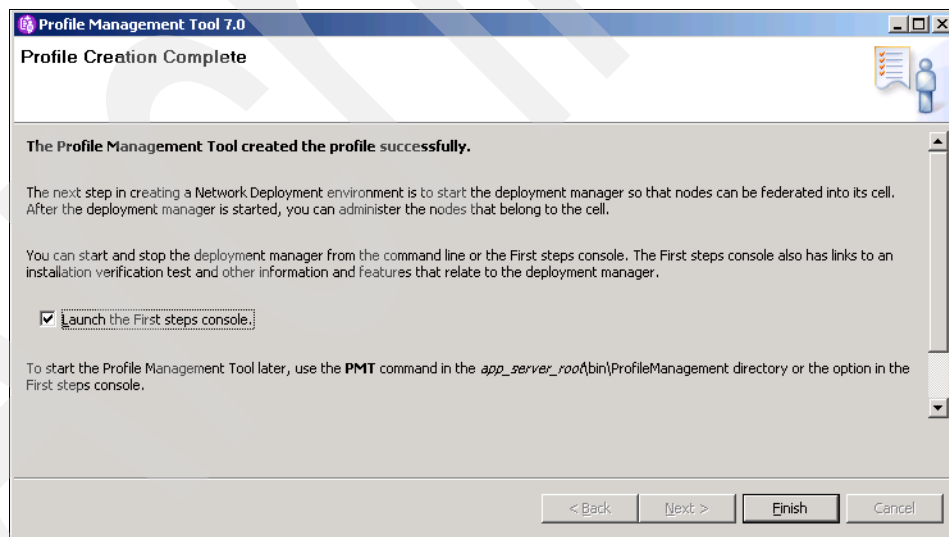


Figure 2-53 Profile Creation Complete



- ## 10. Start the Deployment Manager.

Creating a custom profile

To create a custom profile follow the steps below:

1. Launch the WebSphere Profile Management Tool (by clicking **Start** → **All Programs** → **IBM WebSphere** → **Application Server Network Deployment V7.0** → **Profile Management Tool**).
2. From the Environment Selection page (Figure 2-55), select **Custom profile** and click **Next**.

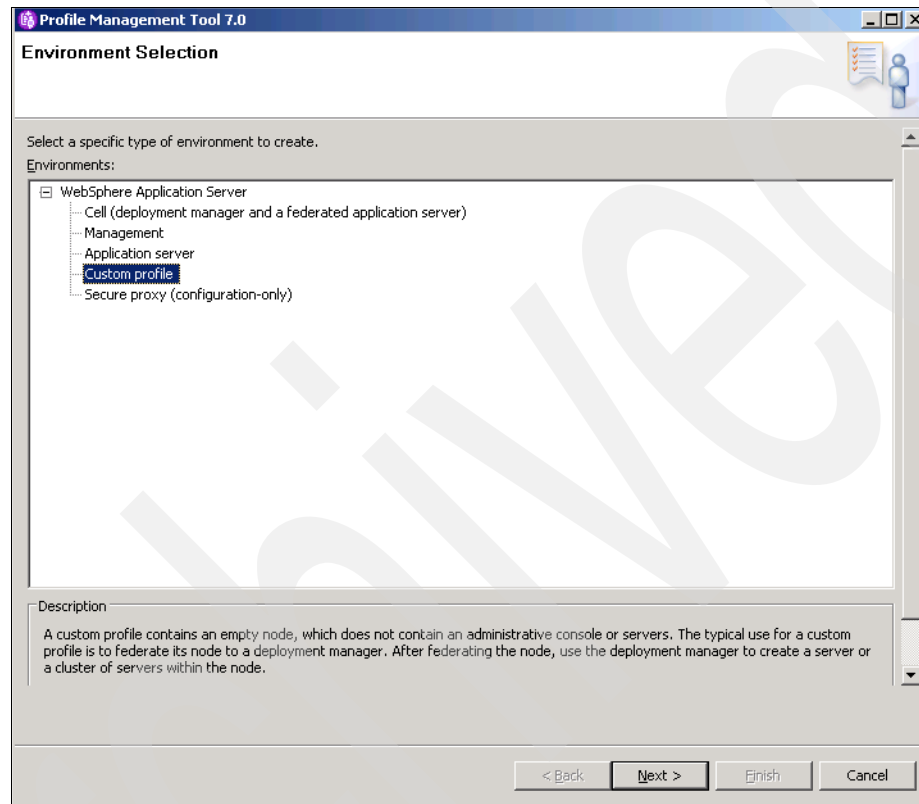


Figure 2-55 Environment Selection

3. From the Profile Creation Options page (Figure 2-56), select **Typical profile creation** and click **Next**.

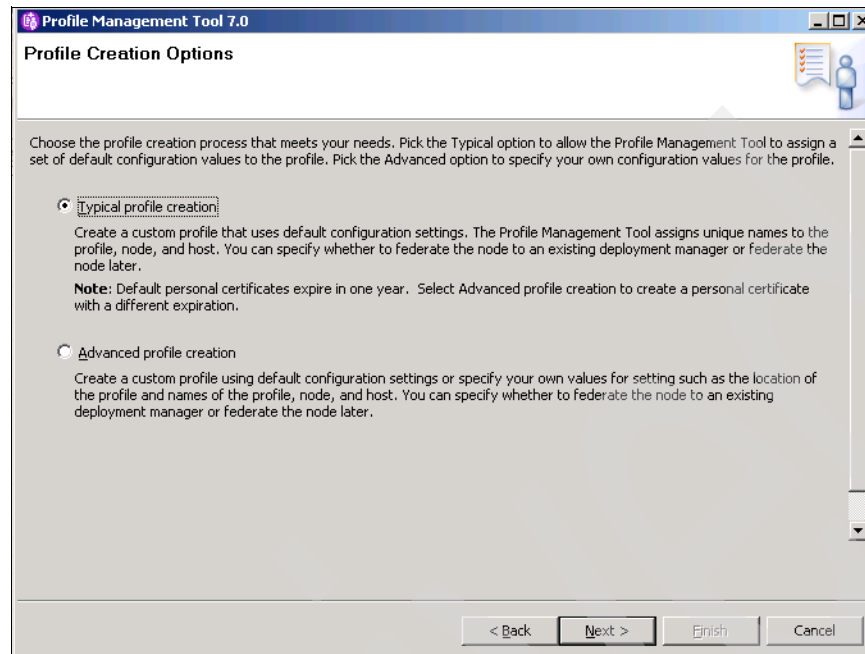


Figure 2-56 Profile Creation Options

4. On the Federation page (Figure 2-57), specify the host name for the Deployment Manager (for example, demo) and accept the default SOAP port number (8879). Also specify the WebSphere Application Server administrator user name and password and click **Next**.

The screenshot shows the 'Federation' window in the Profile Management Tool 7.0. The window title is 'Profile Management Tool 7.0' and the subtitle is 'Federation'. It contains the following fields and options:

- Deployment manager host name or IP address:** A text box containing 'demo'.
- Deployment manager SOAP port number (Default 8879):** A text box containing '8879'.
- Deployment manager authentication:** A section with the instruction 'Provide a user name and password that can be authenticated, if administrative security is enabled on the deployment manager.' It includes:
 - User name:** A text box containing 'wasadmin'.
 - Password:** A text box with masked characters (dots).
- Federate this node later:** An unchecked checkbox.
- Instructions:** 'You must federate this node later using the **addNode** command if the deployment manager:
 - is not running
 - has the SOAP connector disabled

At the bottom, there are four buttons: '< Back', 'Next >', 'Finish', and 'Cancel'.

Figure 2-57 Federation

5. Review the Profile Creation Summary (Figure 2-58) and click **Create**.

The screenshot shows the 'Profile Creation Summary' window in the Profile Management Tool 7.0. The window title is 'Profile Management Tool 7.0' and the subtitle is 'Profile Creation Summary'. It contains the following information:

- Review the information in the summary for correctness. If the information is correct, click **Create** to start creating a new profile. Click **Back** to change values on the previous panels.**
- Application server environment to create:** Custom profile
 - Location:** E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
 - Disk space required:** 10 MB
- Profile name:** Custom01
 - Make this profile the default:** False
- Node name:** demoNode01
 - Host name:** demo.tamesso.com
- Federate to deployment manager:** demo:8879

At the bottom, there are four buttons: '< Back', 'Create', 'Finish', and 'Cancel'.

Figure 2-58 Profile Creation Summary

- Click **Finish** on the Profile Creation Complete page (Figure 2-59).

Note: You can launch the First steps console by checking the **Launch the First Steps console** check box before clicking **Finish**.

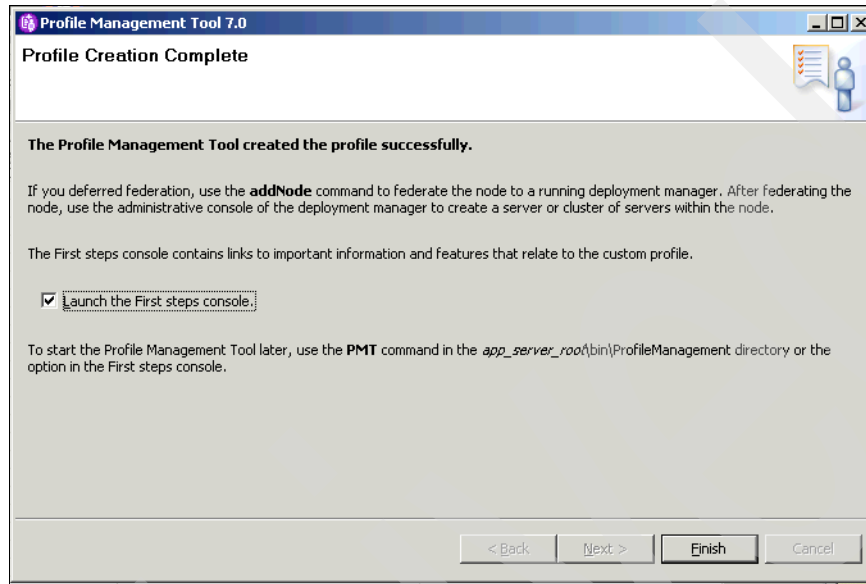


Figure 2-59 Profile Creation Complete

- From the Profile Management Tool, verify that both the Deployment Manager profile and the custom profile are listed under the profiles (Figure 2-60).

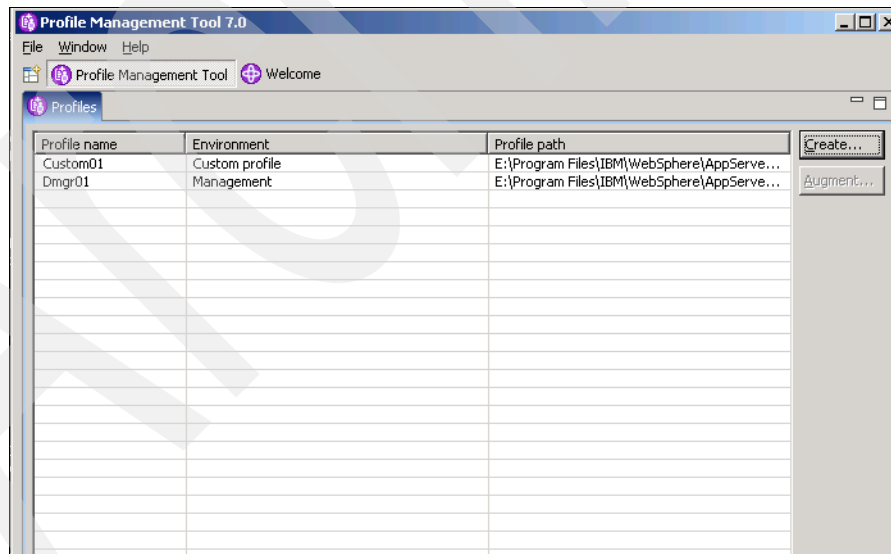


Figure 2-60 Profile Management Tool 7.0 - Profiles tab

- At this time, start the node agent for the custom profile (Custom01) using the startnode utility from the bin directory of the newly created profile (for example, E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\bin).

Note: Similarly, create custom profiles for all the nodes to be added to the WebSphere Application Server cluster.

Creating WebSphere cluster

To create a WebSphere cluster follow the steps below:

1. Open the WebSphere Integrated Solutions Console.
2. Select **Start** → **All Programs** → **IBM WebSphere** → **Application Server<version>** → **Profiles** → **<profileName>** → **Administrative Console**.

Note: If global security has been enabled, enter your login credentials on the IBM Integrated Solutions Console and click **Log In**.

3. Select **Servers** → **Clusters** → **WebSphere Application clusters** (Figure 2-61). Click **New**.

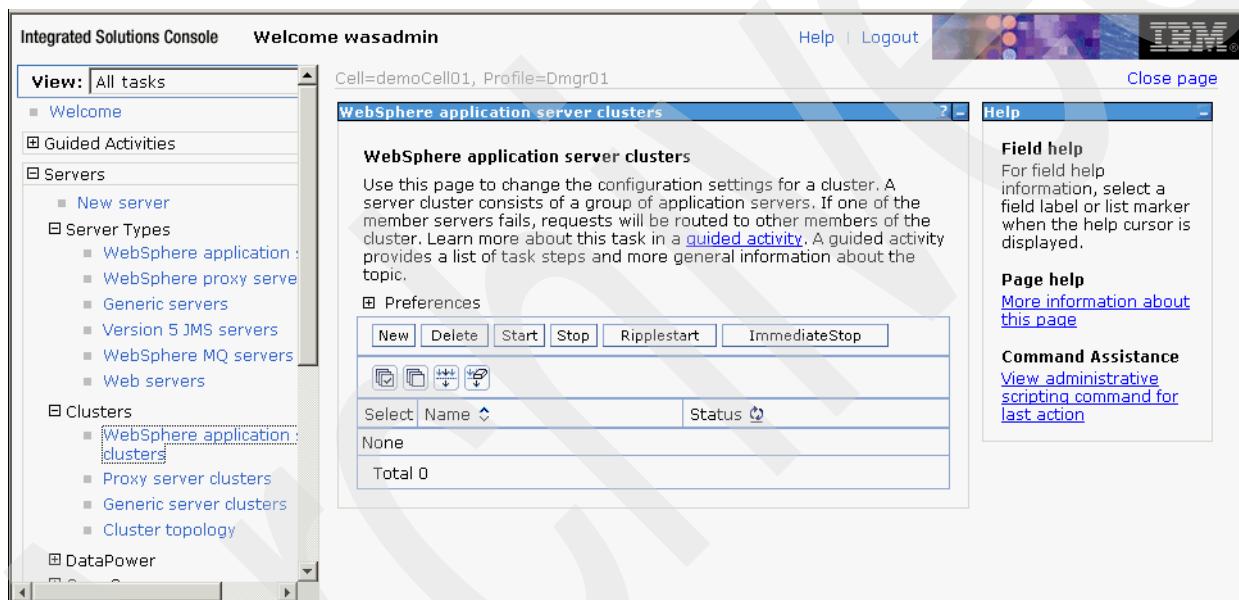


Figure 2-61 WebSphere Application Server clusters

4. Enter a name for the cluster (for example, cluster1). Select the **Prefer local** check box. Also select the **Configure HTTP session memory-memory replication** check box (Figure 2-62). Click **Next**.

The screenshot shows the 'Integrated Solutions Console' with a left-hand navigation tree. The main content area displays the 'Create a new cluster' wizard. The 'Enter basic cluster information' step is highlighted, showing a text field for 'Cluster name' with the value 'cluster1'. Below this, two checkboxes are checked: 'Prefer local. Specifies whether enterprise bean requests will be routed to the node on which the client resides when possible.' and 'Configure HTTP session memory-memory replication'. The 'Next' button is visible at the bottom of the wizard.

Figure 2-62 Create a new cluster

5. Enter a unique name for the server to be added as the first cluster member (for example, server1). Select the corresponding node accordingly from the drop-down list. Ensure that Generate unique HTTP ports is set and click **Next** (Figure 2-63).

The screenshot shows the 'Integrated Solutions Console' with the 'Create first cluster member' wizard. The 'Create first cluster member' step is highlighted, showing a text field for 'Member name' with the value 'server1'. Below this, a 'Select node' dropdown menu is set to 'demoNode01(ND 7.0.0.7)'. A 'Weight' field is set to '2' with a range of '(0..20)'. The 'Generate unique HTTP ports' checkbox is checked. Under the 'Select basis for first cluster member:' section, the first option 'Create the member using an application server template.' is selected, with 'default' chosen from the dropdown. The 'Next' button is visible at the bottom of the wizard.

Figure 2-63 Create first cluster member

Click **Next** to continue.

6. From the Create a new Cluster page (Figure 2-64), review the cluster details and click **Finish**.

Integrated Solutions Console Welcome wasadmin Help | Logout IBM

Cell=demoCell01, Profile=Dmgr01 Close page

Create a new cluster

Create a new cluster

Step 1: Enter basic cluster information
Step 2: Create first cluster member
Step 3: Create additional cluster members
→ **Step 4: Summary**

Summary

Summary of actions:

Options	Values
Cluster Name	cluster1
Core Group	DefaultCoreGroup
Node group	DefaultNodeGroup
Prefer local	true
Configure HTTP session memory-to-memory replication	true
Server name	server1
Node	demoNode01(ND 7.0.0.7)
Weight	2
Clone Template	default
Clone Basis	Create the member using an application server template.
Generate unique HTTP ports	true

Previous Finish Cancel

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](#)

Figure 2-64 Create a new cluster - Summary

7. In the message box that appears at the top of the page, click **Save** to save changes to the master configuration.
8. Add additional members (application servers) to the cluster by repeating these steps.

Note: The application server names need to be unique. Even if the node names are different, you cannot use the same name for the application server (for example, if you specified server1 in the earlier configuration, you cannot specify another member with the same name. Instead, create the additional server as server2, and so on).

- Verify that the new cluster displays in the integrated solutions console (Figure 2-65).

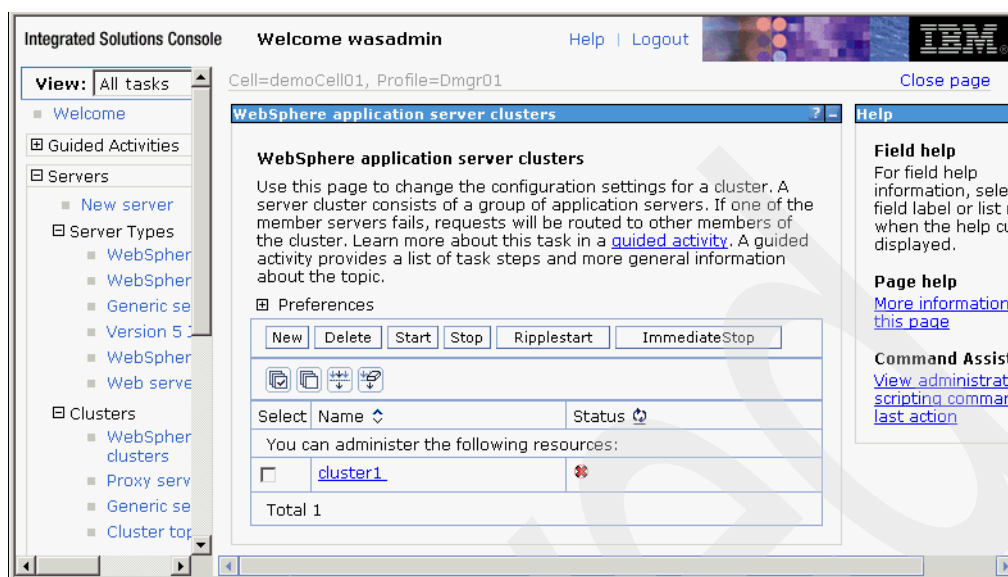


Figure 2-65 WebSphere Application Server clusters

2.3 IBM HTTP Server

This section details the installation steps for the IBM HTTP Server:

- Run `launchpad.exe` from the installation media. Select **IBM HTTP Server Installation** and click the **Launch the installation wizard for IBM HTTP Server** link to install the IBM HTTP Server using the installation wizard (Figure 2-66).

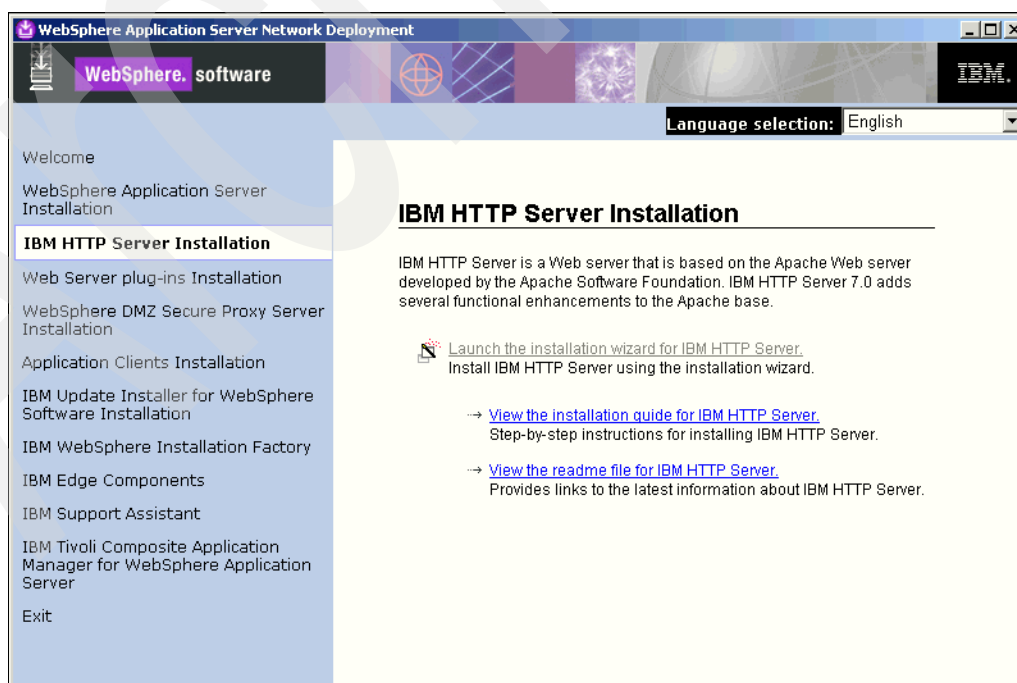


Figure 2-66 IBM HTTP Server Installation

Click **Next** to continue (Figure 2-67).

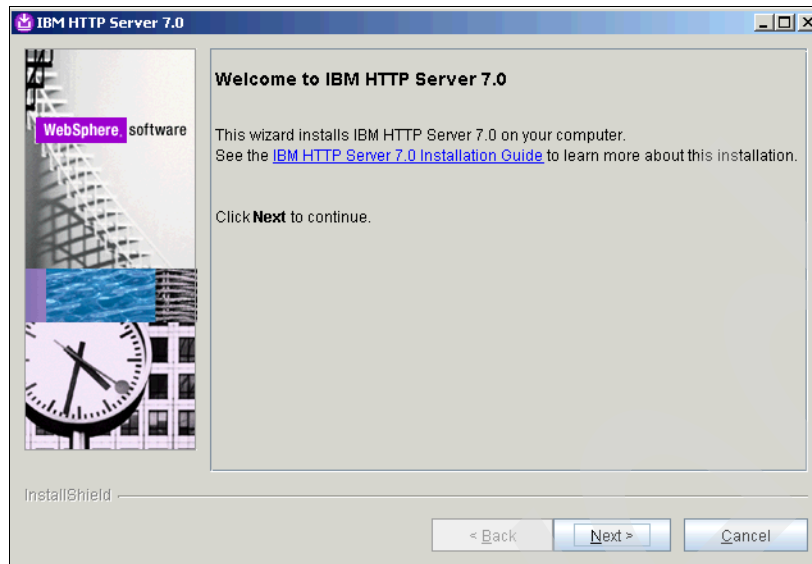


Figure 2-67 Welcome to IBM HTTP Server 7.0

2. Read and accept the IBM and non-IBM terms and click **Next** to continue with the installation (Figure 2-68).

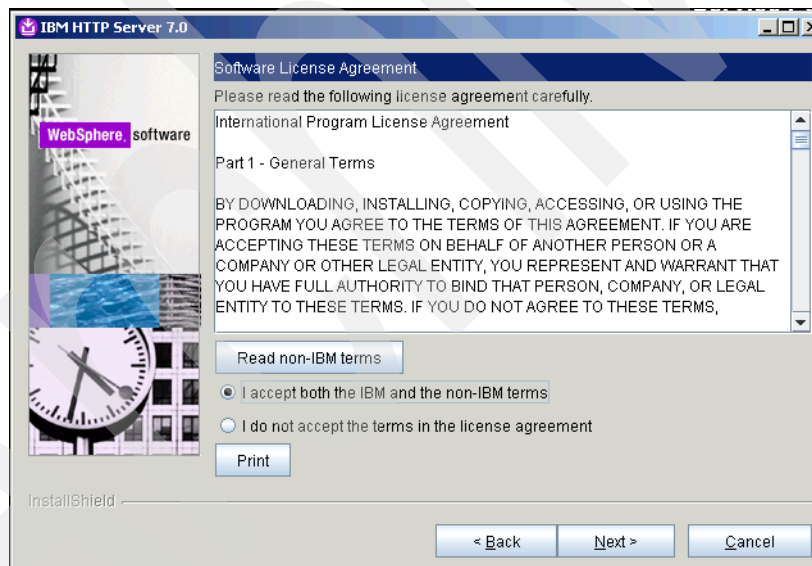


Figure 2-68 Software License Agreement

3. Click **Next** when you see the Passed message on the System Prerequisites Check page (Figure 2-69).

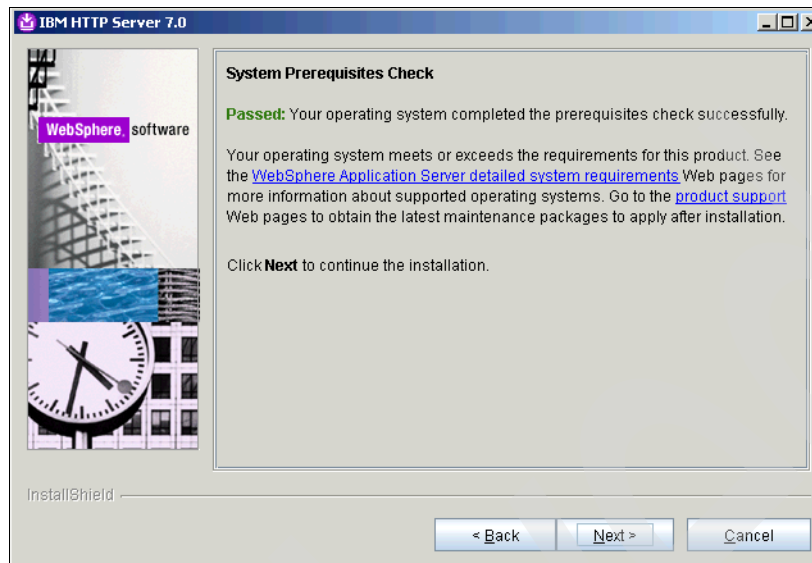


Figure 2-69 System Prerequisites Check

4. Select the default installation directory or change it as necessary (Figure 2-70). Click **Next**.

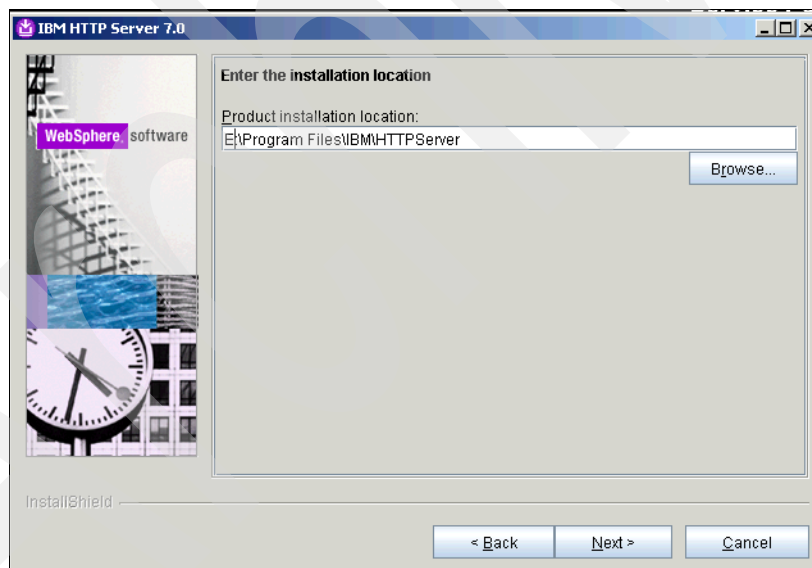


Figure 2-70 Enter the installation location

5. Configure the port numbers for IBM HTTP Server communications (Figure 2-71). Use the default port numbers and ensure that no other applications (like IIS) are using the same port number on the HIS server. When finished, click **Next**.

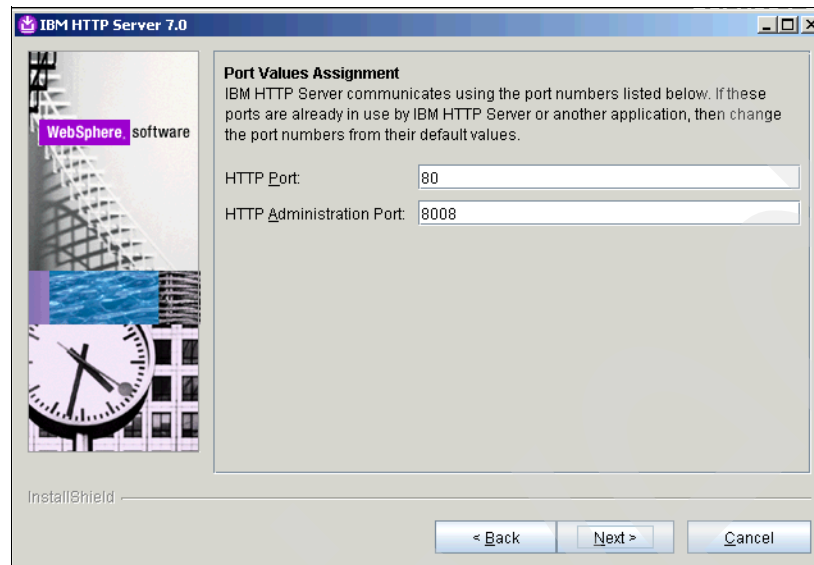


Figure 2-71 Port Values Assignment

6. Define how Windows will start IHS and the IHS Administrative processes. To run the HTTP Server and HTTP Administration Server as Windows Services, click the appropriate check boxes. Specify a local system account and password and select **Automatic** as the startup type (Figure 2-72). Click **Next**.

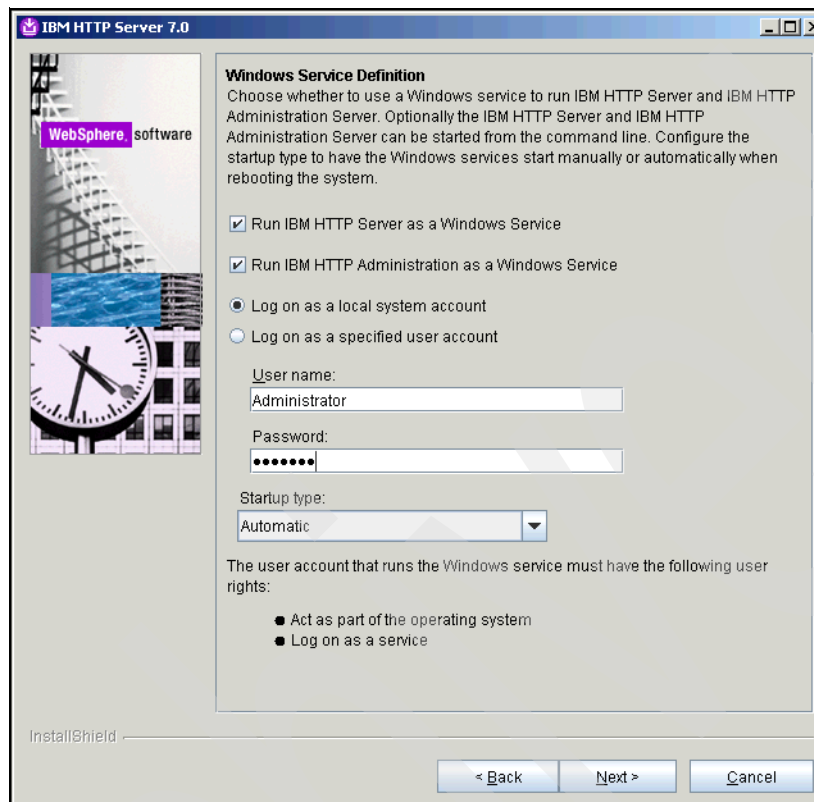
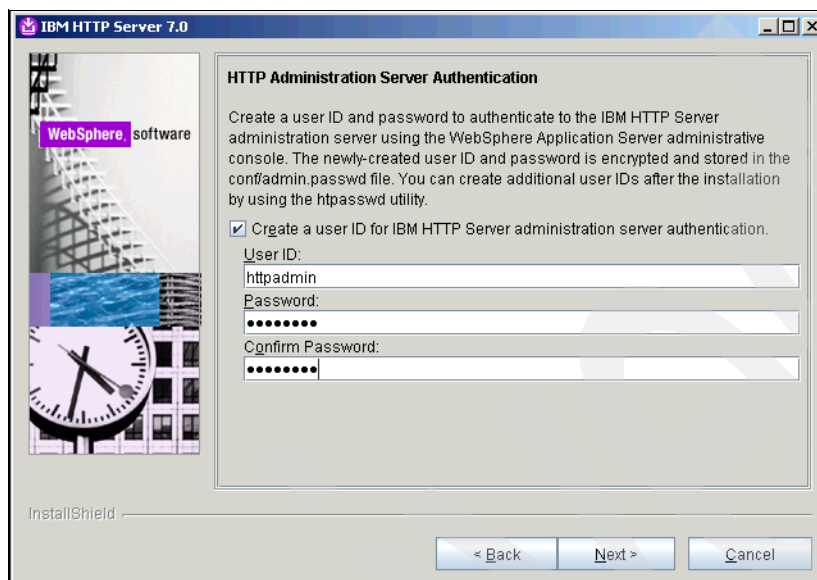


Figure 2-72 Windows Service Definition

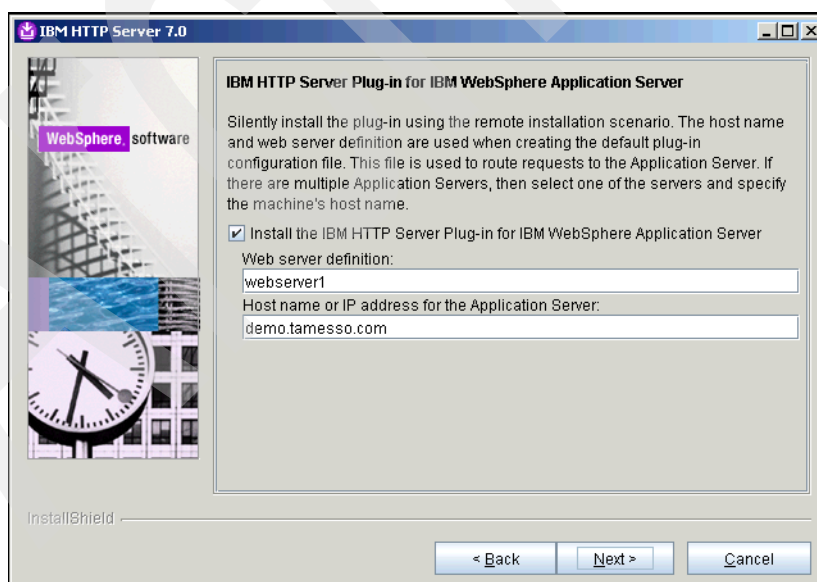
7. Specify an account that can be used to administer IHS from within WebSphere (Figure 2-73). This account can be created by the install process. The account is a WebSphere Application Server account and not an operating system account. It is used to authenticate to IHS for management purposes from WebSphere Application Server (for example, httpadmin). When finished, click **Next**.



The screenshot shows the 'IBM HTTP Server 7.0' window with the 'HTTP Administration Server Authentication' tab selected. The window has a title bar with the IBM logo and 'IBM HTTP Server 7.0'. On the left, there is a graphic with 'WebSphere software' text. The main area contains instructions: '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 httpasswd utility.' Below this, there is a checkbox labeled 'Create a user ID for IBM HTTP Server administration server authentication.' which is checked. Underneath the checkbox are three input fields: 'User ID:' with the value 'httpadmin', 'Password:' with masked characters '.....', and 'Confirm Password:' with masked characters '.....'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Figure 2-73 HTTP Administration Server Authentication

8. Check the **Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server** check box (Figure 2-74). Also, specify the web server definition (default is webserver1) and enter the host name of the WebSphere Application Server (for example, demo.tamesso.com). When finished, click **Next**.



The screenshot shows the 'IBM HTTP Server 7.0' window with the 'IBM HTTP Server Plug-in for IBM WebSphere Application Server' tab selected. The window has a title bar with the IBM logo and 'IBM HTTP Server 7.0'. On the left, there is a graphic with 'WebSphere software' text. The main area contains instructions: '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.' Below this, there is a checkbox labeled 'Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server' which is checked. Underneath the checkbox are two input fields: 'Web server definition:' with the value 'webserver1' and 'Host name or IP address for the Application Server:' with the value 'demo.tamesso.com'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'. The 'InstallShield' logo is visible in the bottom left corner.

Figure 2-74 IBM HTTP Server Plug-in for IBM WebSphere Application Server

9. Review the Installation summary page (Figure 2-75) and click **Next**.

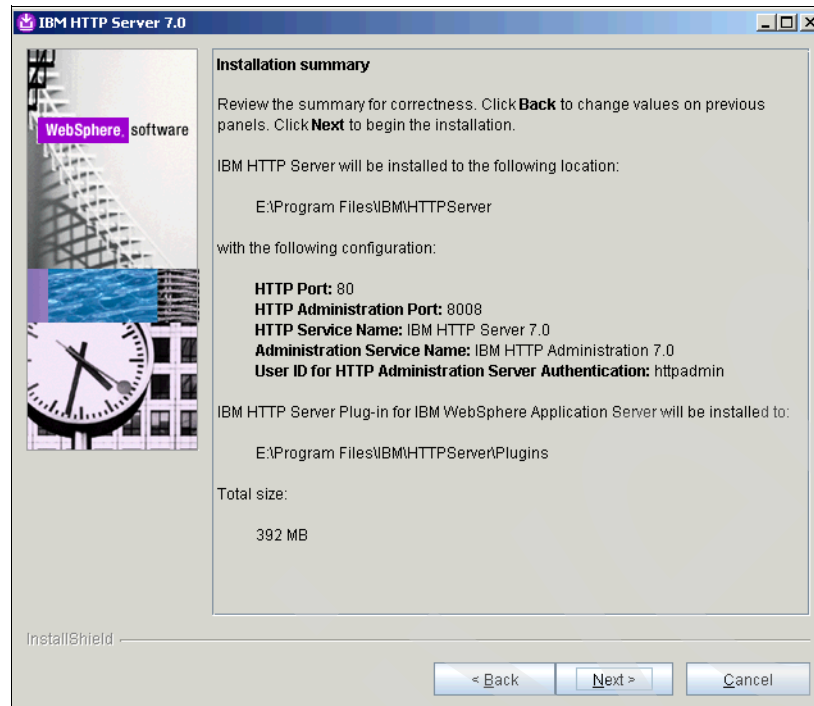


Figure 2-75 Installation summary

10. When the installation completes and the successful message is displayed (Figure 2-76), click **Finish**.

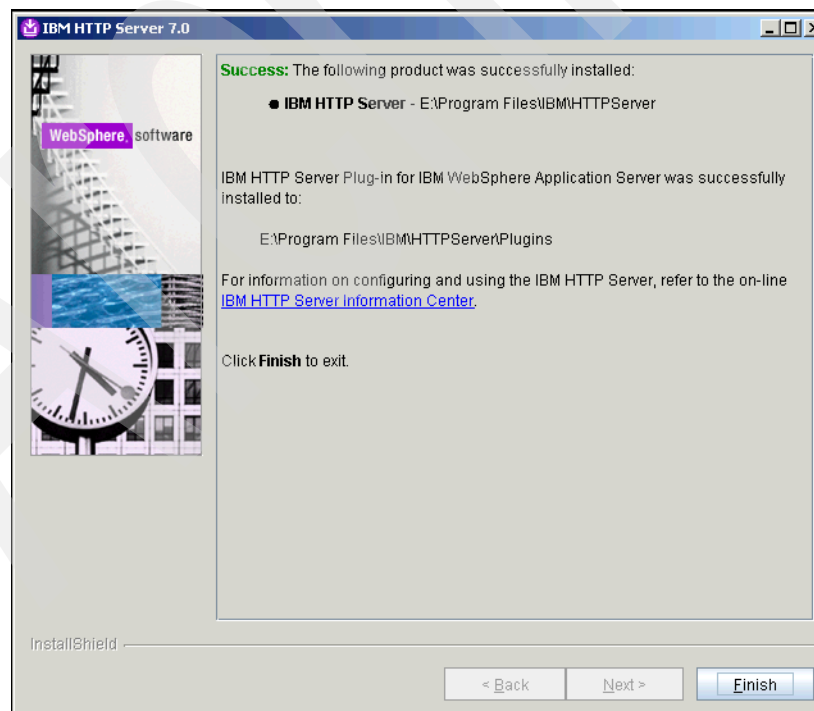


Figure 2-76 Success

This completes the IHS installation.

2.3.1 IBM HTTP Server fix pack

This section details the steps for installing fix pack 7 for the IBM HTTP Server:

1. If you have not already copied the IHS fix pack to the Update Installer maintenance directory, copy it to the WebSphere Application Server Update Installer maintenance directory (for example, E:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance).
2. Run update.bat (from the E:\Program Files\IBM\WebSphere\UpdateInstaller directory) to start the IBM Update Installer for WebSphere Software wizard (Figure 2-77). Click **Next** to proceed with the upgrade process.

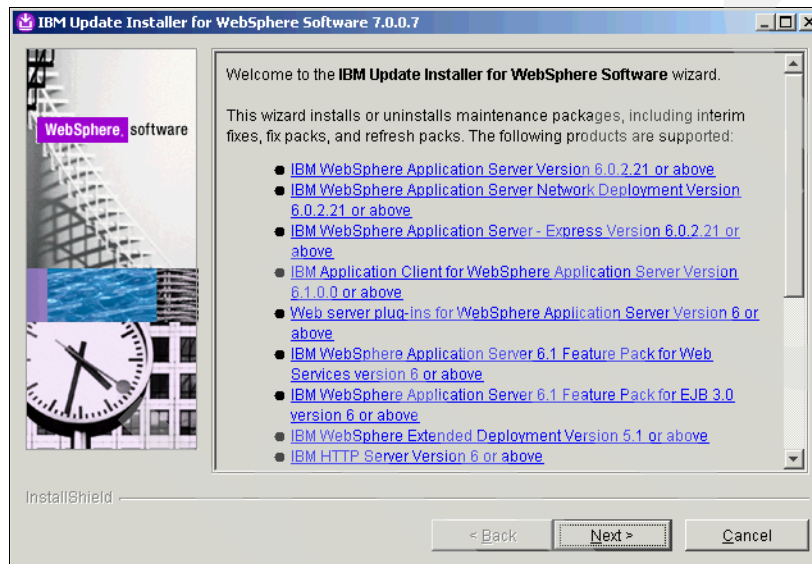


Figure 2-77 Welcome to the IBM Update Installer for WebSphere Software wizard

3. From the Product Selection page (Figure 2-78), accept the default directory or enter or select another directory and click **Next**.

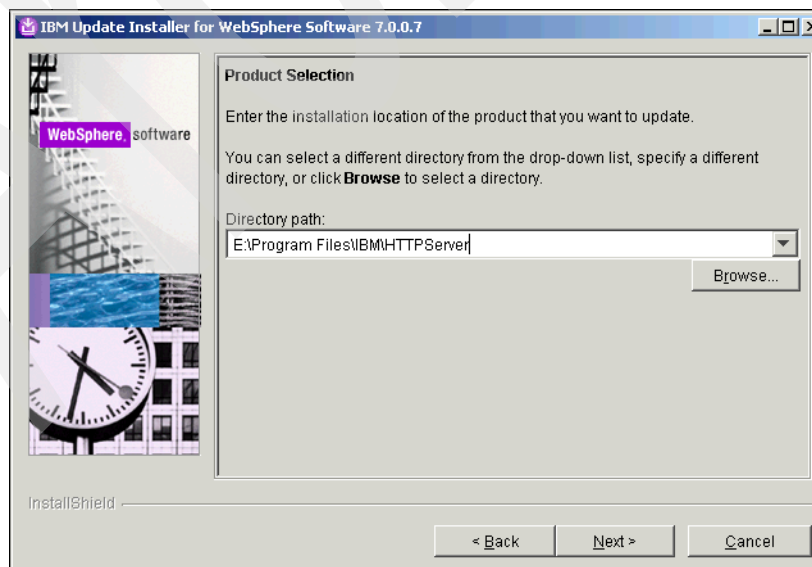


Figure 2-78 Product Selection

4. Select **Install maintenance package** from the Maintenance Operation Selection page (Figure 2-79) and click **Next** to continue.

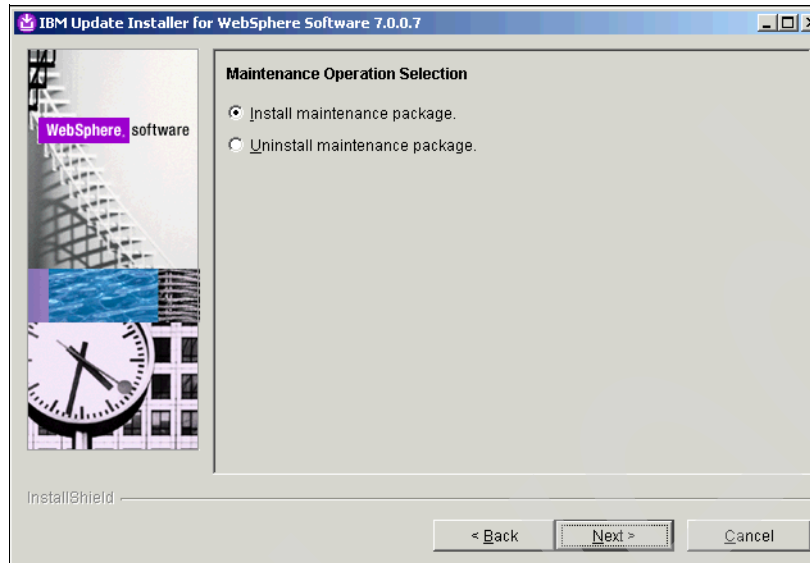


Figure 2-79 Maintenance Operation Selection

5. On the Maintenance Package Directory Selection page (Figure 2-80), browse to the WebSphere Update Installer maintenance directory and click **Next**.

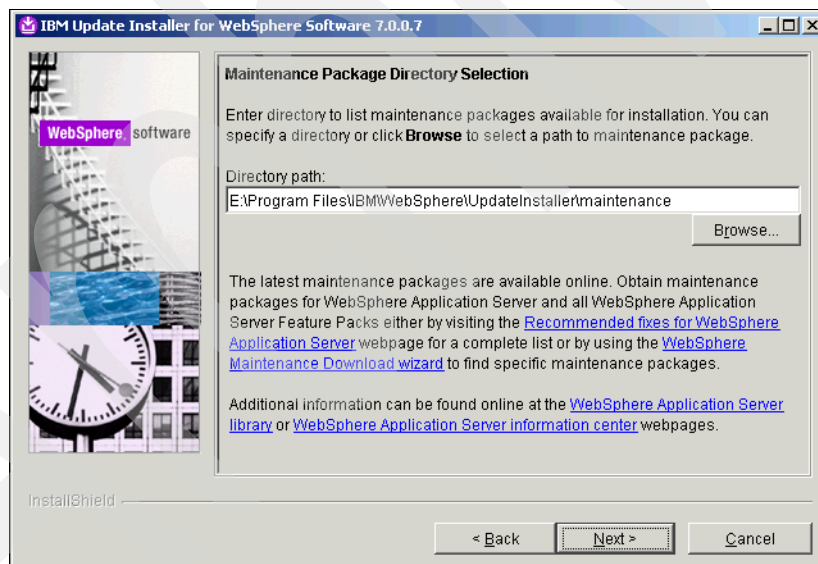


Figure 2-80 Maintenance Package Directory Selection

6. Select the IHS fix pack (7.0.0-WS-IHS-WinX32-FP0000007.pak) and click **Next** (Figure 2-81).

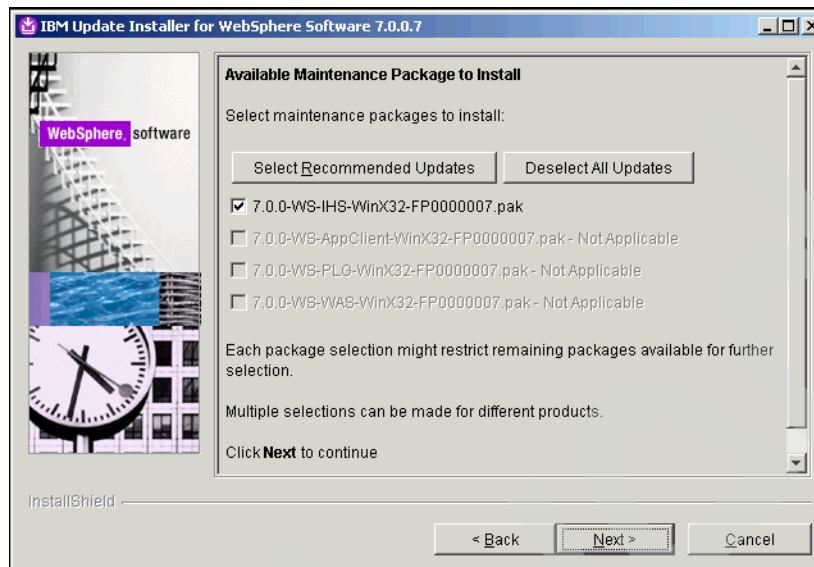


Figure 2-81 Available Maintenance Package to Install

7. Review the installation summary (Figure 2-82) and click **Next**.

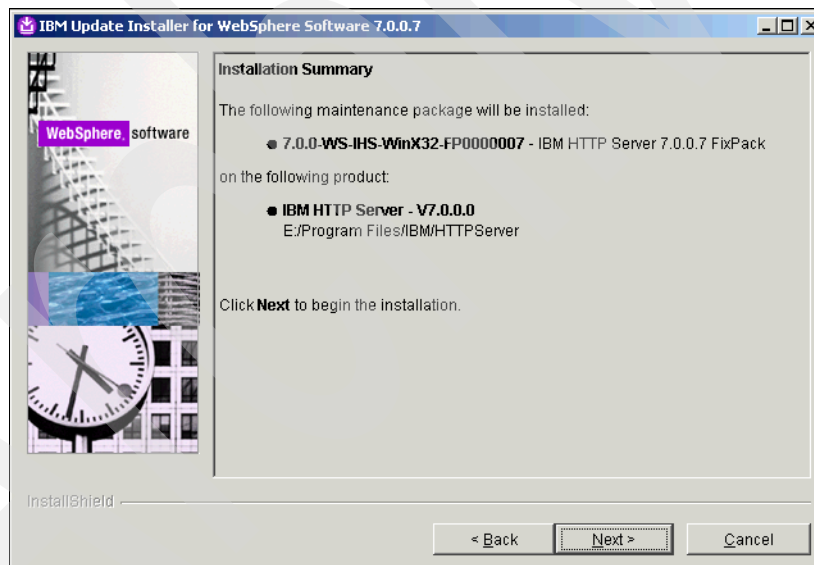


Figure 2-82 Installation Summary

8. Click **Finish** when you see the success message on the Installation Complete page (Figure 2-83).

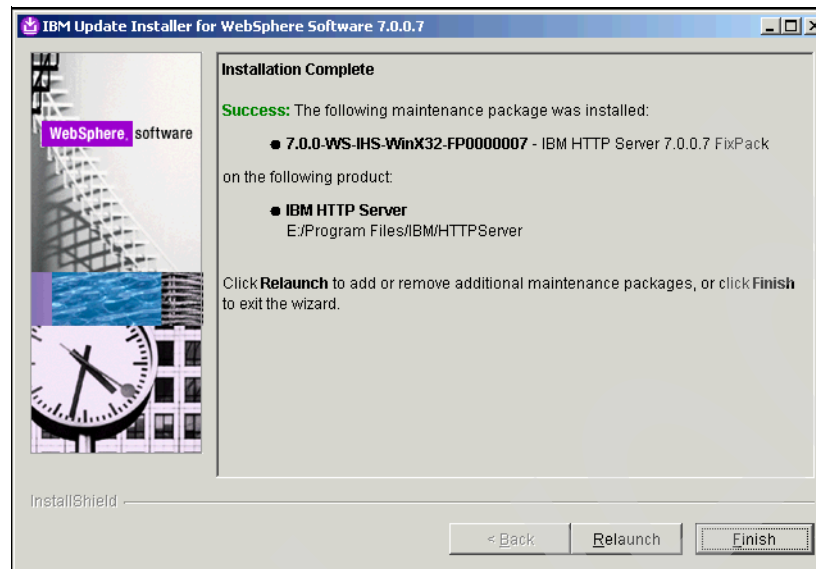


Figure 2-83 Installation Complete

This completes the IHS fix pack installation.

2.3.2 IBM HTTP Server plug-in pack

This section details the steps for installing fix pack 7 for the IBM HTTP Server plug-in.

1. Copy the IHS plug-in fix pack to the WebSphere Application Server Update Installer maintenance directory (for example, E:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance).

2. Run `update.bat` (from the `E:\Program Files\IBM\WebSphere\UpdateInstaller` directory) to start the IBM Update Installer for WebSphere Software wizard (Figure 2-84). Click **Next** to proceed with the upgrade process.

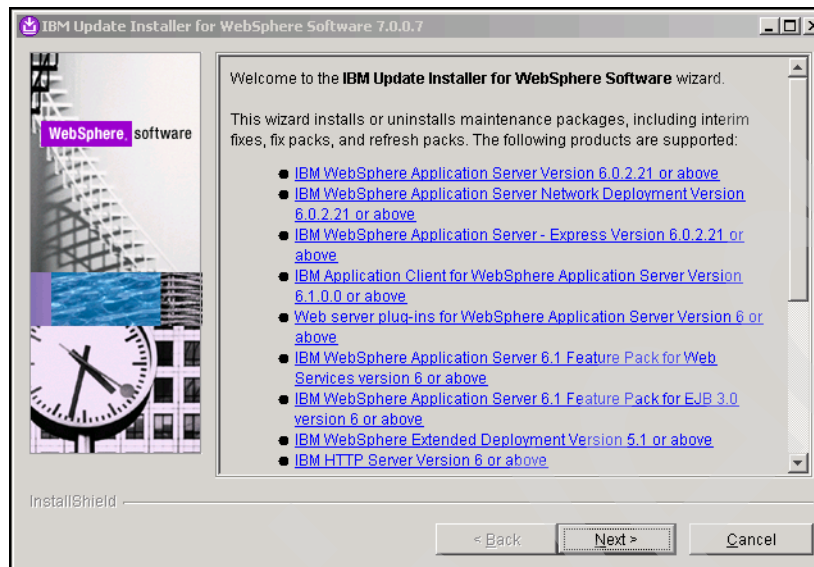


Figure 2-84 Welcome to the IBM Update Installer for WebSphere Software wizard

3. From the Product Selection page (Figure 2-85), browse to the installation directory of the HTTP Server plug-in and click **Next**.

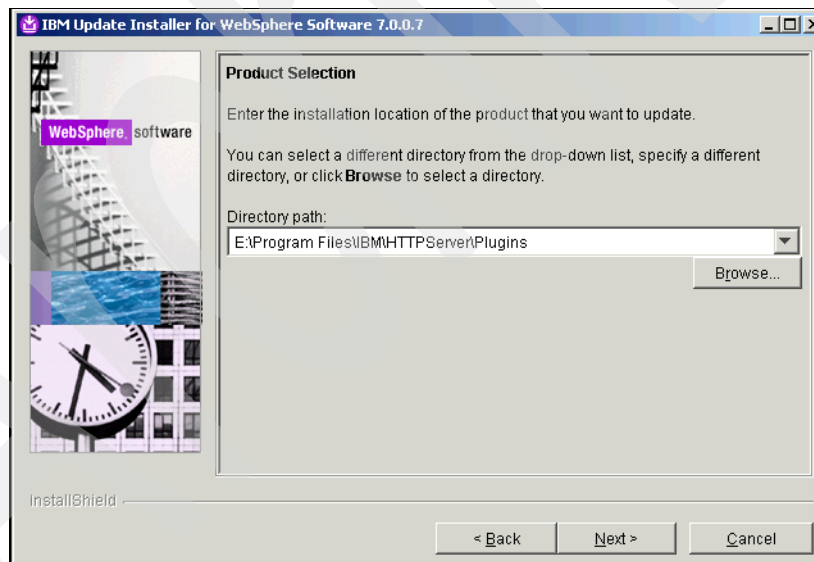


Figure 2-85 Product Selection

4. Select **Install maintenance package** on the Maintenance Operation Selection page (Figure 85) and click **Next**.

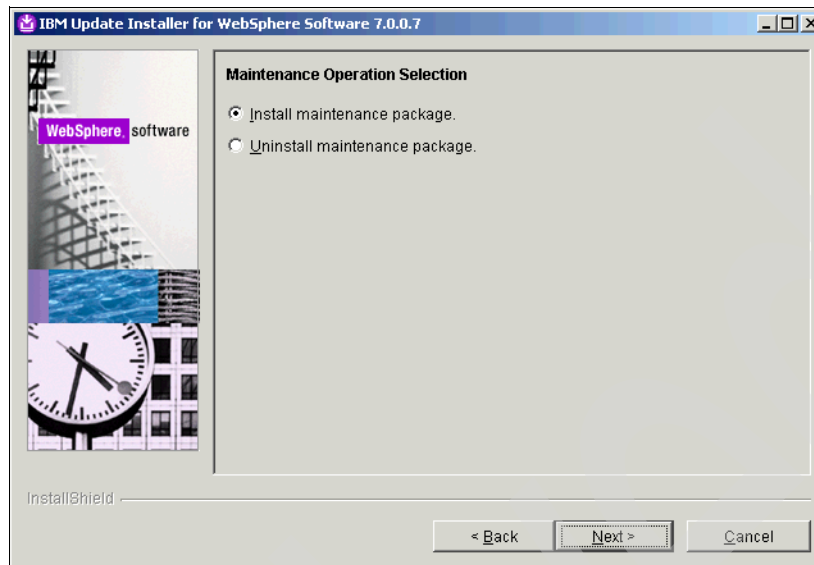


Figure 2-86 Maintenance Operation Selection

5. Select the WebSphere Update Installer maintenance directory (Figure 2-87) and click **Next**.

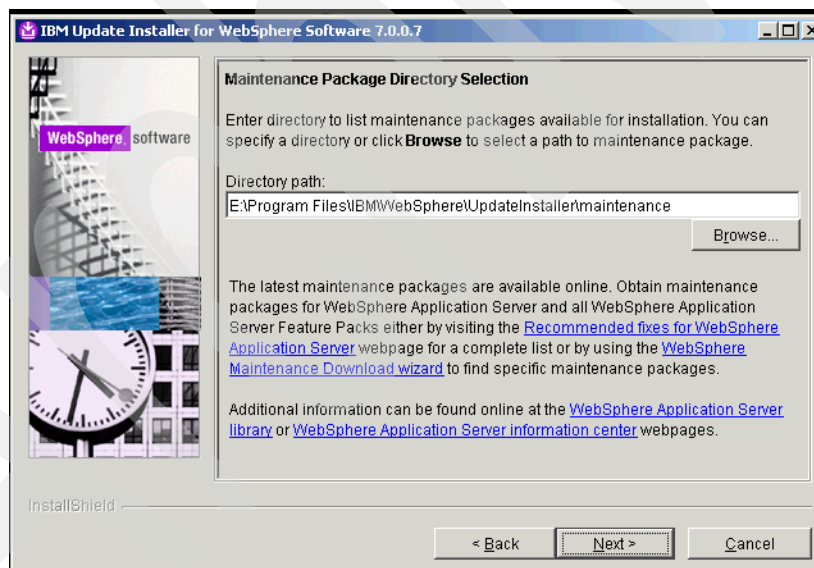


Figure 2-87 Maintenance Package Directory Selection

6. From the Available Maintenance Package to Install page (Figure 2-88), select **WS-PLG-WinX32-FP0000007.pak** and click **Next**.

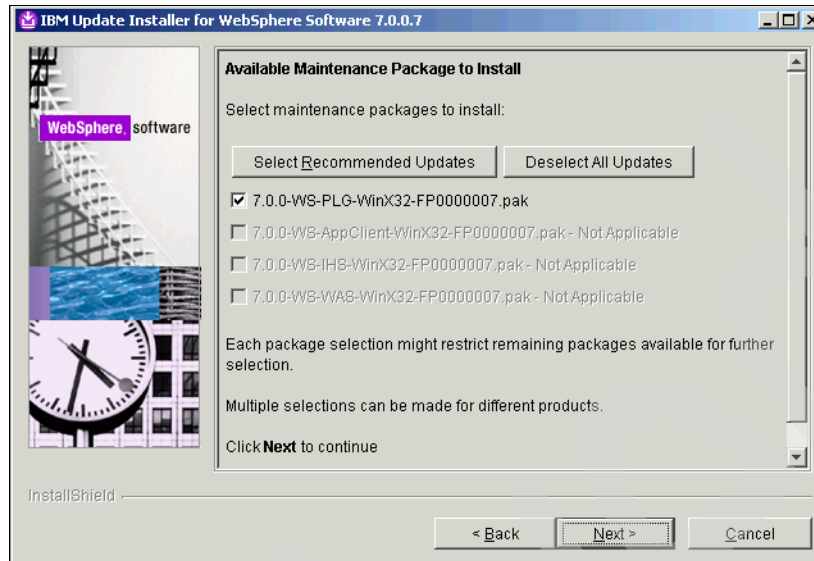


Figure 2-88 Available Maintenance Package to Install

7. Review the Installation summary (Figure 2-89) and click **Next**.

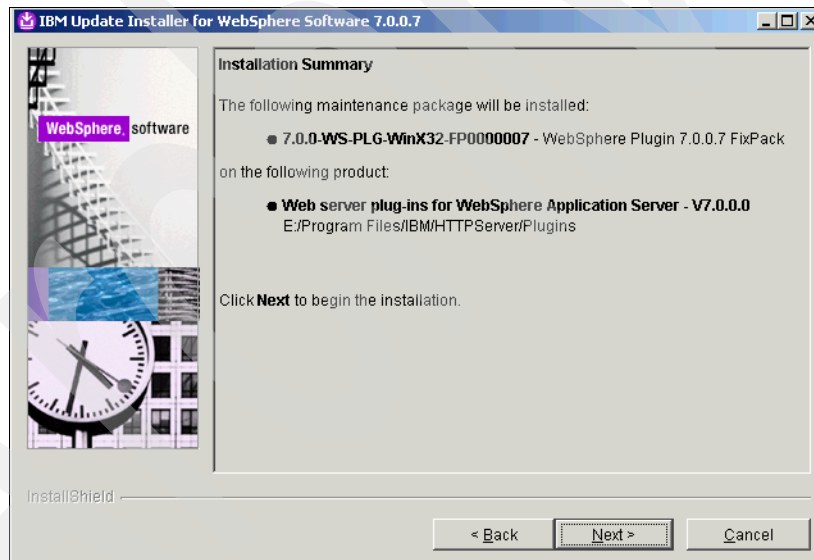


Figure 2-89 Installation Summary

- Click **Finish** when you see the success message on the Installation Complete page (Figure 2-90).

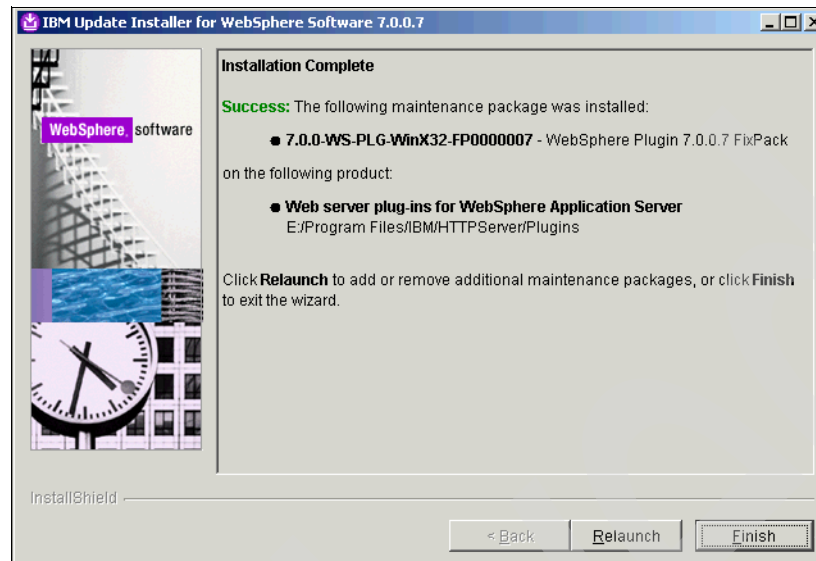


Figure 2-90 Installation Complete

This completes the installation of the IHS plug-in fix pack.

Adding HTTP Server to the WebSphere Deployment Manager

This section documents how to add the HTTP Server to the WebSphere Deployment Manager.

- From the WebSphere Integrated Solutions console, click **Servers** → **Server Types** → **Web servers** → **New**.
- From the New Server window (Figure 2-91), select **Web server** from the drop-down menu of server types. Click **Next**.

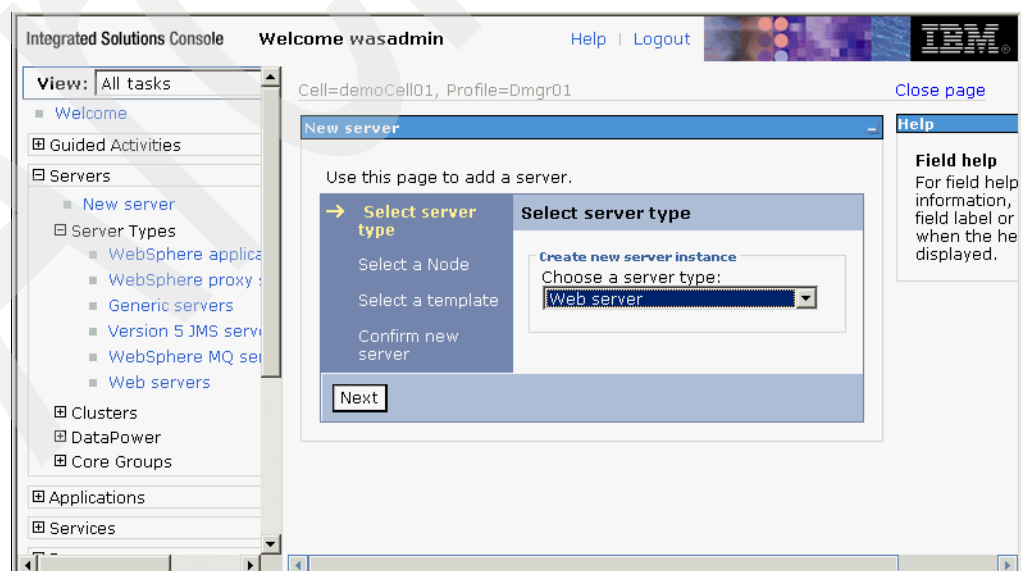


Figure 2-91 Select server type

- On the Create new Web server definition page (Figure 2-92), select the appropriate node and server name for the web server (for example, demoNode01 and webserver1) and select **IBM HTTP Server** for the type. Click **Next**.

Integrated Solutions Console - Microsoft Internet Explorer

Address: https://demo.tanesso.com:9043/ibm/console/secure/securelogin.do

Integrated Solutions Console Welcome wasadmin Help | Logout

Cell=demoCell01, Profile=Dmgr01 Close page

Create new Web server definition

Use this page to create a new Web server.

→ **Step 1: Select a node for the Web server and select the Web server type**

Select a node for the Web server and select the Web server type

Select a node that corresponds to the Web server you want to add.

Select node: demoNode01

Server name: webserver1

Type: IBM HTTP Server

Next Cancel

Figure 2-92 Select a node for the Web server and select the Web server type

- From the Select a Web server template page (Figure 2-93), verify that the IHS template is selected and click **Next**.

Integrated Solutions Console Welcome wasadmin Help | Logout

Cell=demoCell01, Profile=Dmgr01 Close page

Create new Web server definition

Use this page to create a new Web server.

→ **Step 2: Select a Web server template**

Select a Web server template

Select the template that corresponds to the server that you want to create.

Select	Template Name	Type	Description
<input checked="" type="radio"/>	IHS	System	The IHS Web Server Template

Previous Next Cancel

Figure 2-93 Select a Web server template

5. Verify the installation location (for example, E:\Program Files\IBM\HTTPServer) and other properties on the Create new Web server definition page (Figure 2-94), and click **Next**.

Integrated Solutions Console Welcome wasadmin Help | Logout IBM

Cell=demoCell01, Profile=Dmgr01 Close page

Create new Web server definition

Use this page to create a new Web server.

Step 1: Select a node for the Web server and select the Web server type

Step 2: Select a Web server template

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

Step 4: Confirm new Web server

Enter the properties for the new Web server

Enter the Web server properties.

* Port 80

* Web server installation location E:\Program Files\IBM\HTTPServer

* Service name IBMHTTPServer7.0

* Plug-in installation location E:\Program Files\IBM\HTTPServer\Plugins

Application mapping to the Web server All

Previous Next Cancel

Figure 2-94 Enter the properties for the new Web server

6. On the Confirm new Web server page (Figure 2-95), verify the information for the web server and click **Finish**.

Integrated Solutions Console Welcome wasadmin Help | Logout IBM

Cell=demoCell01, Profile=Dmgr01 Close page

Create new Web server definition

Use this page to create a new Web server.

Step 1: Select a node for the Web server and select the Web server type

Step 2: Select a Web server template

Step 3: Enter the properties for the new Web server

→ Step 4: Confirm new Web server

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 "webserver1" will be created on node "demoNode01" Platform Type "Windows" Web server installation root "E:\Program Files\IBM\HTTPServer"

Previous Finish Cancel

Figure 2-95 Confirm new Web server

7. Click **Save** to save to the master configuration (Figure 2-96).

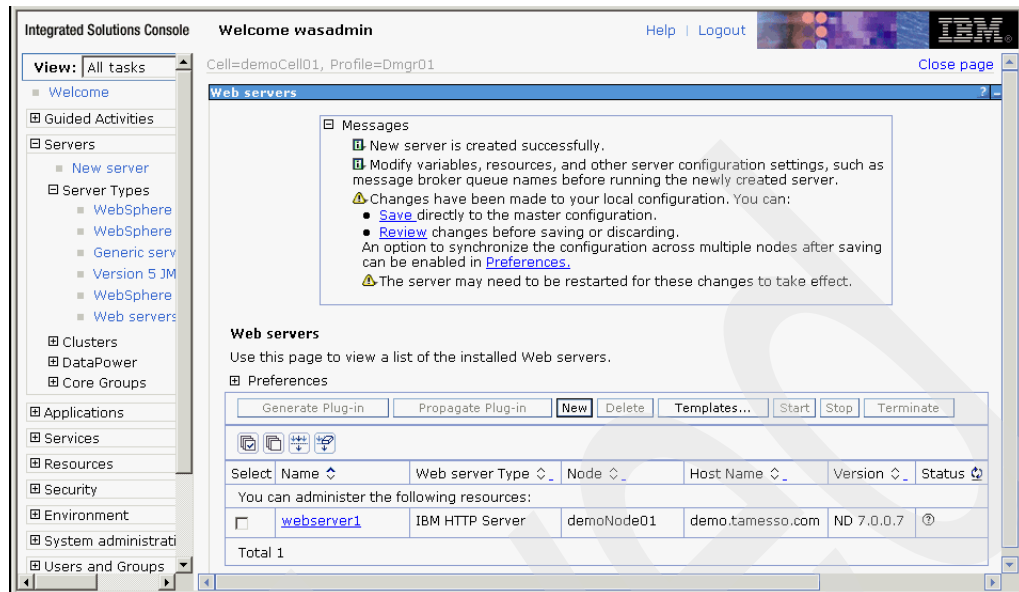


Figure 2-96 Welcome wasadmin

8. Click **OK** (Figure 2-97).

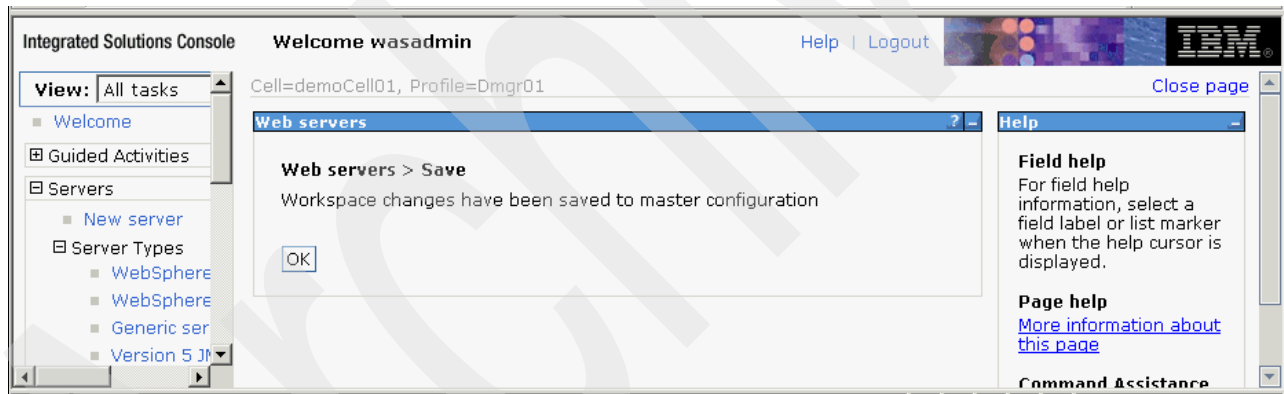


Figure 2-97 Welcome wasadmin - Save web servers

Starting the web server

Select the check box for the web server (for example, webserver1) and click **Start** (Figure 2-98).

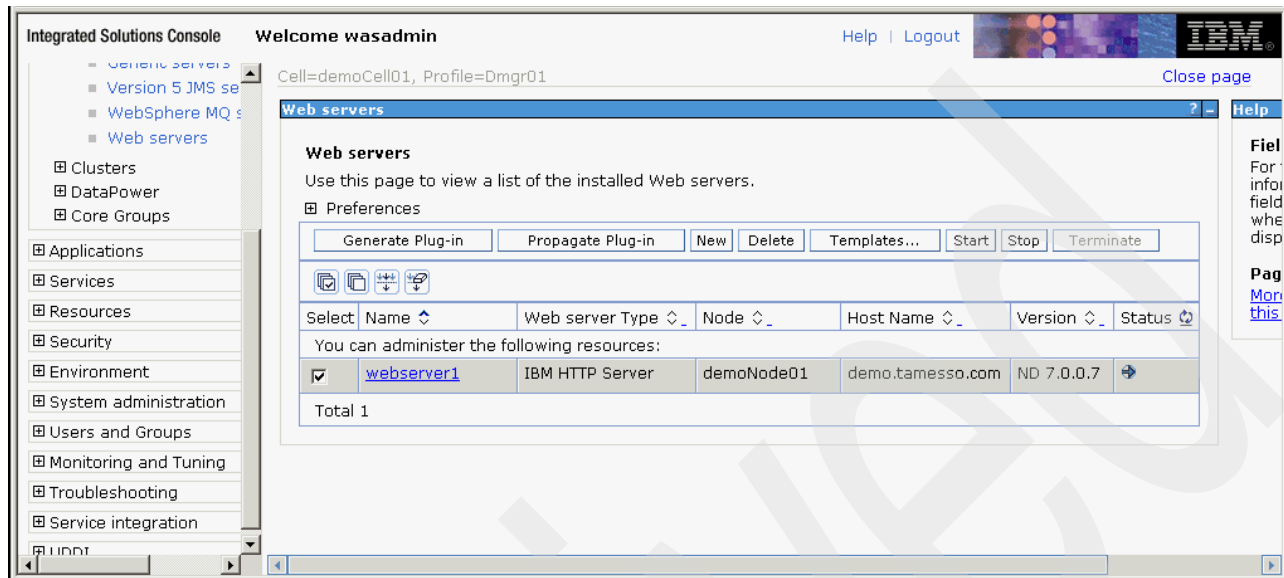


Figure 2-98 Web servers

Generating the plug-in

Select the check box for the web server (for example, webserver1) and click **Generate Plug-in** (Figure 2-99).

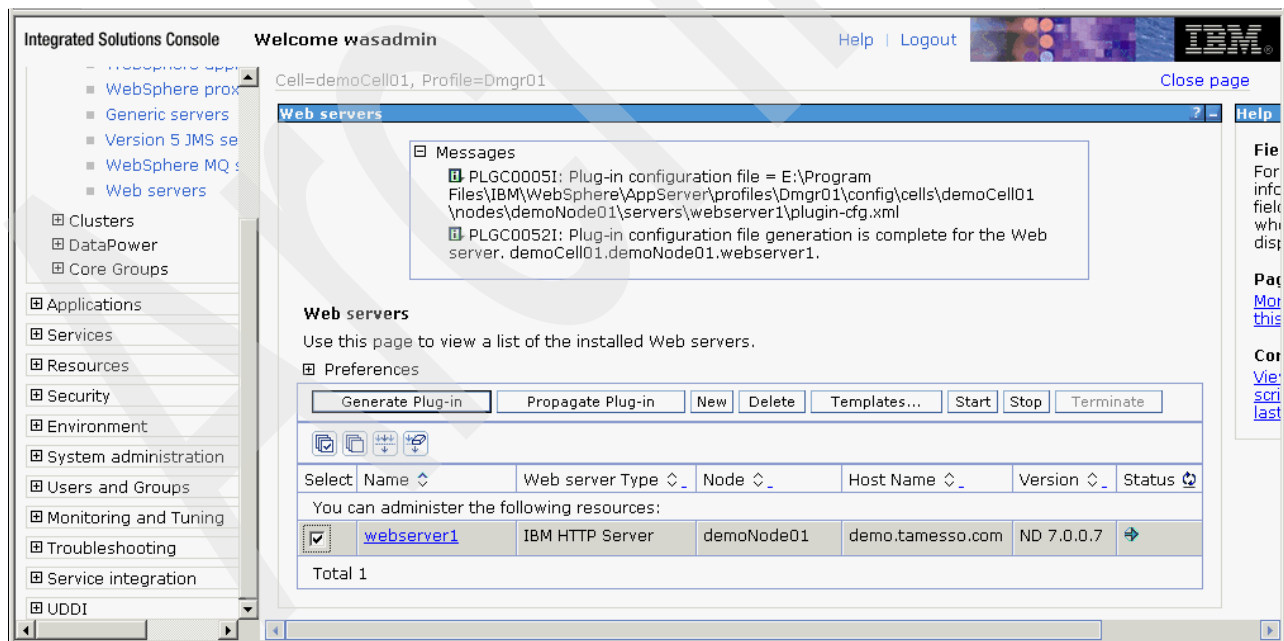


Figure 2-99 Messages

Propagating the plug-in

Select the check box for the web server (for example, webserver1) and click **Propagate Plug-in** (Figure 2-100).

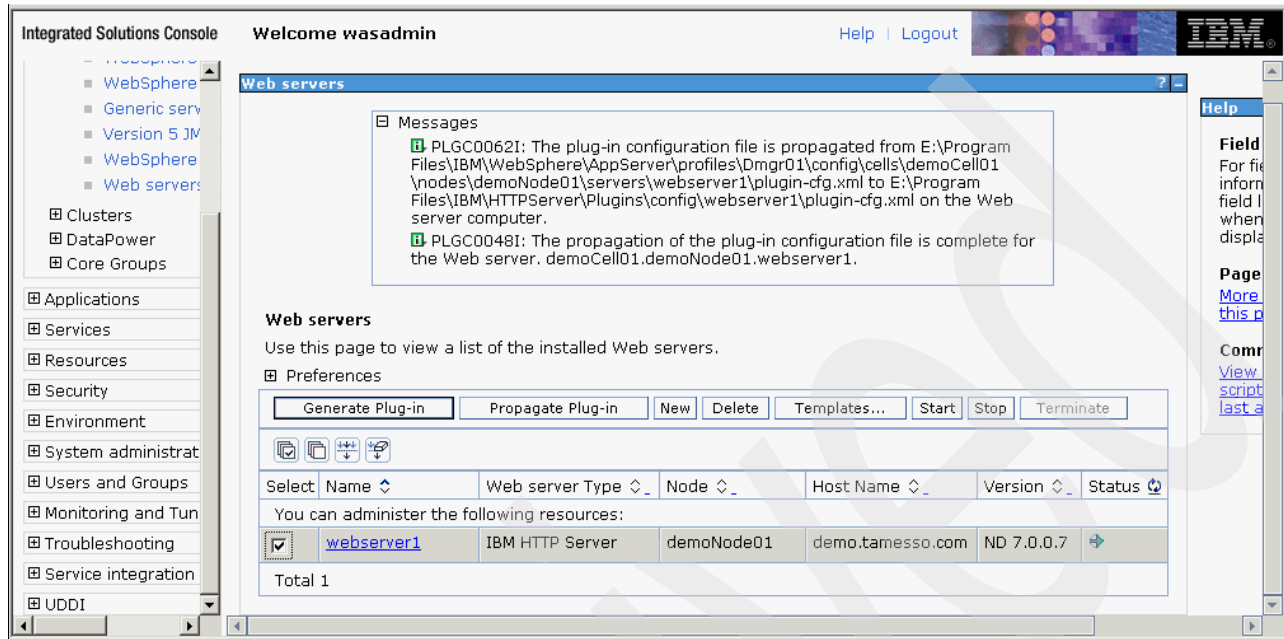


Figure 2-100 Messages

2.4 IMS Server

This section details the installation of the Tivoli Access Manager for Enterprise Single Sign-On IMS Server (referred to as IMS from now on).

1. Before proceeding further into this section, ensure that the WebSphere Application Server has been started and is running. Also ensure that global application security and administrative security have been enabled via the WebSphere Administrative Console (via the Security → Global Security settings).
2. Run `imsinstaller.exe`.

3. Figure 2-101 displays the initial startup interface when the Tivoli Access Manager for Enterprise Single Sign-On IMS Server installation begins. Select the language from the drop-down menu and click **OK**.

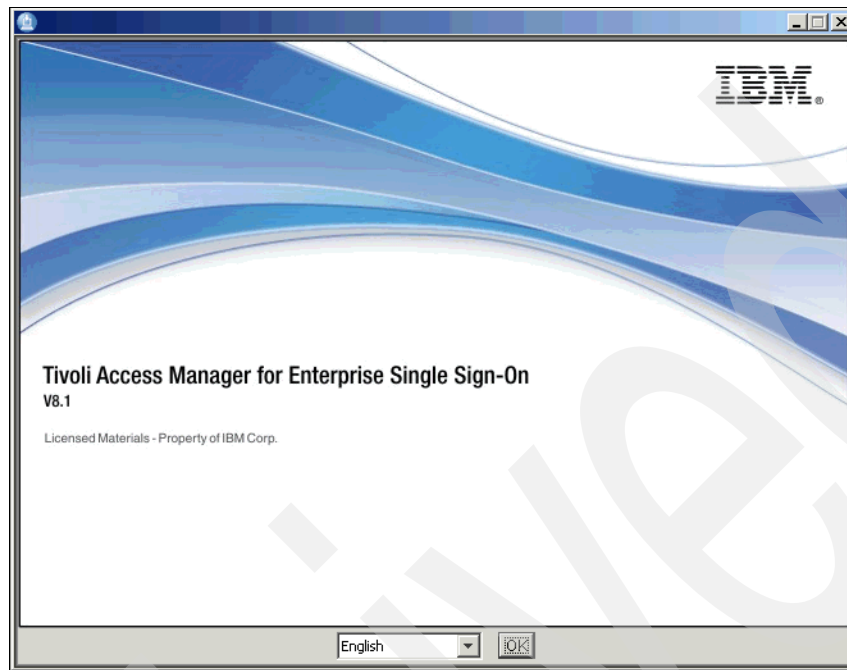


Figure 2-101 Tivoli Access Manager for Enterprise Single Sign-On V8.1

4. Read and accept the terms of the license agreement (Figure 2-102) and click **Next**.

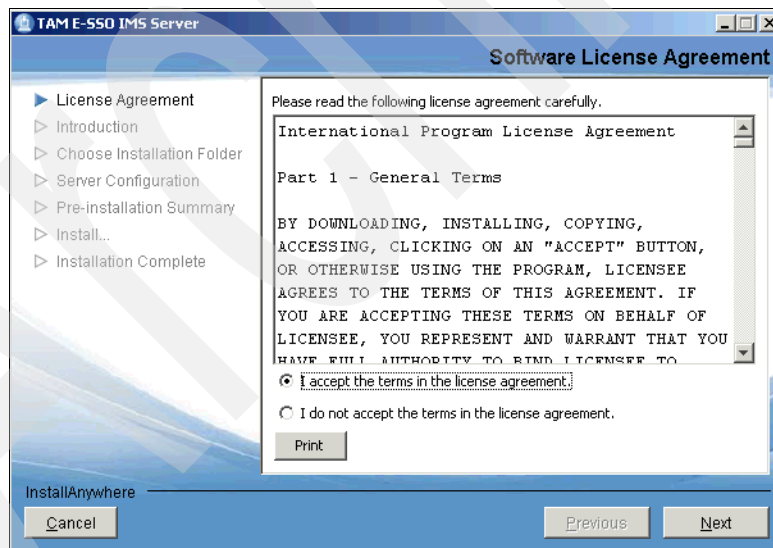


Figure 2-102 License Agreement

Click **Next** to proceed with the installation (Figure 2-103).

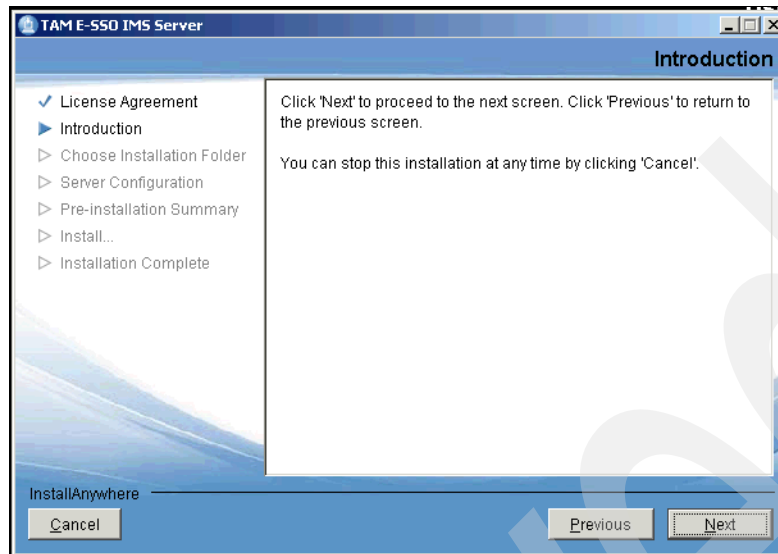


Figure 2-103 Introduction

5. Accept the default location or specify the installation directory (Figure 2-104) and click **Next**.

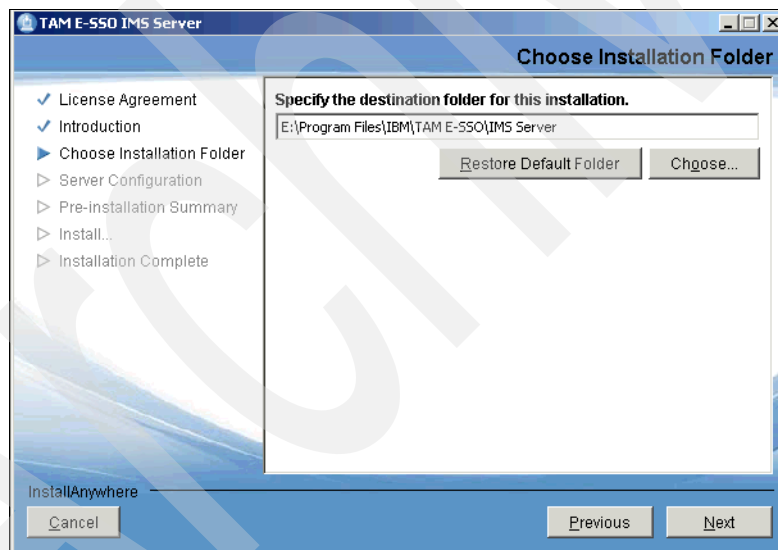


Figure 2-104 Choose Installation Folder

6. Do not use the installer to deploy the TAMESSO IMS Server to WebSphere Application Server. Select **No** and click **Next** (Figure 2-105).

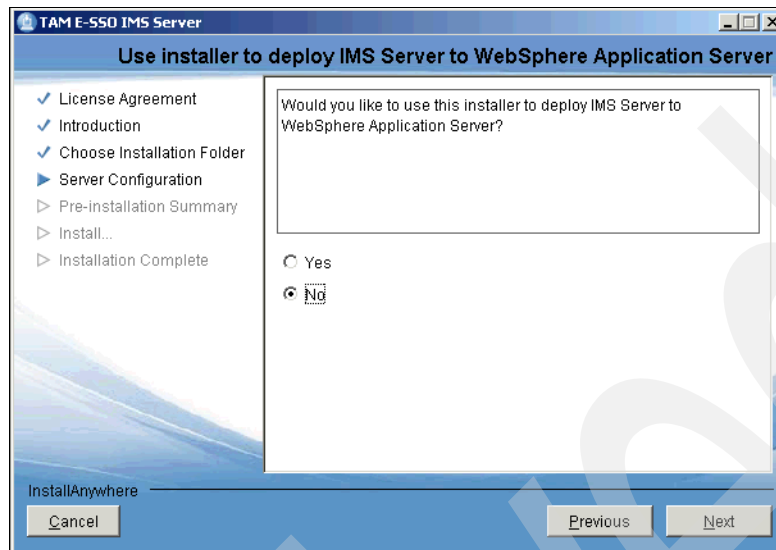


Figure 2-105 Server Configuration

7. Review the pre-installation summary information (Figure 2-106) and click **Install** to continue.

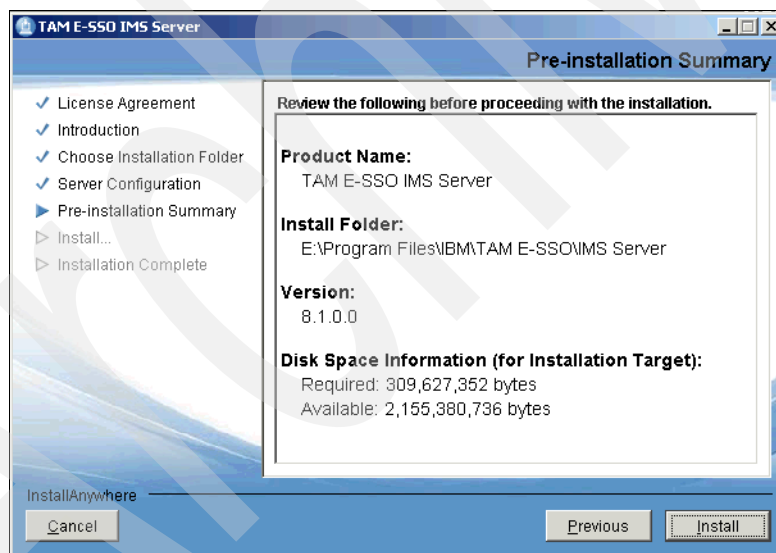


Figure 2-106 Pre-installation Summary

Wait for the installation to complete (Figure 2-107).

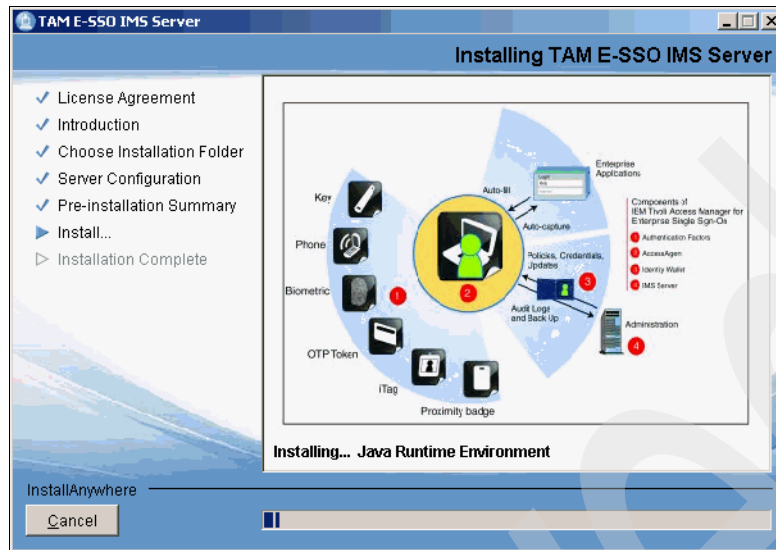


Figure 2-107 Install

8. Click **Done** when you see the successful installation message (Figure 2-108).

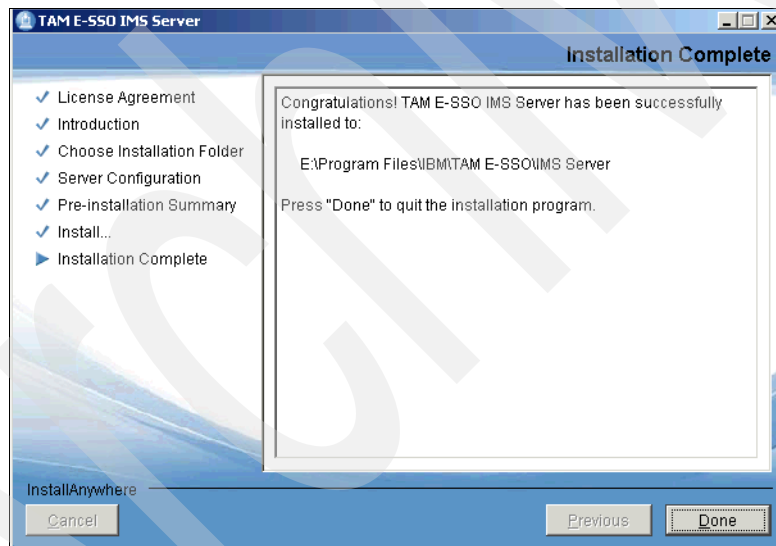


Figure 2-108 Installation Complete

This completes the IMS installation.

IMS Server fix pack

We now apply the latest Tivoli Access Manager for Enterprise Single Sign-On IMS fix pack:

1. Extract the IMS fix pack to the WebSphere Update Installer maintenance directory (for example, E:\Program Files\IBM\WebSphere\UpdateInstaller\maintenance).
2. Launch the Update Installer for WebSphere (Figure 2-109).

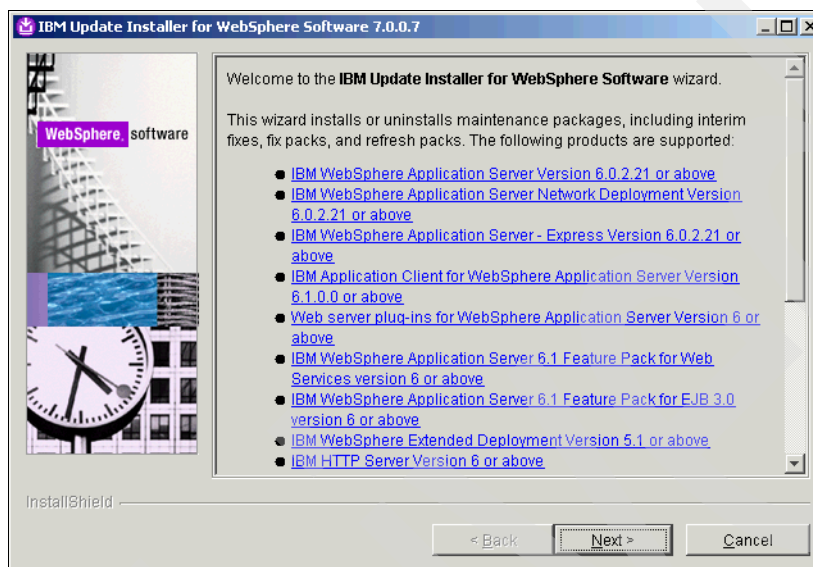


Figure 2-109 Welcome to the IBM Update Installer for WebSphere Software wizard

3. On the Product Selection page (Figure 2-110), browse to the installation directory for the IMS Server (for example, E:\Program Files\IBM\TAM E-SSO\IMS Server) and click **Next**.

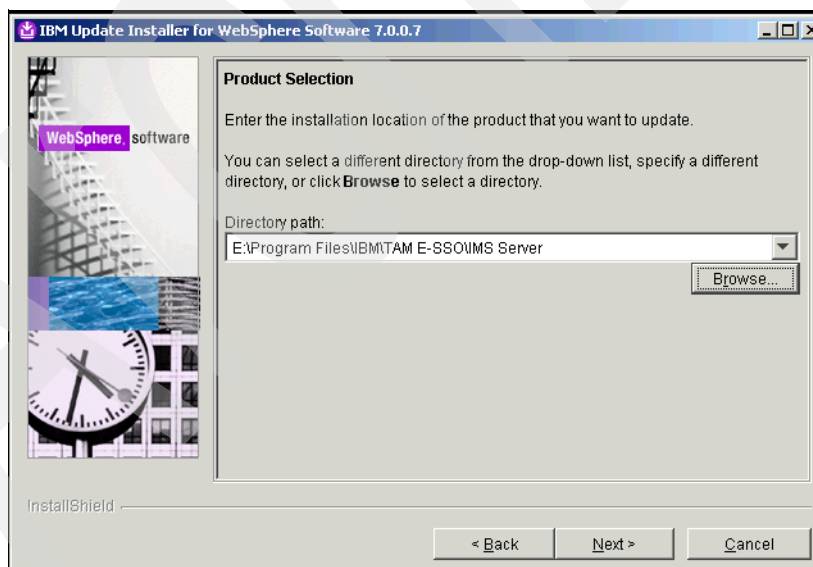


Figure 2-110 Product Selections

4. Select **Install maintenance package** (Figure 2-111) and click **Next**.

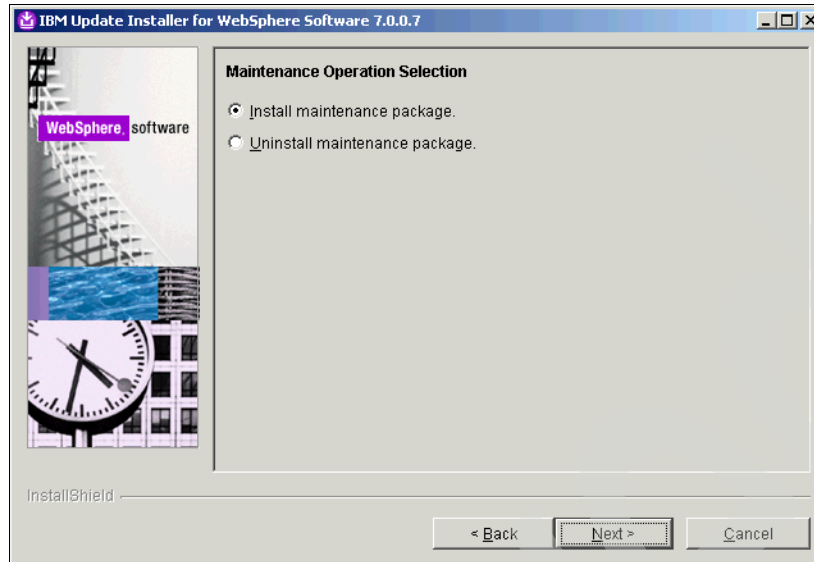


Figure 2-111 Maintenance Operation Selection

5. On the Maintenance Package Directory Selection page (Figure 2-112), browse for the installation package location and update the directory path. Click **Next**.

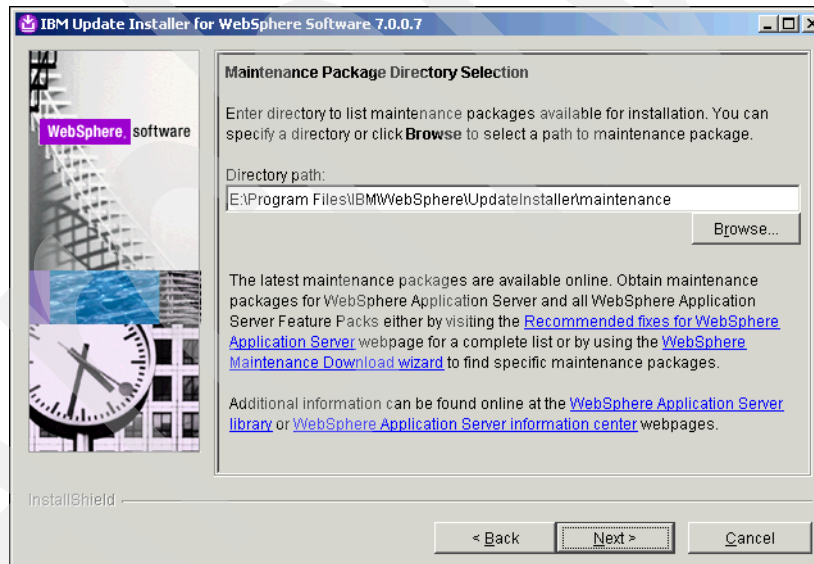


Figure 2-112 Maintenance Package Directory Selection

6. Select **TAMESSO FP00001.pak** (Figure 2-113) and click **Next** to continue.

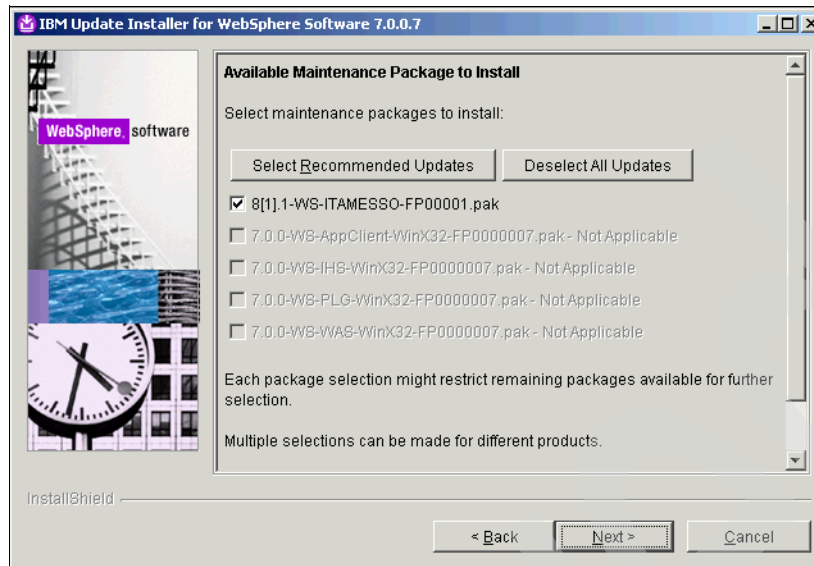


Figure 2-113 Available Maintenance Package to Install

7. From the Installation Summary page, review the installation information and click **Next** (Figure 2-114).

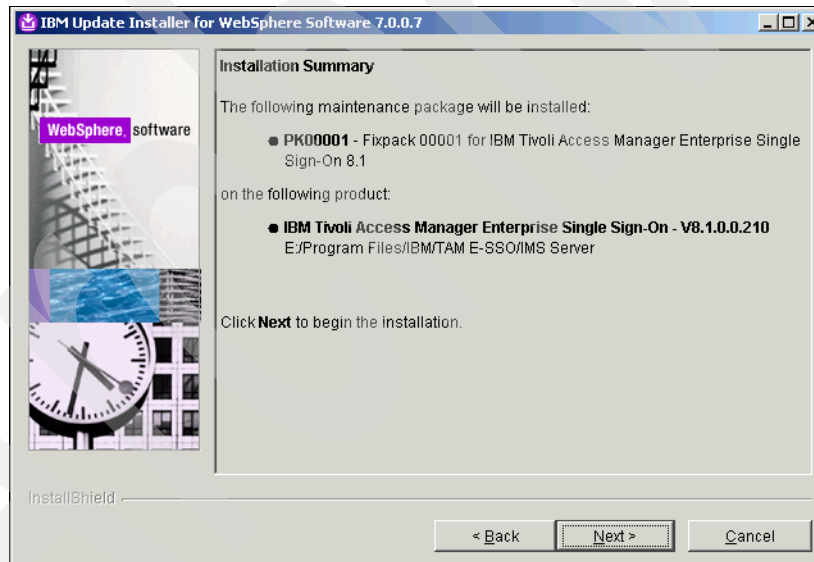


Figure 2-114 Installation Summary

Wait for the installation to complete (Figure 2-115).

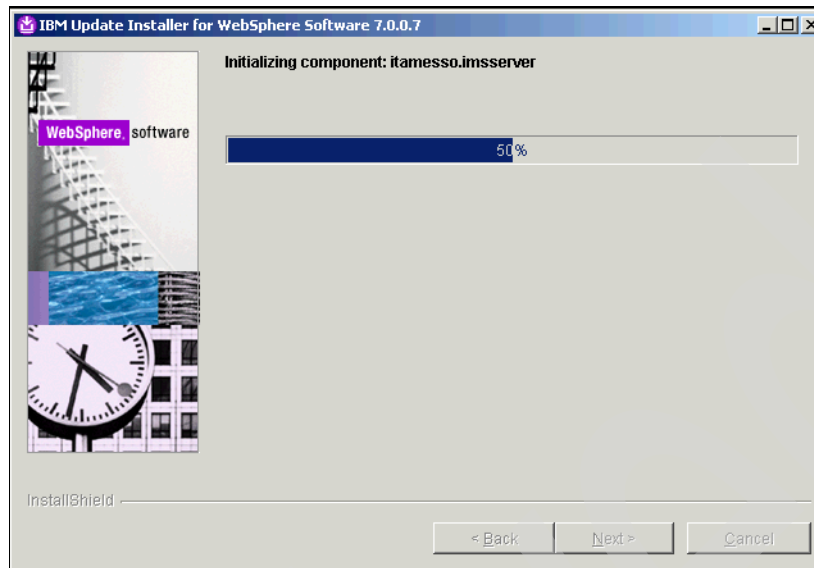


Figure 2-115 Initializing component

8. If the installation is successful, you see the installation complete message (Figure 2-116). Click **Finish** to exit the wizard.

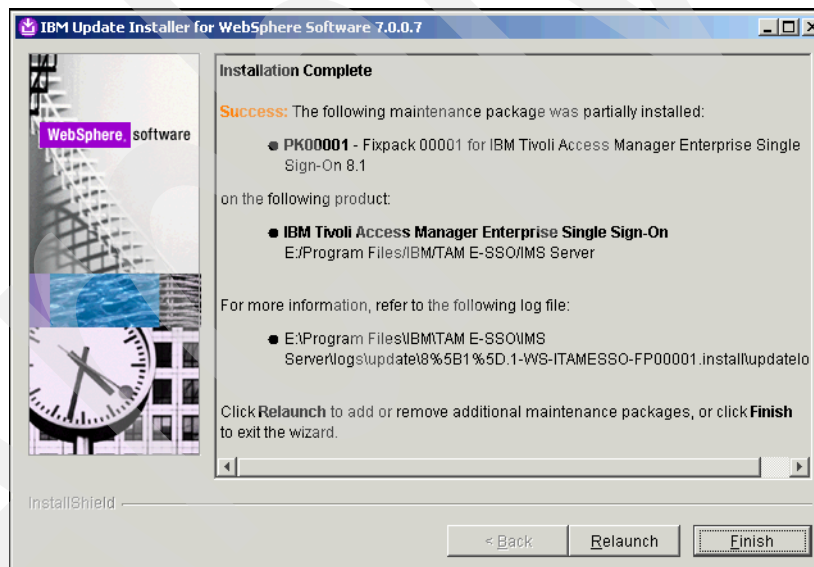


Figure 2-116 Installation Complete

Note: You will see the following message under the Installation Complete heading Success:

The following maintenance package was partially installed.

This message is expected.

2.5 Configuration on WebSphere Application Server

Next we install the Native Library Invoker (NLI) rar file on every node in the WebSphere cluster, install the EAR file, and set up the necessary J2C authentication data.

2.5.1 Installing Native Library Invoker rar file

Log on to the WebSphere Application Server ISC (from the managed node where you ran the IMS installation).

Installing the NLI.RAR on every node in the WebSphere cluster

To install the file:

1. Click **Resources** → **Resource adapters** (Figure 2-117).
2. Click **Install RAR**.

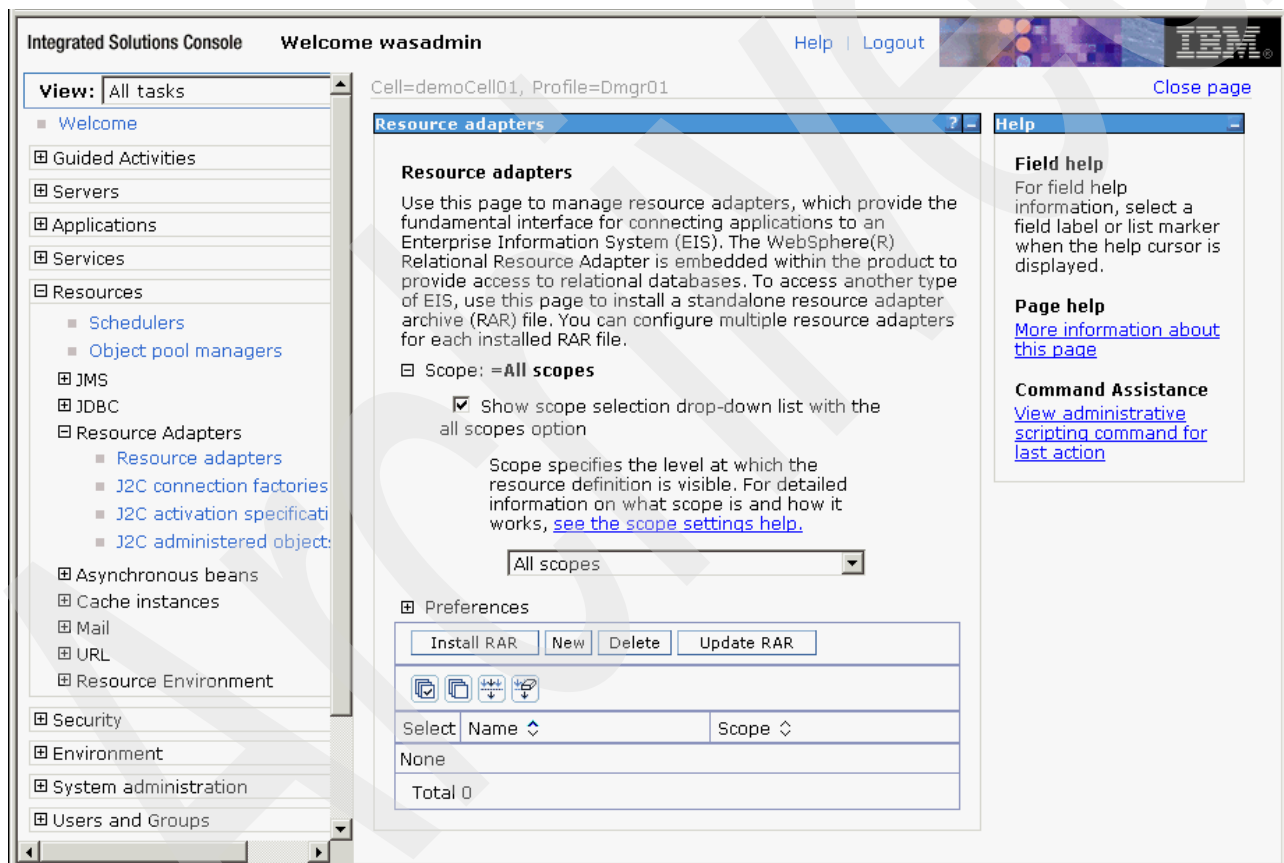


Figure 2-117 Resource adapters

3. On the Install RAR File page (Figure 2-118), select the node (for example, demoNode01) from the Node drop-down menu. Also specify the local file system and enter the path for com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar (for example, E:\Program Files\IBM\TAM E-SSO\IMS Server\com.ibm.tamesso.ims-delhi.j2c.adapters.win32.rar). Click **Next** to continue.

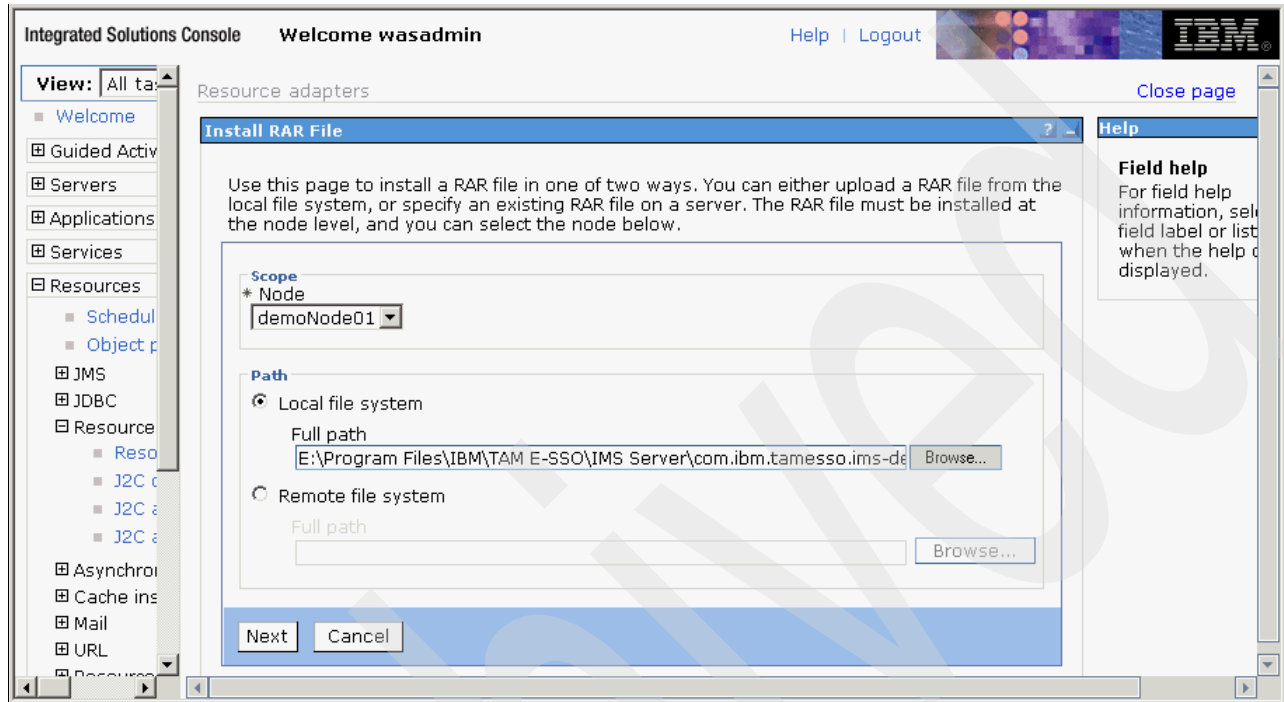


Figure 2-118 Install RAR File

4. Review the general properties (Figure 2-119) and click **OK** to continue.

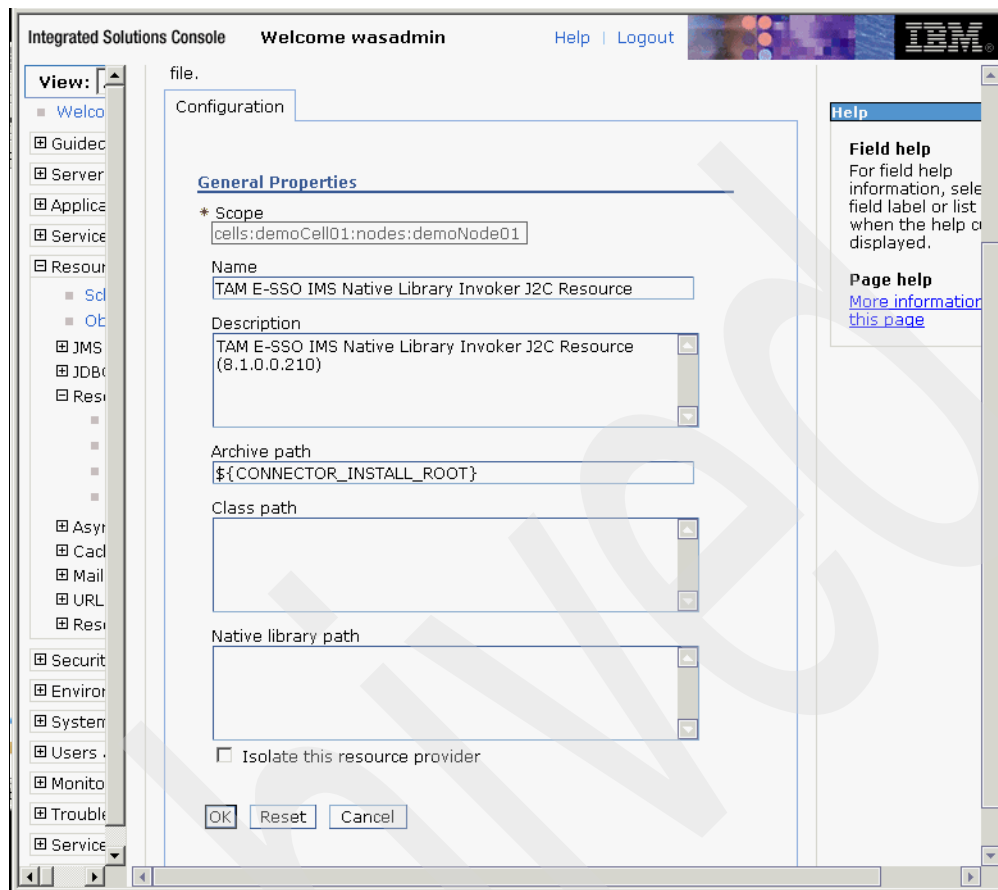


Figure 2-119 Configuration tab - General Properties

5. Click **Save** to save the changes to the master configuration (Figure 2-120).

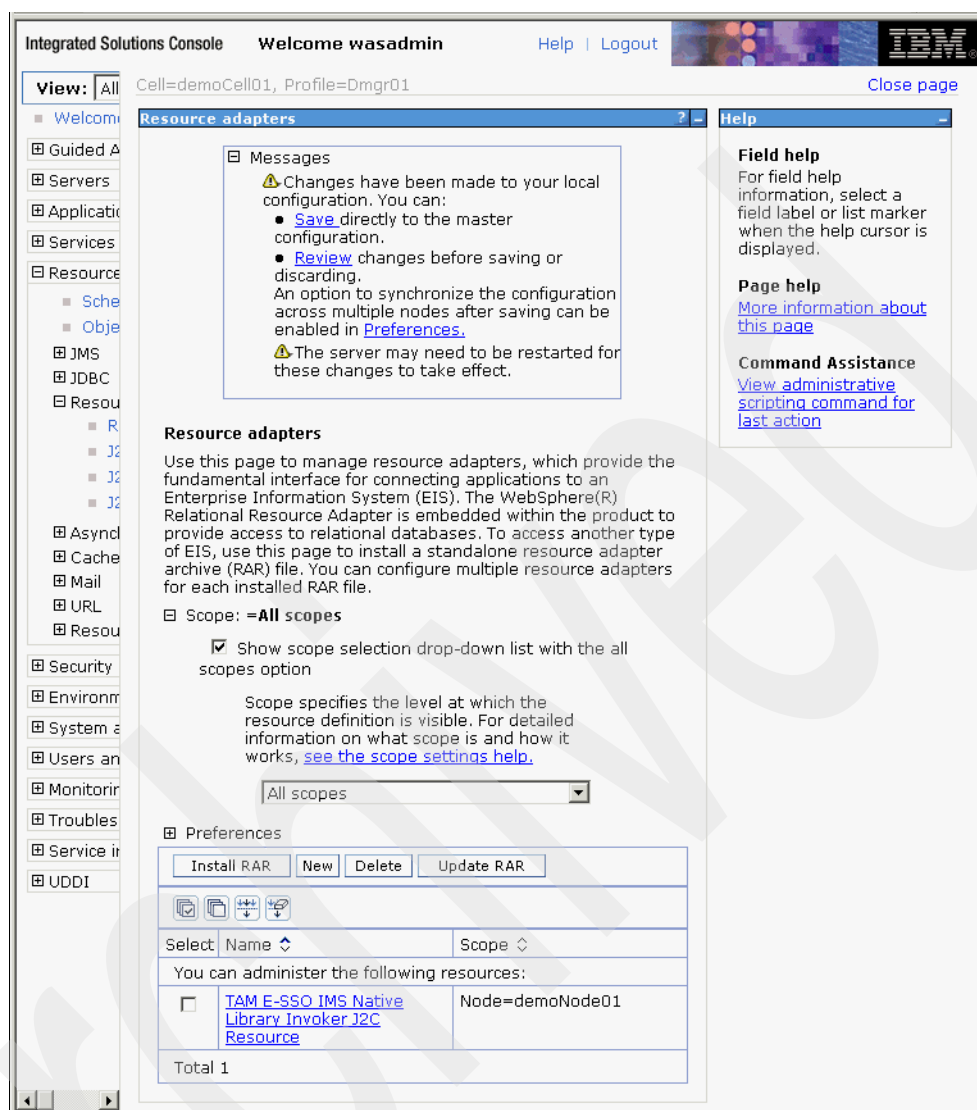


Figure 2-120 Resource adapters

Adding JNDI Key to the connection factory of the NLI Resource Adapter

To add the JNDI Key to the connection factory of the NLI Resource Adapter:

1. From the ISC, click **Resources** → **Resource adapters** → **TAM E-SSO IMS Native Library Invoker J2C Resource**.
2. Under Additional Properties, click **J2C connection factories** (Figure 2-121).

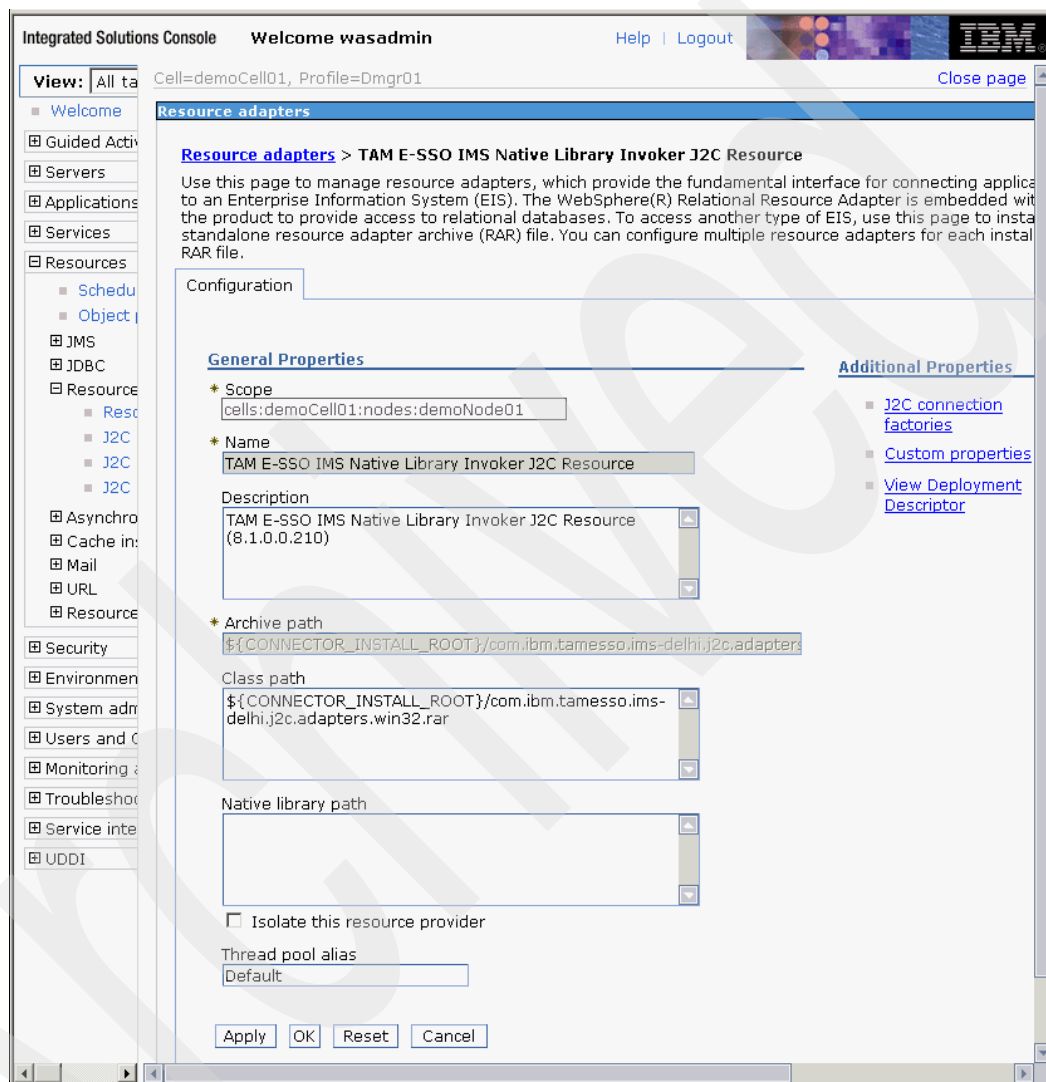


Figure 2-121 Configuration tab - General Properties

3. Click **New** (Figure 2-122).

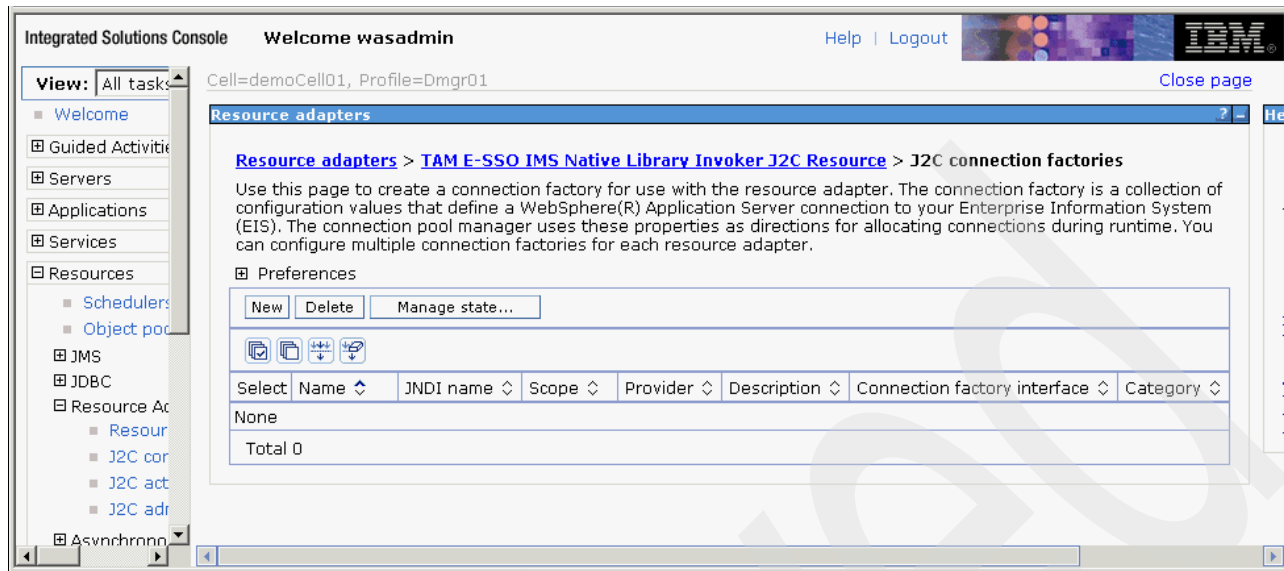


Figure 2-122 J2C connection factories

- From the General Properties page (Figure 2-123), enter TAMESSO_NLI_J2C_ConnFactory in the Name field. Enter tamesso/nli/j2c/shared in the JNDI Name field.

Keep the default values for the other fields. Click **OK** to continue.

Integrated Solutions Console Welcome wasadmin Help | Logout

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
 - Schedule
 - Object pool
 - JMS
 - JDBC
 - Resource Adapter
 - Resource Adapter
 - J2C connection factory
 - J2C connection pool
 - J2C connection pool
 - Asynchronous
 - Cache instance
 - Mail
 - URL
 - Resource bundle
- Security
- Environment
- System administration
- Users and Groups
- Monitoring and Alerts
- Troubleshooting
- Service integration
- UDDI

Use this page to create a connection factory for use with the resource adapter. The connection factory is a collection of configuration values that define a WebSphere(R) Application Server connection to your Enterprise Information System (EIS). The connection pool manager uses these properties as directions for allocating connections during runtime. You can configure multiple connection factories for each resource adapter.

Configuration

General Properties

* Scope
cells:demoCell01:nodes:demoNode01

* Provider
TAM E-SSO IMS Native Library
Invoker J2C Resource

* Name
TAMESSO_NLI_J2C_ConnFactory

JNDI name
tamesso/nli/j2c/shared

Description

* Connection factory interface
javax.resource.cci.ConnectionFactory

Category

Security settings

Select the authentication values for this resource.

Component-managed authentication alias
(none)

Mapping-configuration alias
DefaultPrincipalMapping

Container-managed authentication alias
(none)

Container-managed authentication

Authentication preference
None

Apply OK Reset Cancel

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

Additional Properties

- Connection pool properties
- Advanced connection factory properties
- Custom properties

Related Items

- JAAS - J2C authentication data

Figure 2-123 JNDI name

5. Click **Save** to save the changes to the master configuration (Figure 2-124).

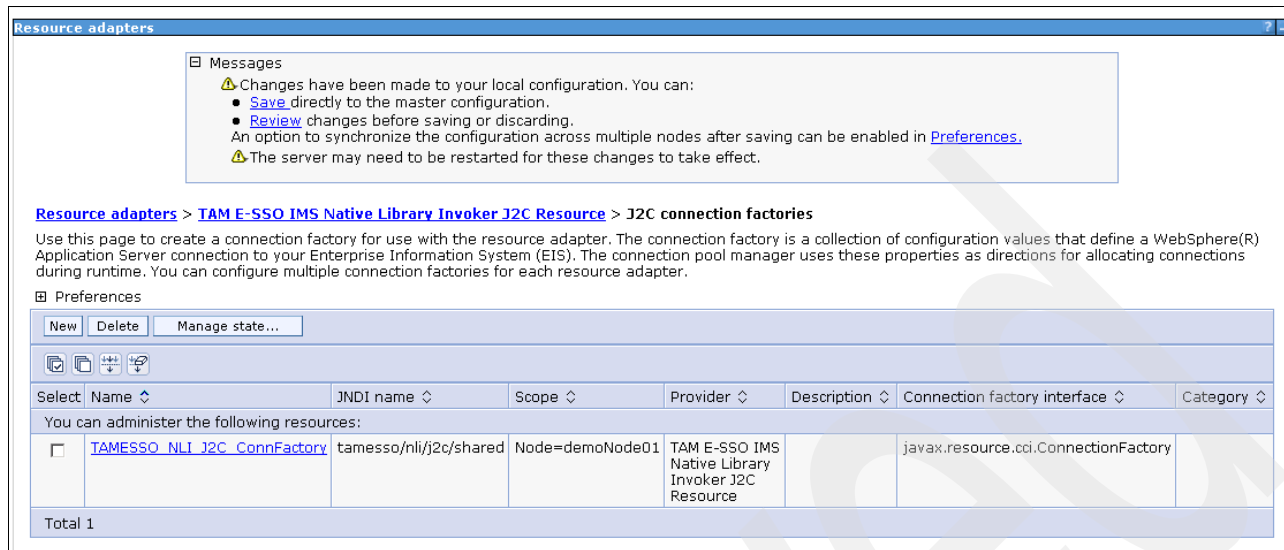


Figure 2-124 J2C connection factories

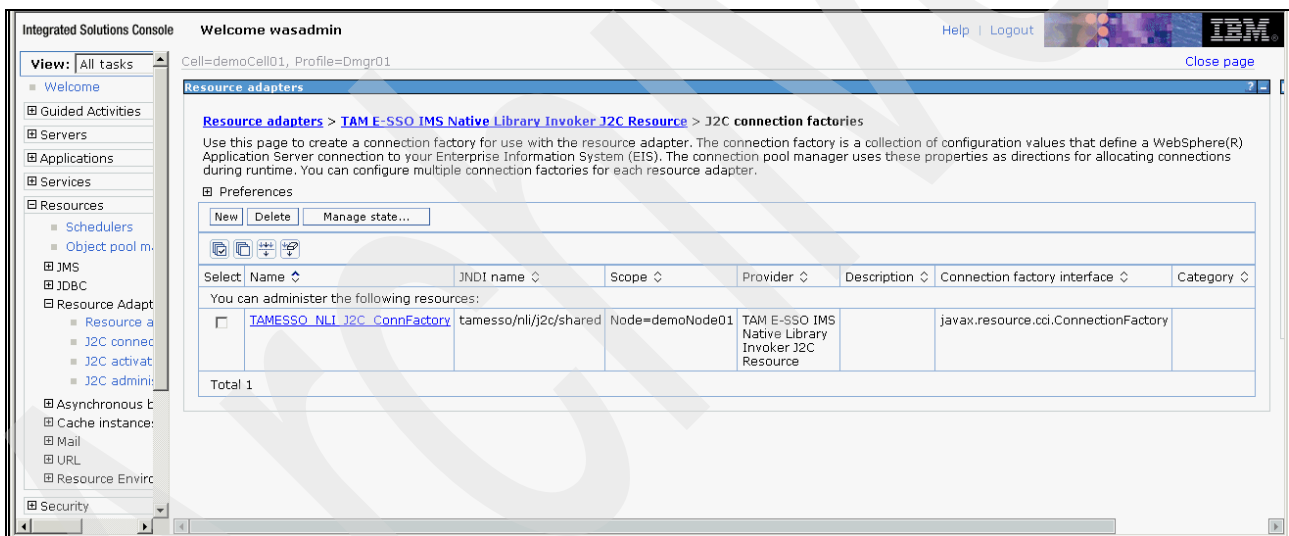


Figure 2-125 J2C connection factories

Note: For every node in the WebSphere Cluster, repeat the previous steps for all other nodes in the WebSphere cluster.

2.5.2 Installing IMS Server ear file

To install the IMS Server ear file:

1. Log in to the WebSphere Application Server ISC (on the managed node where you ran the IMS Server installation).
2. Click Applications → Application types → WebSphere Enterprise Applications (Figure 2-126).
3. Click **Install**.

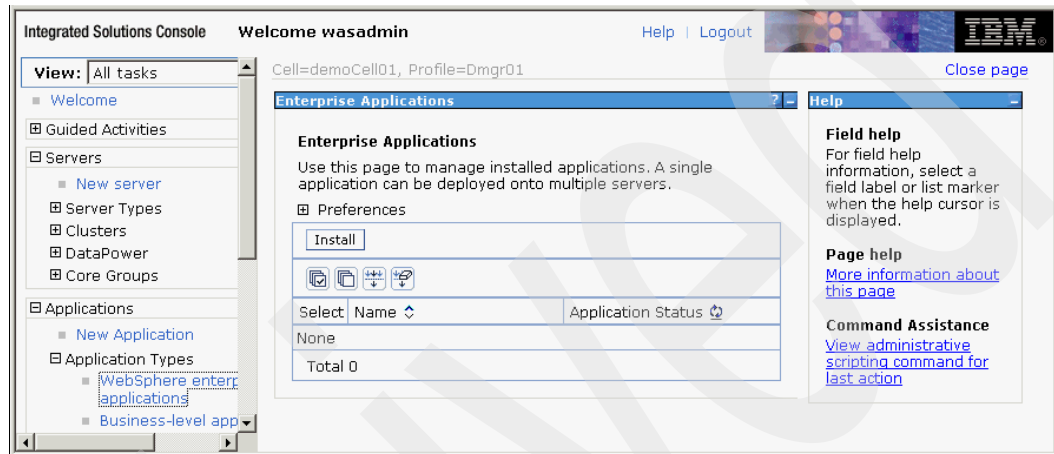


Figure 2-126 Enterprise Applications

4. On the Preparing for the application installation page (Figure 2-127), select **Local file system** and specify the full path for the EAR file (for example, E:\Program Files\IBM\TAM E-SSO\IMS Server\com.ibm.tamesso.ims-delhi.deploy.all.ear). Click **Next**.

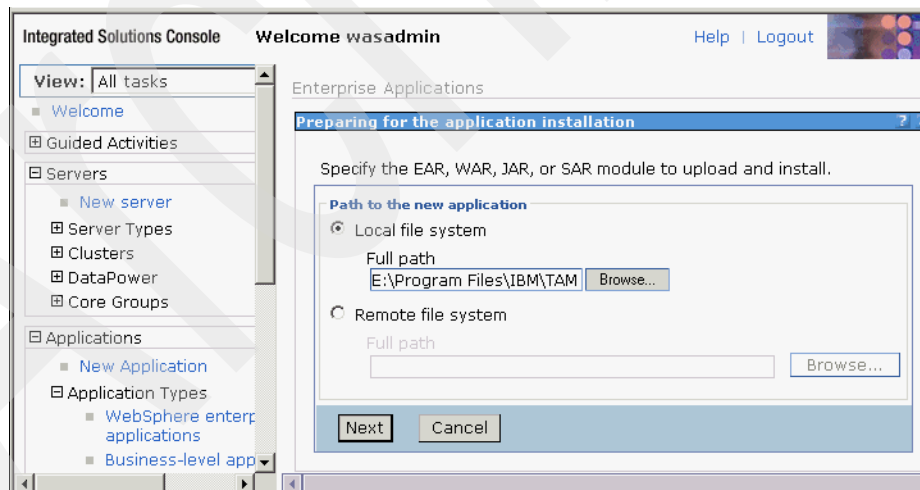


Figure 2-127 Preparing for the application installation

5. Select **Fast Path** to only prompt when additional information is required (Figure 2-128) and click **Next**.

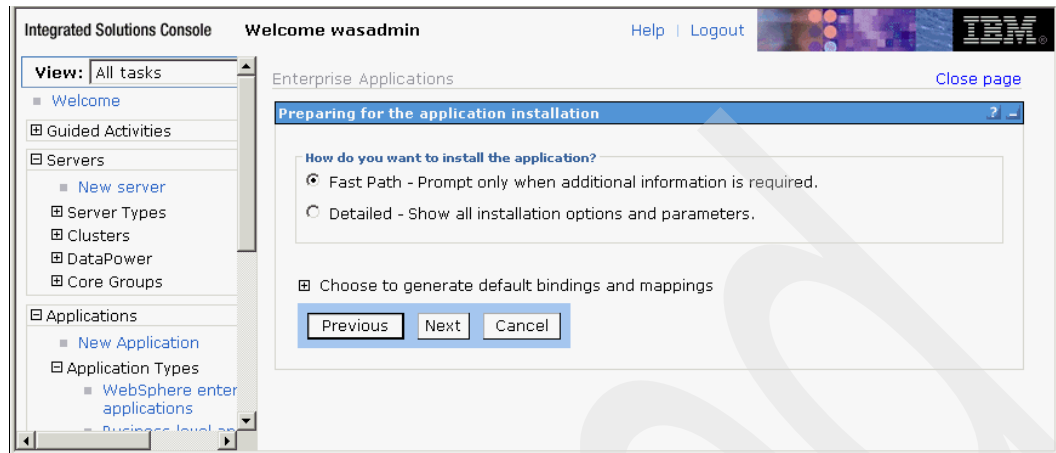


Figure 2-128 Preparing for the application installation - Fast Path

6. Retain the default values (Figure 2-129) and click **Next**.

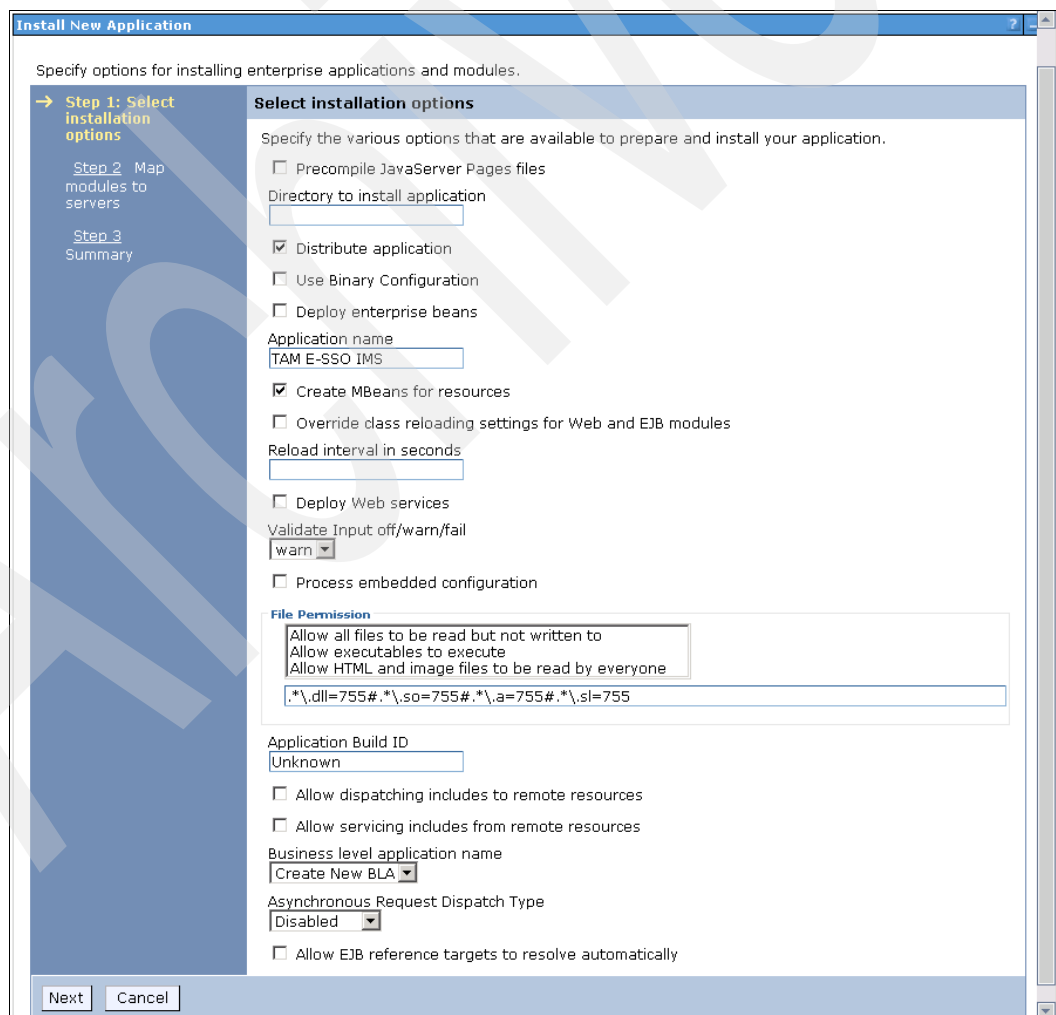


Figure 2-129 Select installation options

Install New Application

Specify options for installing enterprise applications and modules.

Step 1 Select installation options

→ Step 2: Map modules to servers

Step 3 Summary

Map modules to servers

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 route requests to this application. The plug-in configuration file (plugin-cfg.xml) for each Web server is generated on the applications that are routed through.

Clusters and servers:

WebSphere:cell=demoCell01,cluster=cluster1

WebSphere:cell=demoCell01,node=demoNode01,server=webserver1

Apply

Select

Module

URI

Server

☒

TAM E-SSO IMS Static Assets (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-static.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS Frontdoor (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-front.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS WebConfigurator (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-webConfigurator.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS AccessAdmin (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-accessAdmin.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS Legacy Runtime (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.runtime.ws-axis1.0.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS AccessAssistantWebWorkplace (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-accessAssistant.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS AccessAdmin Help (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-help-accessAdmin.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

☒

TAM E-SSO IMS AccessAssistant Help (8.1.0.0.281)

com.ibm.tamesso.ims-delhi.webapp-help-accessAssistant.war,WEB-INF/web.xml

WebSphere:cell=demoCell01,cluster=cluster1

Previous

Next

Cancel

Figure 2-130 Map modules to servers

- On the Map modules to servers page (Figure 2-131), select all check boxes. Then select both the target cluster and the web server from the Clusters and servers list.. Click **Apply**, and then click **Next** to continue.

Install New Application

Specify options for installing enterprise applications and modules.

Step 1 Select installation options

→ Step 2: Map modules to servers

Step 3 Summary

Map modules to servers

Specify targets such as application servers or clusters of application servers where you want to install the your application. Modules can be installed on the same application server or dispersed among several app the Web servers as targets that serve as routers for requests to this application. The plug-in configuration Web server is generated, based on the applications that are routed through.

Clusters and servers:

WebSphere:cell=demoCell01,cluster=cluster1

WebSphere:cell=demoCell01,node=demoNode01,server=webserver1

Apply

Select	Module	URI	Server
<input type="checkbox"/>	TAM E-SSO IMS Static Assets (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-static.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS Frontdoor (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-front.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS WebConfigurator (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-webConfigurator.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS AccessAdmin (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-accessAdmin.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS Legacy Runtime (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.runtime.ws-axis1.0.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS AccessAssistantWebWorkplace (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-accessAssistant.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS AccessAdmin Help (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-help-accessAdmin.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1
<input type="checkbox"/>	TAM E-SSO IMS AccessAssistant Help (8.1.0.0.281)	com.ibm.tamesso.ims-delhi.webapp-help-accessAssistant.war,WEB-INF/web.xml	WebSphere:cell=demoCell01,node=demoNode01,server=webserver1

Previous

Next

Cancel

Figure 2-131 Map modules to servers

8. Review the installation summary (Figure 2-132) and click **Finish**.

Install New Application

Specify options for installing enterprise applications and modules.

Step 1 Select installation options

Step 2 Map modules to servers

→ Step 3: Summary

Summary

Summary of installation options

Options	Values
Precompile JavaServer Pages files	No
Directory to install application	
Distribute application	Yes
Use Binary Configuration	No
Deploy enterprise beans	No
Application name	TAM E-SSO IMS
Create MBeans for resources	Yes
Override class reloading settings for Web and EJB modules	No
Reload interval in seconds	
Deploy Web services	No
Validate Input off/warn/fail	warn
Process embedded configuration	No
File Permission	.*\,dll=755#.*\,so=755#.*\,a=755#.*\,sl=755
Application Build ID	Unknown
Allow dispatching includes to remote resources	No
Allow servicing includes from remote resources	No
Business level application name	
Asynchronous Request Dispatch Type	Disabled
Allow EJB reference targets to resolve automatically	No
Cell/Node/Server	Click here

Previous

Finish

Cancel

Figure 2-132 Summary

9. Click **Save** (Figure 2-133) to save changes directly to the master configuration.



Figure 2-133 Installing

2.5.3 Administering Tivoli Access Manager for Enterprise Single Sign-On from WebSphere Application Server

To perform this administration:

1. From the WebSphere ISC, click **Applications** → **Application Types** → **WebSphere Enterprise Applications**.
2. Click **TAM E-SSO IMS** to administer it (Figure 2-134).

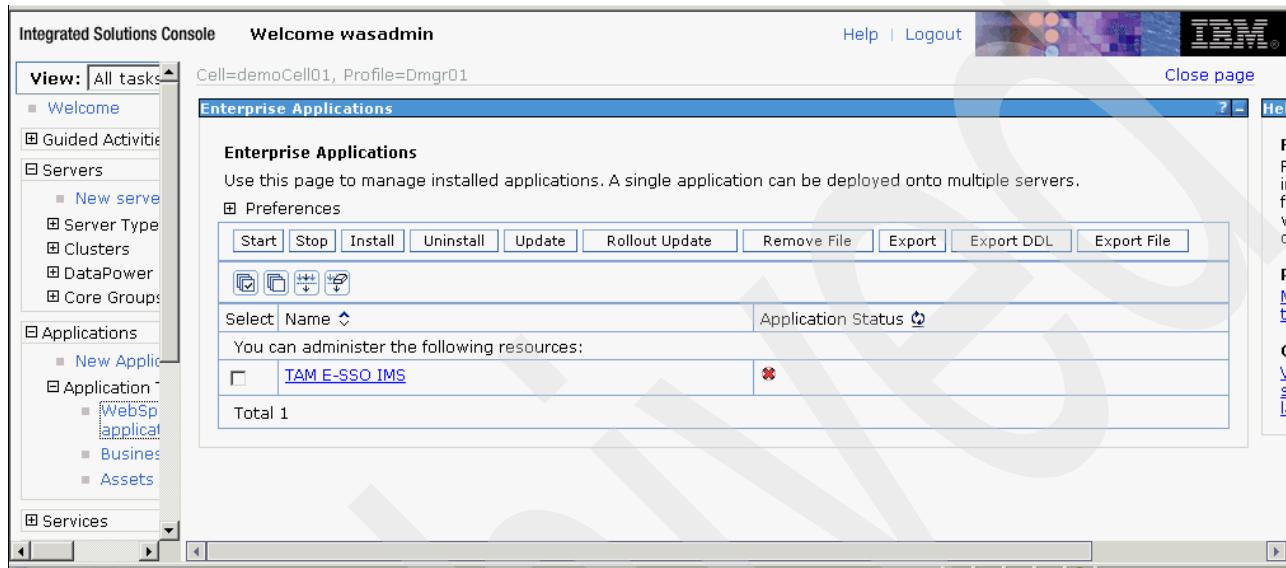


Figure 2-134 Enterprise Applications

3. Under Web Module Properties, click **Session management** (Figure 2-135).

The screenshot shows the 'Enterprise Applications' configuration window for 'TAM E-SSO IMS'. The window has a title bar and a breadcrumb trail 'Enterprise Applications > TAM E-SSO IMS'. Below the breadcrumb, there is a brief instruction: 'Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.' A 'Configuration' tab is selected. The main content area is divided into several sections: 'General Properties' with fields for 'Name' (TAM E-SSO IMS) and 'Application reference validation' (Issue warnings); 'Detail Properties' with links for 'Target specific application status', 'Startup behavior', 'Application binaries', 'Class loading and update detection', 'Request dispatcher properties', 'Security role to user/group mapping', 'View Deployment Descriptor', 'Last participant support extension', and 'References' (Shared library references, Shared library relationships); 'Modules' with a link for 'Manage Modules'; 'Web Module Properties' with links for 'Session management', 'Context Root For Web Modules', 'JSP and JSF options', and 'Virtual hosts'; 'Enterprise Java Bean Properties' with a link for 'Default messaging provider references'; and 'Database Profiles' with a link for 'SQLJ profiles and pureQuery bind files'. At the bottom, there are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

Enterprise Applications

Enterprise Applications > TAM E-SSO IMS

Use this page to configure an enterprise application. Click the links to access pages for further configuring of the application or its modules.

Configuration

General Properties

* Name
TAM E-SSO IMS

Application reference validation
Issue warnings

Detail Properties

- Target specific application status
- Startup behavior
- Application binaries
- Class loading and update detection
- Request dispatcher properties
- Security role to user/group mapping
- View Deployment Descriptor
- Last participant support extension

References

- Shared library references
- Shared library relationships

Modules

- Manage Modules

Web Module Properties

- Session management
- Context Root For Web Modules
- JSP and JSF options
- Virtual hosts

Enterprise Java Bean Properties

- Default messaging provider references

Database Profiles

- SQLJ profiles and pureQuery bind files

Apply OK Reset Cancel

Figure 2-135 Tivoli Access Manager for Enterprise Single Sign-On IMS

4. Under General Properties (Figure 2-136), check the Override session management check box to select it. Click **Apply**.

Enterprise Applications

[Enterprise Applications](#) > [TAM E-SSO IMS](#) > **Session management**

Use this page to configure session manager properties to control the behavior of Hypertext Transfer Protocol (HTTP) session support. These settings apply to both the SIP container and the Web container.

Configuration

General Properties	Additional Properties
<input checked="" type="checkbox"/> Override session management	Custom properties
Session tracking mechanism: <input type="checkbox"/> Enable SSL ID tracking <input checked="" type="checkbox"/> Enable cookies <input type="checkbox"/> Enable URL rewriting <input type="checkbox"/> Enable protocol switch rewriting	Distributed environment settings
<input checked="" type="checkbox"/> Allow overflow Maximum in-memory session count: <input type="text" value="1000"/> sessions	
Session timeout: <input type="radio"/> No timeout <input checked="" type="radio"/> Set timeout <input type="text" value="30"/> minutes	
<input type="checkbox"/> Security integration	
Serialize session access: <input type="checkbox"/> Allow serial access Maximum wait time <input type="text" value="0"/> seconds <input checked="" type="checkbox"/> Allow access on timeout	

Figure 2-136 Session management

5. Click **Save** (Figure 2-137).

Cell=demoCell01, Profile=Dmgr01

Enterprise Applications

Messages

- ⚠ The session management changes apply to both the SIP container and the Web container.
- ⚠ 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.

[Enterprise Applications](#) > [TAM E-SSO IMS](#) > Session management

Use this page to configure session manager properties to control the behavior of Hypertext Transfer Protocol (HTTP) session support. These settings apply to both the SIP container and the Web container.

Configuration

General Properties

☒ Override session management

Session tracking mechanism:

☐ Enable SSL ID tracking

☒ [Enable cookies](#)

☐ Enable URL rewriting

☐ [Enable protocol switch rewriting](#)

☒ Allow overflow

Maximum in-memory session count:

sessions

Session timeout:

☐ No timeout

☒ Set timeout
 minutes

☐ Security integration

Additional Properties

- [Custom properties](#)
- [Distributed environment settings](#)

Figure 2-137 Configuration tab

6. Click the **TAM E-SSO IMS** hyperlink at the top of the page. Under Additional Properties, click **Distributed environment settings**.

7. Ensure that **None** is selected under distributed sessions (Figure 2-138) and click **OK**.

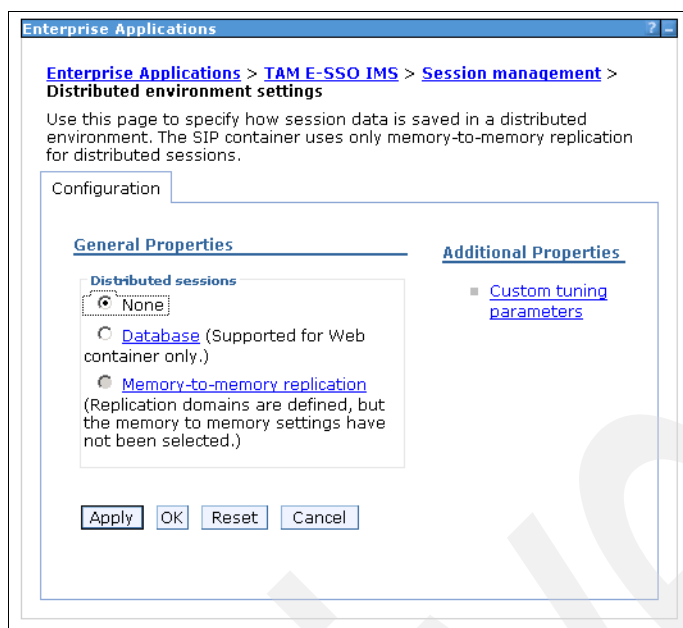


Figure 2-138 General Properties

8. Click **OK**, then click **Save** (Figure 2-139).

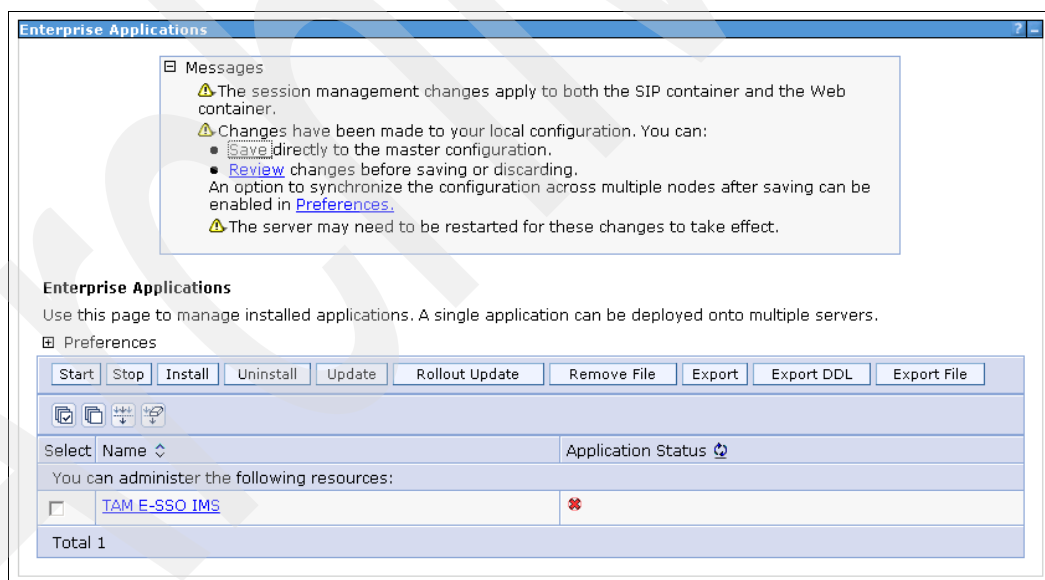


Figure 2-139 Preferences

9. Click the **TAM E-SSO IMS** hyperlink at the top of the page.
10. From the Detail Properties section, click **Target Specific Application Status**.

11. Select the cluster under which IMS is installed and click **Disable Auto Start** (Figure 2-140).

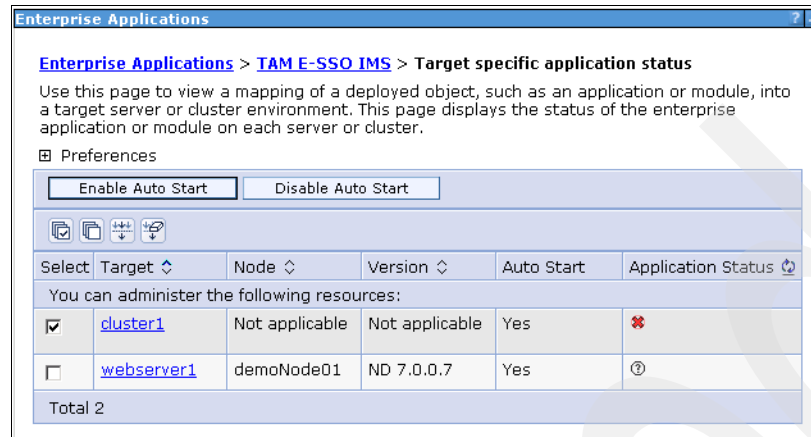


Figure 2-140 Target specific application status

Note: A limitation of the IMS Server 8.1 deployment (prior to IMS Server 8.1 fix pack 2) requires disabling of autostart for the IMS Server. You have to manually start the IMS Server every that time the WebSphere Application Server is restarted.

12. Click **Save** (Figure 2-141) to save changes directly to the master configuration.

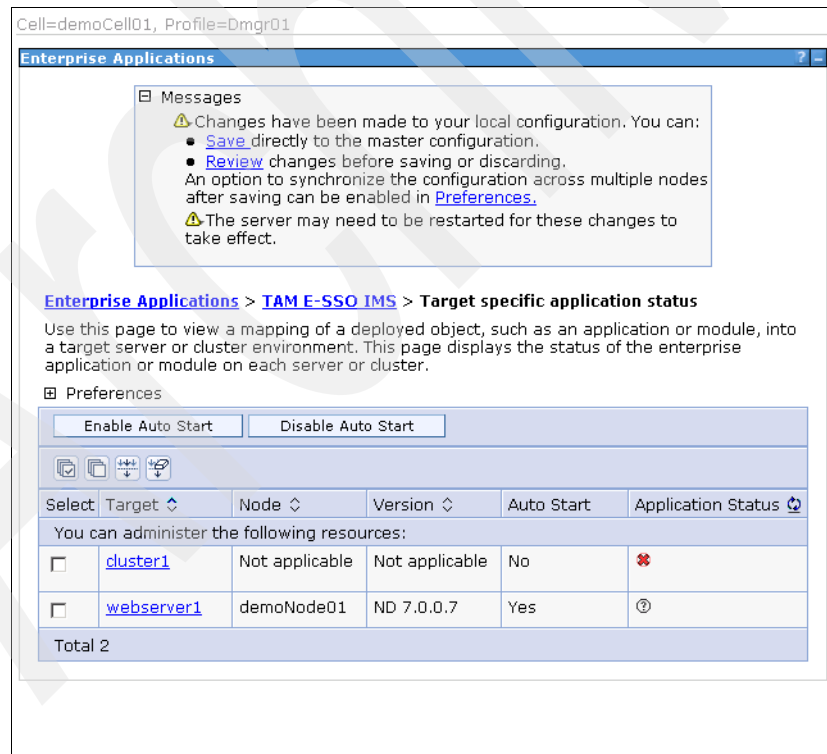


Figure 2-141 Preferences

2.5.4 Importing root certificate to CellDefaultKeyStore

To import the root certificate from the DMgrDefaultRootStore to the CellDefaultKeyStore with the same certificate alias name, follow the steps below:

1. From the WebSphere Integrated Solutions Console, click **Security** → **SSL Certificate and Key management**. Under Related Items, click **KeyStores and certificates** (Figure 2-142).

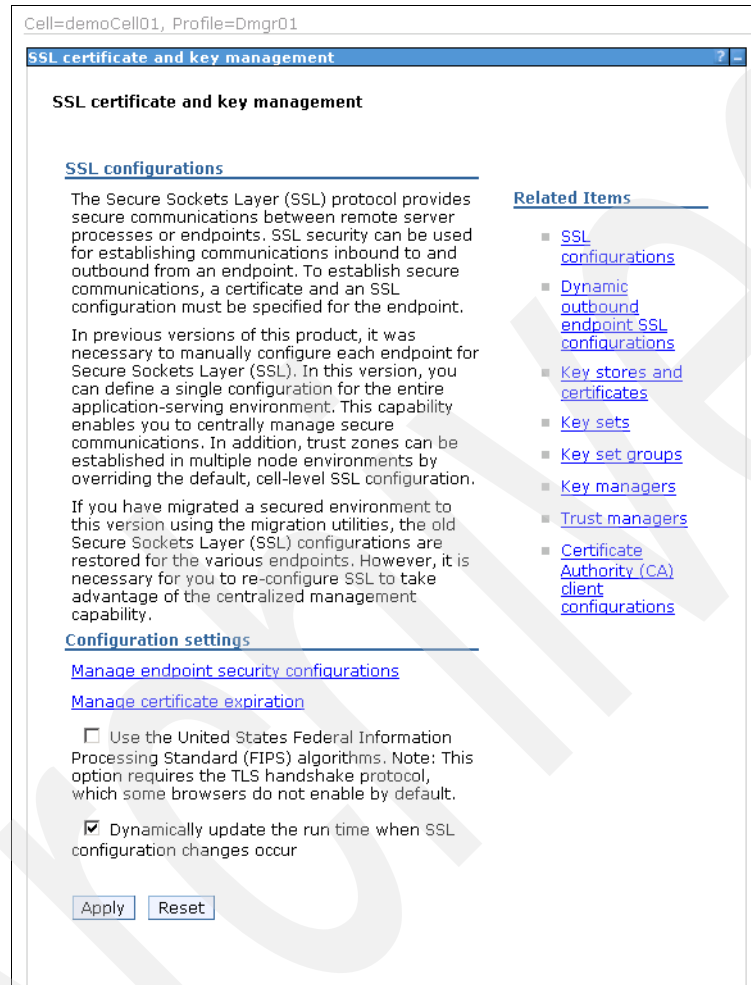


Figure 2-142 SSL certificate and key management

2. Click **CellDefaultKeyStore** (Figure 2-143).

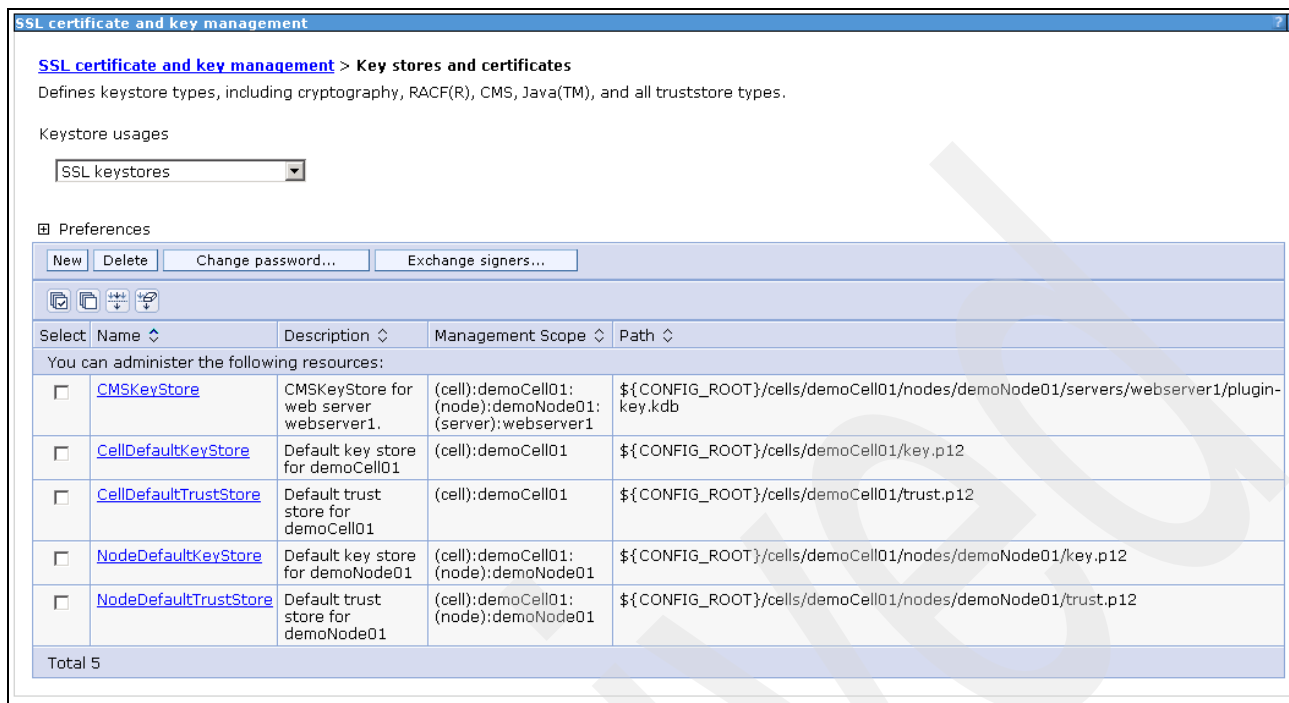


Figure 2-143 Key stores and certificates

3. Under Additional Properties, click **Personal Certificates** (Figure 2-144).

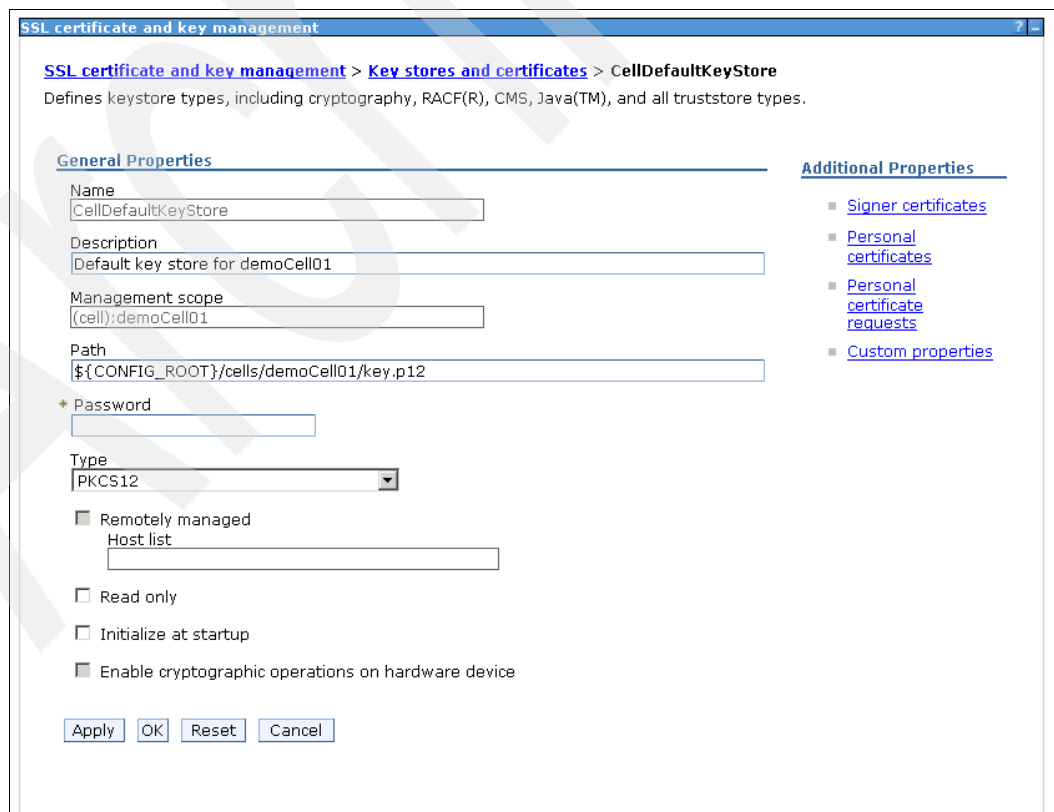


Figure 2-144 CellDefaulttKeyStore

4. Click **Import** (Figure 2-145).

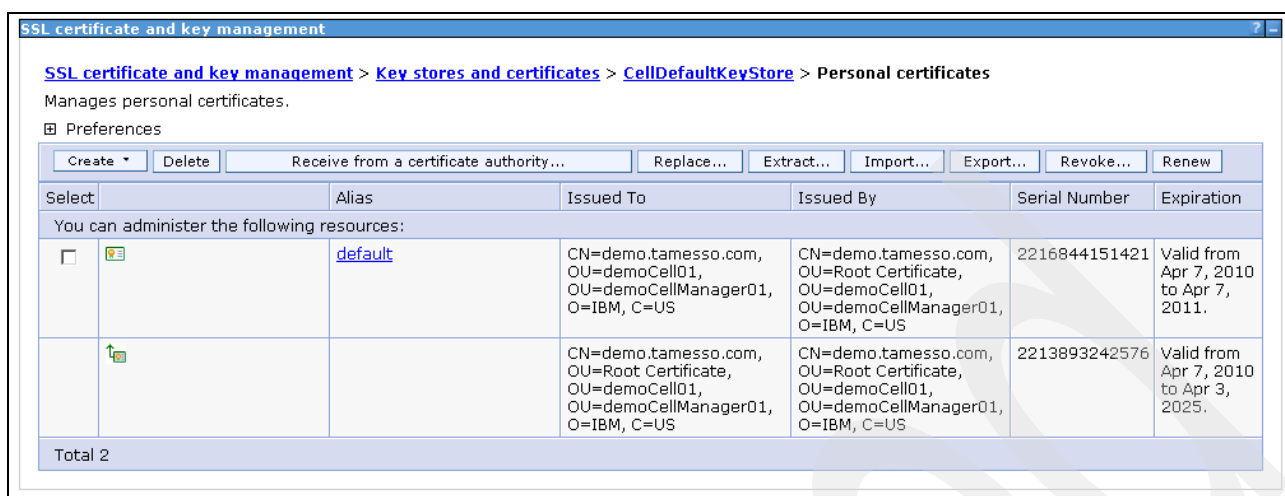


Figure 2-145 Personal certificates

5. Under General Properties, select **Managed key store** (Figure 2-146).

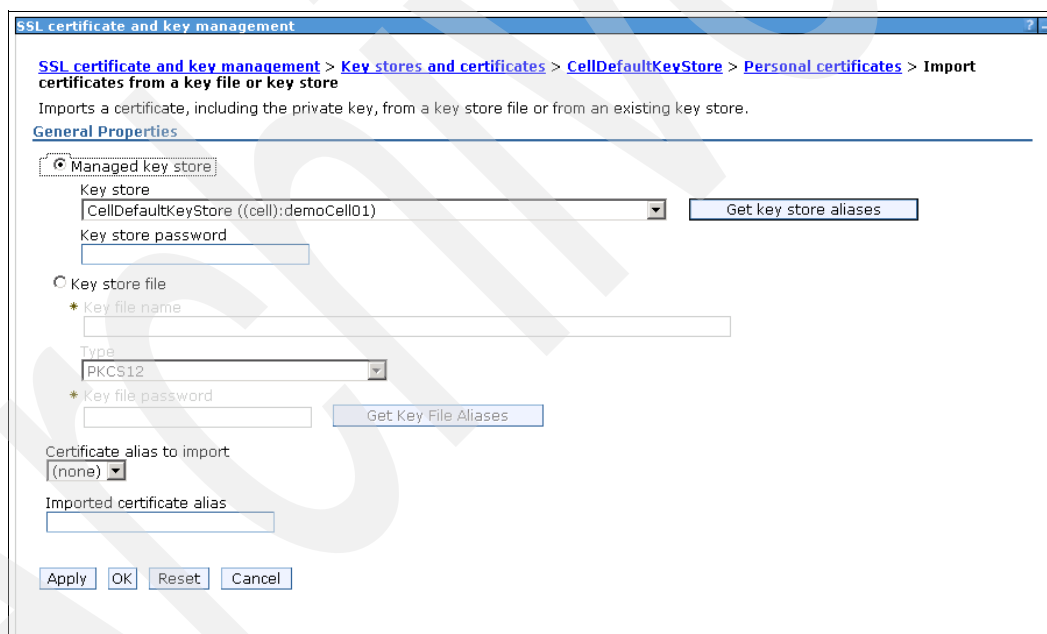


Figure 2-146 Import certificates from a key file or key store

6. Select **DmgrDefaultRootStore** from the KeyStore drop-down menu, enter WebAS as the key store password (Figure 2-147), and click **Get key store aliases**.

SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > Personal certificates > Import certificates from a key file or key store

Imports a certificate, including the private key, from a key store file or from an existing key store.

General Properties

☒ Managed key store

Key store
DmgrDefaultRootStore ((cell):demoCell01:(node):demoCellManager01) [Get key store aliases]

Key store password
WebAS

☐ Key store file

* Key file name

Type
PKCS12

* Key file password [Get Key File Aliases]

Certificate alias to import
(none)

Imported certificate alias

Apply OK Reset Cancel

Figure 2-147 Import certificates from a key file or key store

7. Select **root** for the certificate alias to import. Type root in the Imported certificate alias field. Click **OK** to continue (Figure 2-148).

SSL certificate and key management > Key stores and certificates > CellDefaultKeyStore > Personal certificates > Import certificates from a key file or key store

Imports a certificate, including the private key, from a key store file or from an existing key store.

General Properties

☒ Managed key store

Key store
DmgrDefaultRootStore ((cell):demoCell01:(node):demoCellManager01) [Get key store aliases]

Key store password
WebAS

☐ Key store file

* Key file name

Type
PKCS12

* Key file password [Get Key File Aliases]

Certificate alias to import
root

Imported certificate alias
root

Apply OK Reset Cancel

Figure 2-148 Import certificates from a key file or key store

8. Click **Save** to save directly to the master configuration (Figure 2-149).

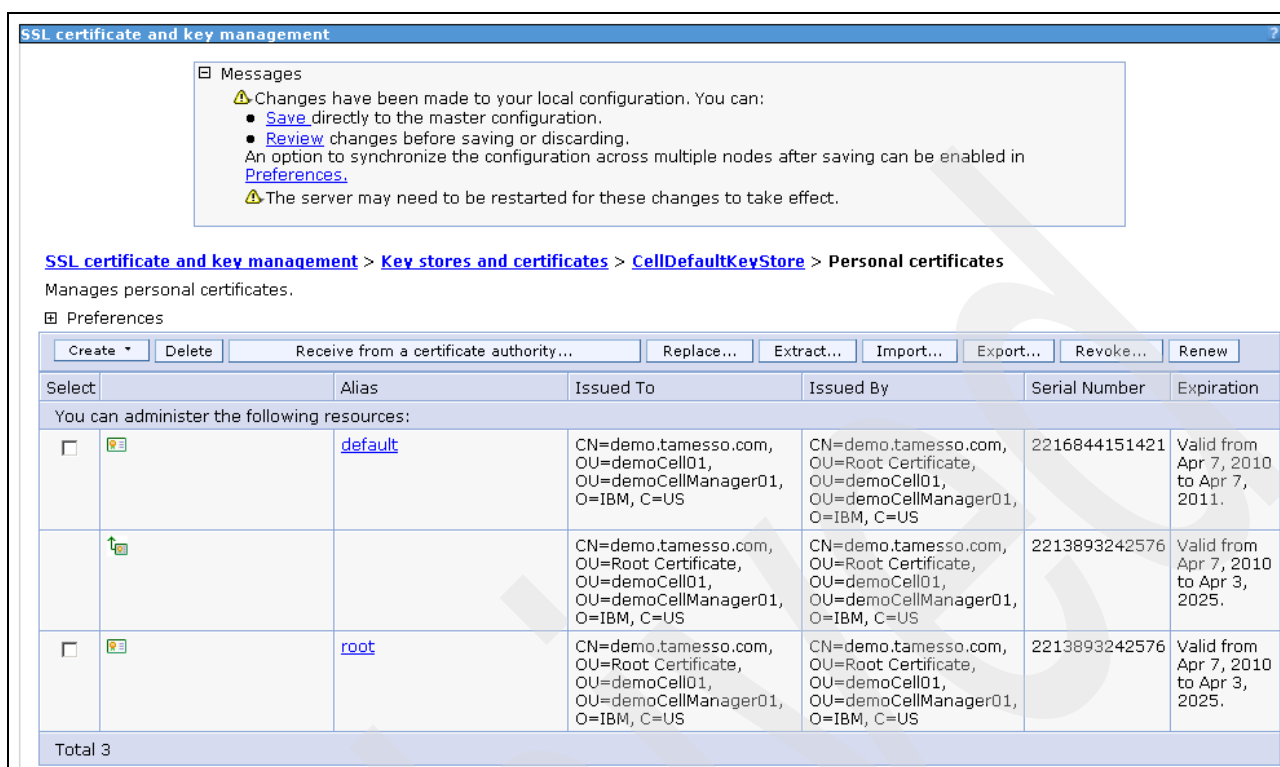


Figure 2-149 Personal certificates

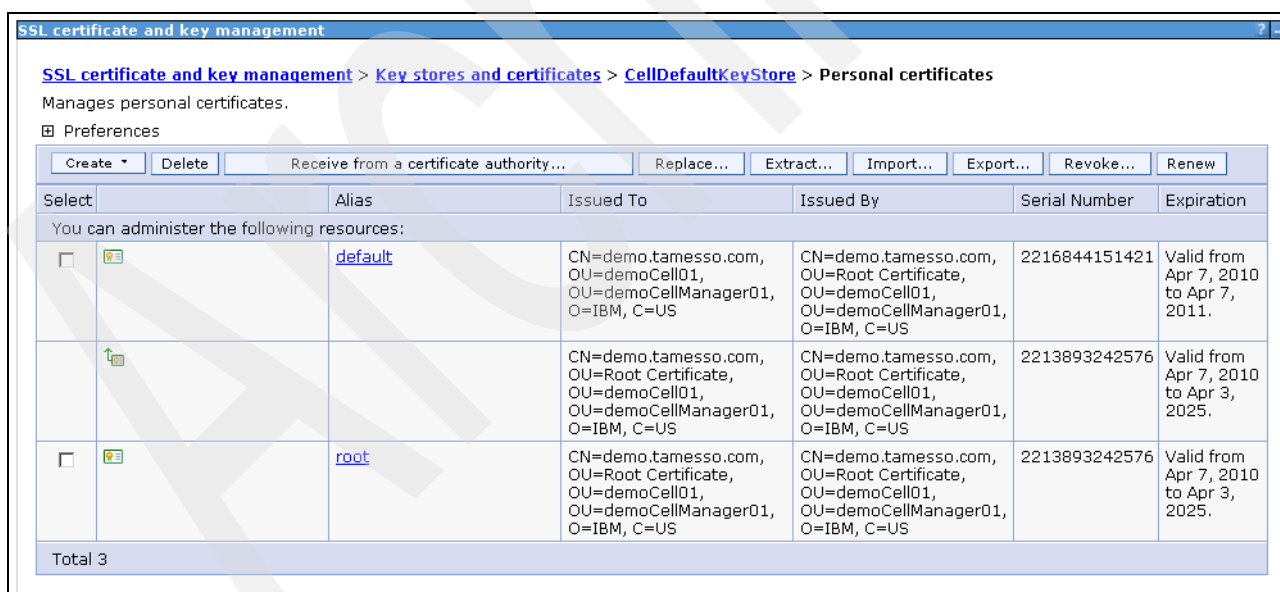


Figure 2-150 Personal certificates

2.5.5 Copying \tamesso directory

Copy the \tamesso directory from the IMS installation directory (E:\Program Files\IBM\TAM E-SSO\IMS Server) to E:\Program Files\IBM\WebSphere\AppServer\profiles\Dmgr01\config.

2.5.6 Resynchronizing nodes

To resynchronize nodes:

1. From the WebSphere ISC, click **System Administration** → **Nodes** (Figure 2-151).

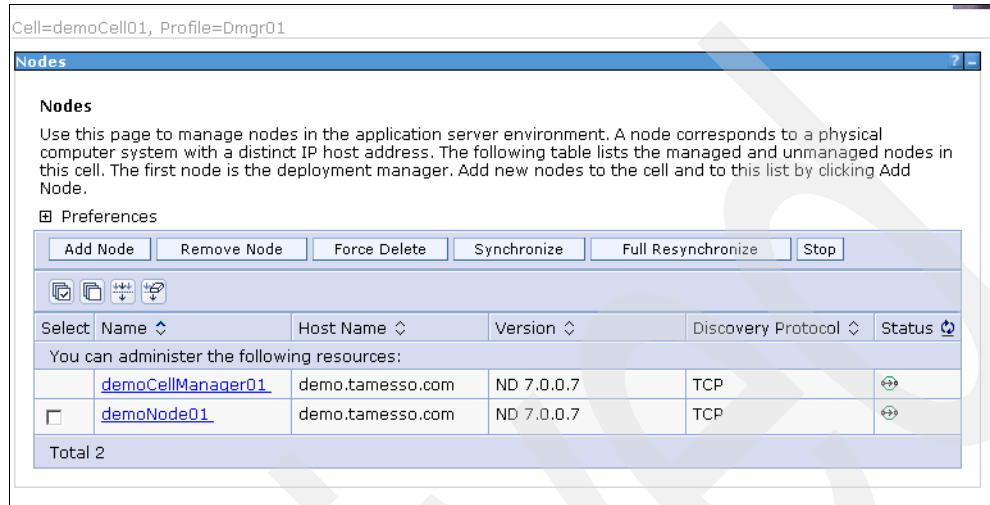


Figure 2-151 Nodes

2. Select the check box for the node on which the IMS Server is installed (for example, demoNode01) and click **Full resynchronize** (Figure 2-152).

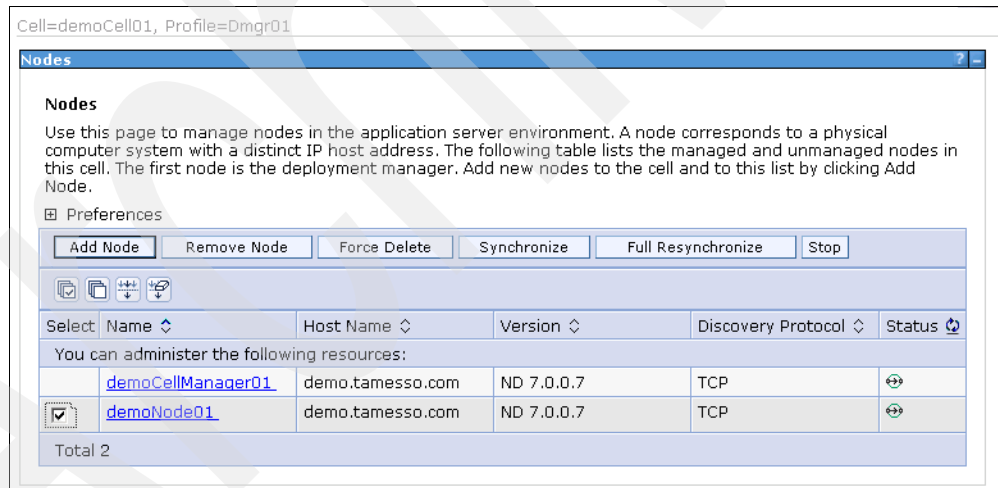


Figure 2-152 Nodes - demoNode01

3. Verify that the synchronization is successfully initiated (Figure 2-153).

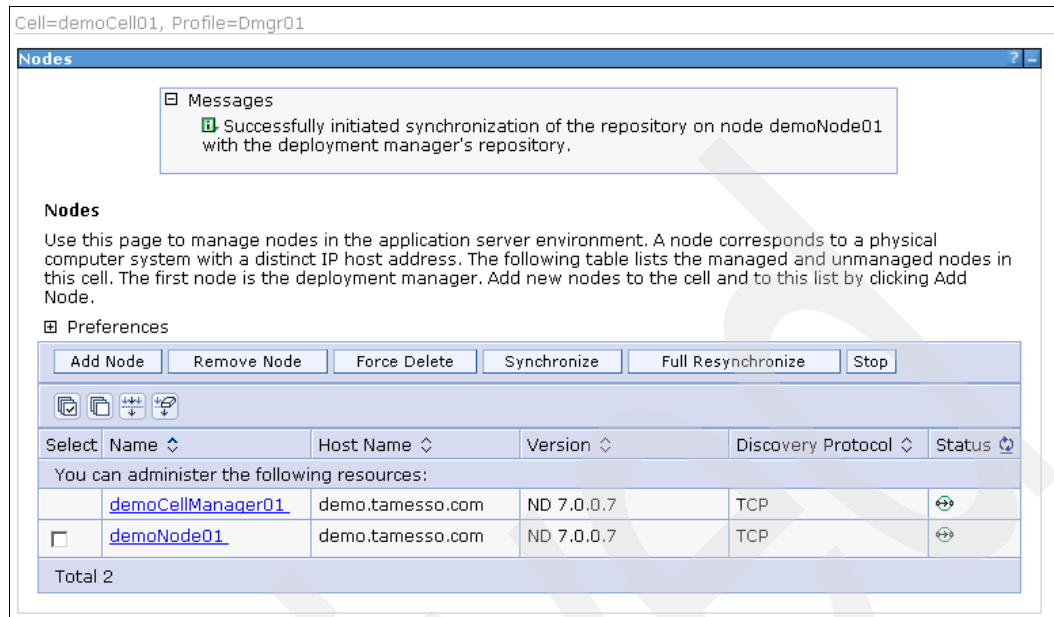


Figure 2-153 Success message

2.5.7 Setting up J2C authentication data

To set up J2C authentication data follow the steps below:

1. From the WebSphere ISC, click **Security** → **Global Security**.
2. Under Authentication, click **Java™ Authentication and Authorization Service**. Click the **J2C authentication data** link (Figure 2-154).

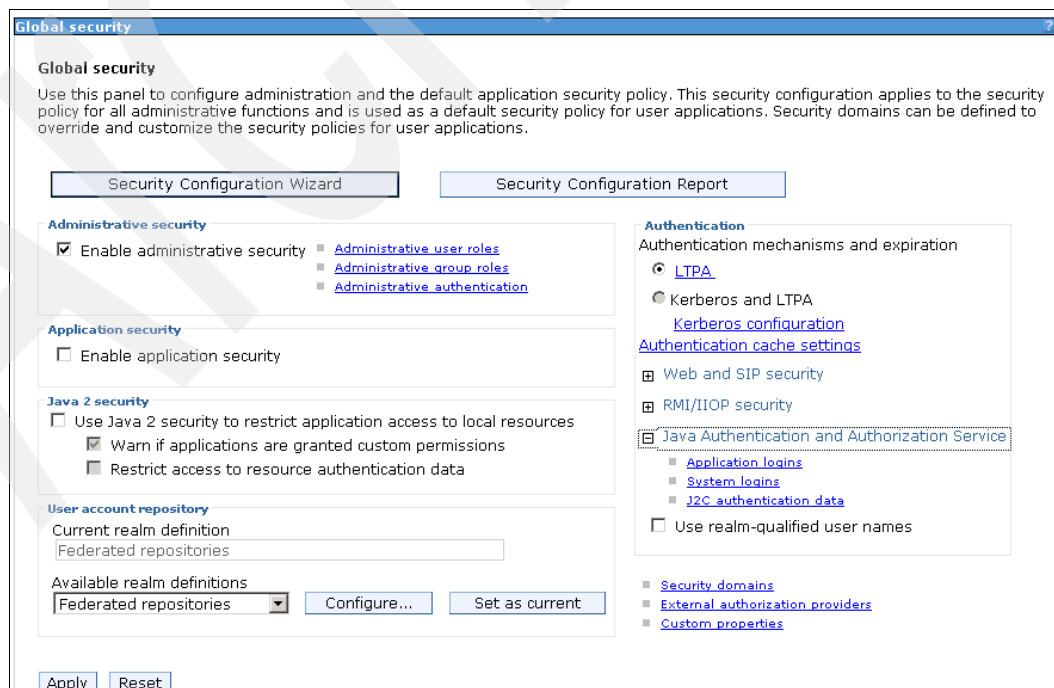


Figure 2-154 Global security

3. Uncheck the “Prefix new alias names with the node name of the cell” check box and click **Apply** (Figure 2-155).

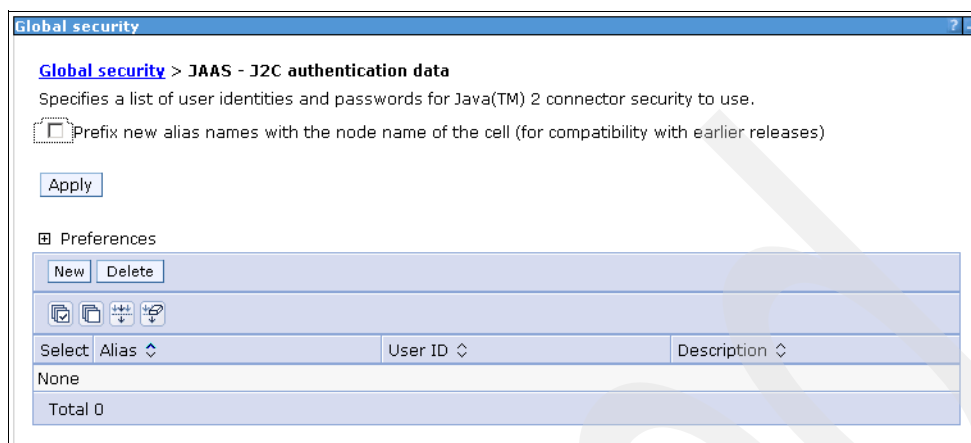


Figure 2-155 J2C authentication data

4. Click **Save** to save changes directly to the master configuration (Figure 2-156).

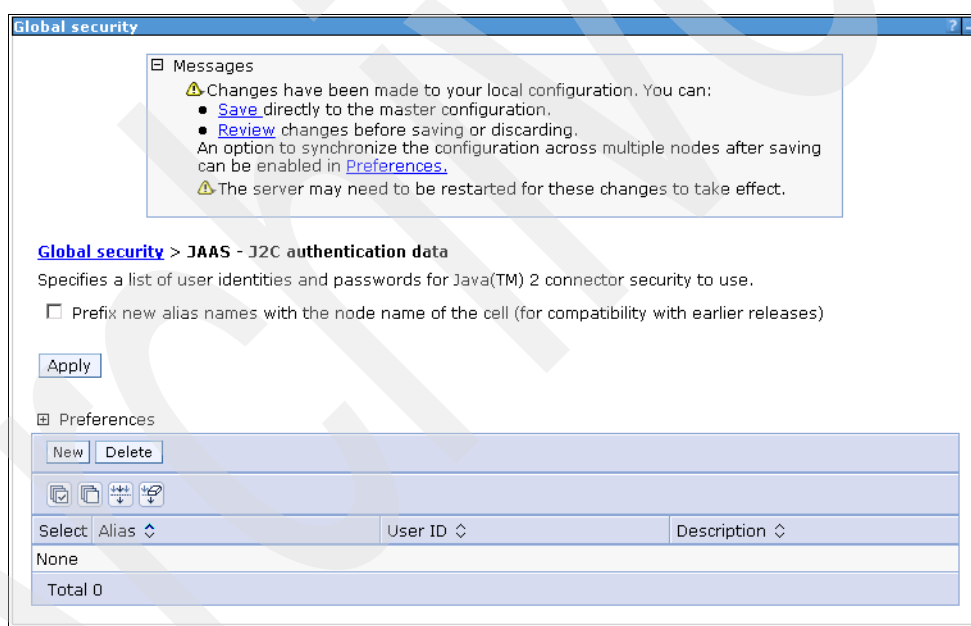


Figure 2-156 Message - Changes

5. From the WebSphere ISC, click **Security** → **Global Security**.
6. Under Authentication, click **Java Authentication and Authorization Service**. Click **J2C authentication data**.
7. Under Preferences, click **New**.

The general properties list displays (Figure 2-157).

Cell=demoCell01, Profile=Dmgr01

Global security

[Global security](#) > [JAAS - J2C authentication data](#) > New

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

General Properties

* Alias

* User ID

* Password

Description

Figure 2-157 General Properties list

- On the General Properties page (Figure 2-158), enter `imsauthdata` in the Alias field. Enter the database user ID and password in the User ID and Password fields (for example, `db2admin`). Click **OK**.

Global security

[Global security](#) > [JAAS - J2C authentication data](#) > New

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

General Properties

* Alias

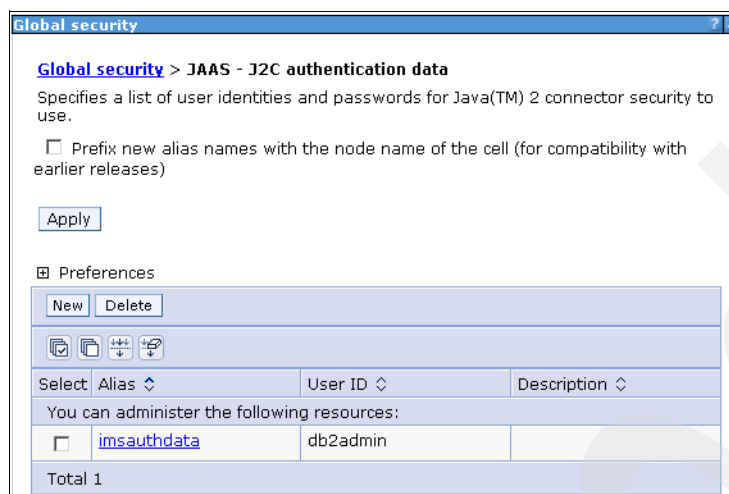
* User ID

* Password

Description

Figure 2-158 Enter user ID and password

9. Click **Save** to save changes to the master configuration (Figure 2-159).



Global security > **JAAS - J2C authentication data**

Specifies a list of user identities and passwords for Java(TM) 2 connector security to use.

☐ Prefix new alias names with the node name of the cell (for compatibility with earlier releases)

Apply

Preferences

New **Delete**

☐ ☐ ☐ ☐

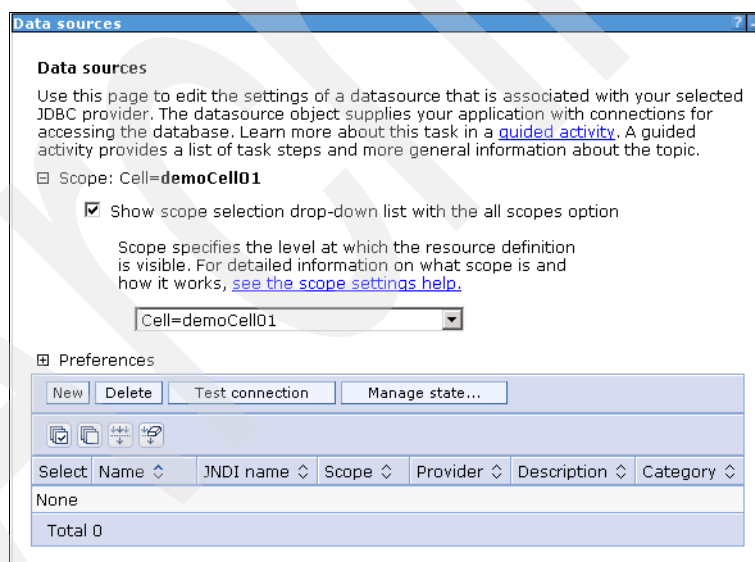
Select	Alias	User ID	Description
You can administer the following resources:			
<input type="checkbox"/>	imsauthdata	db2admin	
Total 1			

Figure 2-159 Save changes to master configuration

2.5.8 Creating data source for DB2 database

To create the data source for the DB2 database follow the steps below:

1. From the WebSphere ISC, click **Resources** → **JDBC** → **Data Sources**.
2. Select **cell scope** from the Scope list.
3. Under Preferences, click **New** to open the Create a data source page (Figure 2-160).



Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=**demoCell01**

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=demoCell01

Preferences

New **Delete** **Test connection** **Manage state...**

☐ ☐ ☐ ☐

Select	Name	JNDI name	Scope	Provider	Description	Category
None						
Total 0						

Figure 2-160 Data sources

Entering basic data source information

To do this:

1. Enter TAM E-SSO IMS Server Data Source for the Data Source Name field (Figure 2-161).
2. Enter jdbc/ims for the JNDI name field. Click **Next**.

The screenshot shows a window titled "Create a data source" with a blue header bar. Inside, there's a sidebar on the left with five steps: "Step 1: Enter basic data source information" (highlighted with a yellow arrow), "Step 2: Select JDBC provider", "Step 3: Enter database specific properties for the data source", "Step 4: Setup security aliases", and "Step 5: Summary". The main area is titled "Enter basic data source information" and contains a paragraph explaining the purpose of a datasource. Below this, there are three input fields: "Scope" with the value "cells:demoCell01", "* Data source name" with the value "TAM E-SSO IMS Server Data", and "* JNDI name" with the value "jdbc/ims". At the bottom, there are "Next" and "Cancel" buttons.

Create a data source

→ Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

Step 5: Summary

Enter basic data source information

Set the basic configuration values of a datasource for association with your JDBC provider. A datasource supplies the physical connections between the application server and the database.

Requirement: Use the Datasources (WebSphere(R) Application Server V4) console pages if your applications are based on the Enterprise JavaBeans(TM) (EJB) 1.0 specification or the Java (TM) Servlet 2.2 specification.

Scope
cells:demoCell01

* Data source name
TAM E-SSO IMS Server Data

* JNDI name
jdbc/ims

Next Cancel

Figure 2-161 Enter basic data source information

Creating a new JDBC Provider

To do this:

1. Select **DB2** as the database type (Figure 2-162).
2. Select **DB2 Universal JDBC Driver Provider** as the provider type.
3. Select **Connection pool data source** as the implementation type.
4. Enter **TAM E-SSO JDBC Provider** in the Name field. Click **Next**.

The screenshot shows a wizard window titled "Create a data source". On the left, a vertical pane lists five steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 2.1: Create new JDBC provider (highlighted with a yellow arrow), Step 2.2: Enter database class path information, Step 3: Enter database specific properties for the data source, Step 4: Setup security aliases, and Step 5: Summary. The main area is titled "Create new JDBC provider" and contains a text box for "Scope" with the value "cells:demoCell01". Below this are four required fields, each marked with an asterisk: "Database type" is a dropdown menu set to "DB2"; "Provider type" is a dropdown menu set to "DB2 Universal JDBC Driver Provider"; "Implementation type" is a dropdown menu set to "Connection pool data source"; and "Name" is a text field containing "TAM E-SSO JDBC Provider". Below these fields is a "Description" text area with the following text: "One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing." At the bottom of the window are three buttons: "Previous", "Next", and "Cancel".

Figure 2-162 Create new JDBC provider

Entering database class path information

Accept the default values and click **Next** (Figure 2-163).

The screenshot shows a wizard window titled "Create a data source". On the left is a vertical pane with five steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 2.1: Create new JDBC provider, Step 2.2: Enter database class path information (highlighted with a yellow arrow), Step 3: Enter database specific properties for the data source, Step 4: Setup security aliases, and Step 5: Summary. The main area is titled "Enter database class path information" and contains the following text: "Set the environment variables that represent the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays the file names; you supply only the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\java on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM). If a value is specified for you, you may click Next to accept the value." Below this is a "Class path:" label and a text area containing three lines of default values: "\${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar", "\${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar", and "\${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar". There is a "Directory location for 'db2jcc.jar, db2jcc_license_cisuz.jar' which is saved as WebSphere variable \${DB2UNIVERSAL_JDBC_DRIVER_PATH}" label and an empty text box. Below that is a "Native library path" label and a "Directory location which is saved as WebSphere variable \${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}" label with an empty text box. At the bottom are "Previous", "Next", and "Cancel" buttons.

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 2.1: Create new JDBC provider

→ Step 2.2: Enter database class path information

Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

Step 5: Summary

Enter database class path information

Set the environment variables that represent the JDBC driver class files, which WebSphere(R) Application Server uses to define your JDBC provider. This wizard page displays the file names; you supply only the directory locations of the files. Use complete directory paths when you type the JDBC driver file locations. For example: C:\SQLLIB\java on Windows(R) or /home/db2inst1/sqllib/java on Linux(TM).

If a value is specified for you, you may click Next to accept the value.

Class path:

`${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar`
`${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar`
`${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar`

Directory location for "db2jcc.jar, db2jcc_license_cisuz.jar" which is saved as WebSphere variable `${DB2UNIVERSAL_JDBC_DRIVER_PATH}`

Native library path

Directory location which is saved as WebSphere variable `${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}`

Previous Next Cancel

Figure 2-163 Enter database class path information

Entering database-specific properties for the data source

On the Enter database specific properties for the data source page (Figure 2-164):

1. Select **4** as the driver type from the values list.
2. Type **IMSDB** into the Database name field.
3. Specify the server name. (In our case, the server name is demo.)
4. Ensure that the port number is set to 50000.
5. Check the **Use this data source in container managed persistence (CMP)** check box. Click **Next**.

The screenshot shows a wizard window titled "Create a data source". On the left is a vertical pane with five steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 2.1: Create new JDBC provider, Step 2.2: Enter database class path information, and Step 3: Enter database specific properties for the data source (which is highlighted with a yellow arrow). Below Step 3 are Step 4: Setup security aliases and Step 5: Summary. The main area of the wizard is titled "Enter database specific properties for the data source" and contains the text: "Set these database-specific properties, which are required by the database vendor JDBC driver to support the connections that are managed through the datasource." Below this text is a table with two columns: "Name" and "Value". The table contains four rows: "Driver type" with a dropdown menu showing "4", "Database name" with a text field containing "IMSDB", "Server name" with a text field containing "demo", and "Port number" with a text field containing "50000". Below the table is a checkbox labeled "Use this data source in container managed persistence (CMP)" which is checked. At the bottom of the wizard are three buttons: "Previous", "Next", and "Cancel".

Name	Value
* Driver type	4
* Database name	IMSDB
* Server name	demo
* Port number	50000

☒ Use this data source in container managed persistence (CMP)

Previous Next Cancel

Figure 2-164 Enter database specific properties for the data source

Note: The above values are for the DB2 database only. Other databases require different settings. Check the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, for details.

Setting up security aliases

To do this:

1. On the Setup security aliases page (Figure 2-165), select **imsauthdata** from the Component-managed authentication alias drop-down menu.
2. Select **none** from the Mapping-configuration alias drop-down menu.
3. Select **none** from the Container-managed authentication alias drop-down menu.
Click **Next**.

The screenshot shows a wizard window titled "Create a data source". On the left is a vertical pane with five steps: Step 1: Enter basic data source information, Step 2: Select JDBC provider, Step 2.1: Create new JDBC provider, Step 2.2: Enter database class path information, Step 3: Enter database specific properties for the data source, and Step 4: Setup security aliases (which is highlighted with a yellow arrow). Step 5: Summary is at the bottom. The main area is titled "Setup security aliases" and contains the text "Select the authentication values for this resource." Below this are three drop-down menus: "Component-managed authentication alias" with "imsauthdata" selected, "Mapping-configuration alias" with "(none)" selected, and "Container-managed authentication alias" with "(none)" selected. A note states: "Note: You can create a new J2C authentication alias by accessing one of the following links. Clicking on a link will cancel the wizard and your current wizard selections will be lost." Below the note are two blue links: "Global J2C authentication alias" and "Security domains". At the bottom are three buttons: "Previous", "Next", and "Cancel".

Figure 2-165 Setup security aliases

Summary

In summary:

1. On the Summary page (Figure 2-166), review the settings and click **Finish**.

Create a data source

Create a data source

Step 1: Enter basic data source information

Step 2: Select JDBC provider

Step 2.1: Create new JDBC provider

Step 2.2: Enter database class path information

Step 3: Enter database specific properties for the data source

Step 4: Setup security aliases

→ Step 5: Summary

Summary

Summary of actions:

Options	Values
Scope	cells:demoCell01
Data source name	TAM E-SSO IMS Server Data
JNDI name	jdbc/ims
JDBC provider name	TAM E-SSO JDBC Provider
Description	One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing.
Class path	\${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar \${UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar \${DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
Native path	\${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}
Implementation class name	com.ibm.db2.jcc.DB2ConnectionPoolDataSource
Driver type	4
Database name	IMSDB
Server name	demo
Port number	50000
Use this data source in container managed persistence (CMP)	true
Component-managed authentication alias	imsauthdata
Mapping-configuration alias	(none)
Container-managed authentication alias	(none)

Previous

Finish

Cancel

Figure 2-166 Summary of actions

2. Click **Save** to save to the master configuration.

- The new data source that we created, Tivoli Access Manager for Enterprise Single Sign-On IMS Server Data Source, now displays under the list of data sources (Figure 2-167).

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=**demoCell01**

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=demoCell01

Preferences

New Delete Test connection Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	TAM E-SSO IMS Server Data Source	jdbc/ims	Cell=demoCell01	TAM E-SSO JDBC Provider	DB2 Universal Driver Datasource	

Total 1

Figure 2-167 Data sources

4. Click the **TAM E-SSO IMS Server Data Source** link.
5. Under Additional properties, click **Connection Pool properties** (Figure 2-168).
6. Enter 800 for maximum connections.
7. Enter 100 for minimum connections.
8. Retain the other default values.
9. Click **Apply**.

The screenshot shows a web-based configuration window titled "Data sources". The breadcrumb trail is "Data sources > TAM E-SSO IMS Server Data Source > Connection pools". Below the breadcrumb, there is a descriptive paragraph: "Use this page to set properties that impact the timing of connection management tasks, which can affect the performance of your application. Consider the default values carefully; your application requirements might warrant changing these values." The main content area is divided into two tabs: "Configuration" (selected) and "Advanced Properties". Under the "Configuration" tab, there are two sections: "General Properties" and "Additional Properties". The "General Properties" section contains several input fields with labels and units: "Scope" (text box with "cells:demoCell01"), "Connection timeout" (spinner with "180" and "seconds"), "Maximum connections" (spinner with "800" and "connections"), "Minimum connections" (spinner with "100" and "connections"), "Reap time" (spinner with "180" and "seconds"), "Unused timeout" (spinner with "1800" and "seconds"), and "Aged timeout" (spinner with "0" and "seconds"). There is also a "Purge policy" dropdown menu set to "EntirePool". The "Additional Properties" section is currently empty. At the bottom of the window, there are four buttons: "Apply", "OK", "Reset", and "Cancel".

Figure 2-168 Connection pools

10. Click **Save** to save to the master configuration.

Data sources

Use this page to edit the settings of a datasource that is associated with your selected JDBC provider. The datasource object supplies your application with connections for accessing the database. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

Scope: Cell=**demoCell01**

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

Cell=demoCell01

Preferences

New Delete Test connection Manage state...

Select	Name	JNDI name	Scope	Provider	Description	Category
<input type="checkbox"/>	TAM E-SSO IMS Server Data	jdbc/ims	Cell=demoCell01	TAM E-SSO JDBC Provider	DB2 Universal Driver Datasource	

Total 1

Figure 2-169 Save to the master configuration

Modifying JDBC provider details

To modify JDBC provider details, follow the steps below:

1. From the WebSphere ISC, click **Resources** → **JDBC** → **JDBC Provider**.
2. Under Preferences, click **TAM E-SSO JDBC Provider** (Figure 2-170).

Cell=demoCell01, Profile=Dmgr01

JDBC providers

Use this page to edit properties of a JDBC provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

☐ Scope: =All scopes

☒ Show scope selection drop-down list with the all scopes option

Scope specifies the level at which the resource definition is visible. For detailed information on what scope is and how it works, [see the scope settings help](#).

All scopes

☐ Preferences

New Delete

Select	Name	Scope	Description
You can administer the following resources:			
<input type="checkbox"/>	TAM E-SSO JDBC Provider	Cell=demoCell01	One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS and supports 2-phase commit processing.

Total 1

Figure 2-170 Click TAM E-SSO JDBC Provider

3. Under General Properties (Figure 2-171), replace the following class path data:

```
{DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc.jar  
{UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cu.jar  
{DB2UNIVERSAL_JDBC_DRIVER_PATH}/db2jcc_license_cisuz.jar
```

with:

E:/Program Files/IBM/WebSphere/AppServer/profiles/Dmgr01/config/tamesso/lib/db2jcc.jar

Click **OK**. Click **Save**.

JDBC providers > TAM E-SSO JDBC Provider

Use this page to edit properties of a Java Database Connectivity (JDBC) provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment.

Configuration

General Properties

* Scope
cells:demoCell01

* Name
TAM E-SSO JDBC Provider

Description
One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS

Class path
E:/Program Files/IBM/WebSphere/AppServer/profiles/Dmgr01/config/tamesso/lib/db2jcc.jar

Native library path
{DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}

☐ Isolate this resource provider

* Implementation class name
com.ibm.db2.jcc.DB2ConnectionPoolDataSource

Apply OK Reset Cancel

Additional Properties

Data sources
Data sources (WebSphere Application Server v4)

Figure 2-171 TAM E-SSO JDBC Provider

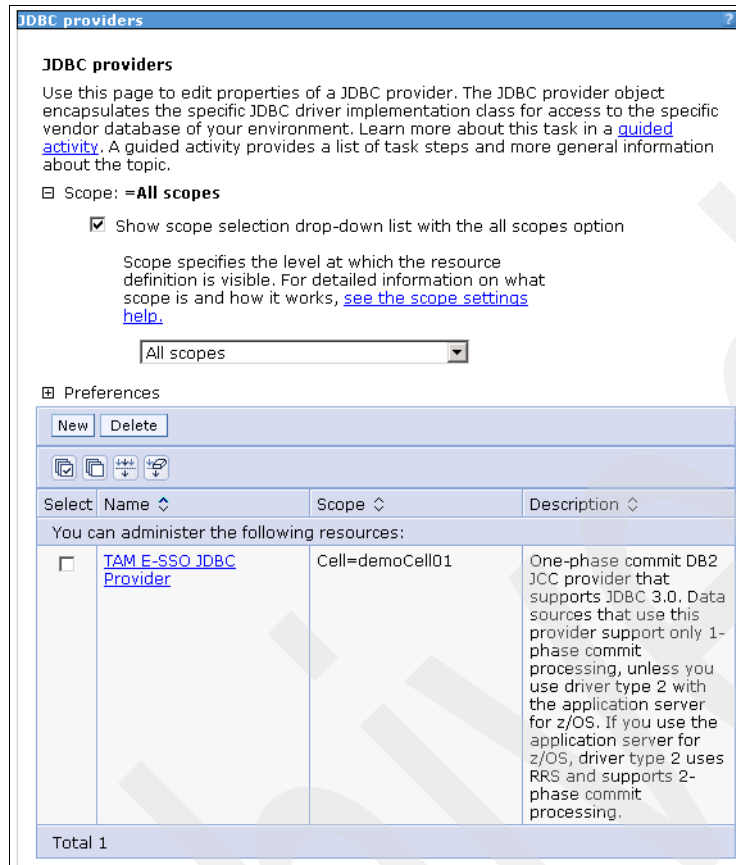


Figure 2-172 JDBCs Providers

Testing data source connection

To test the data source connection, follow the steps below:

1. From the WebSphere ISC, click **Resources** → **JDBCs** → **Data Sources**.
2. Under Preferences, select the **TAM E-SSO IMS Server Data Source** check box. Click **Test connection** (Figure 2-173).

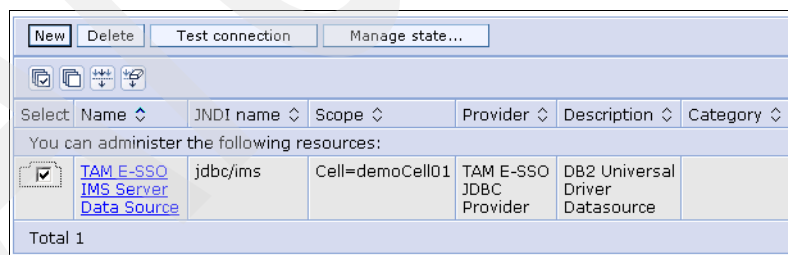


Figure 2-173 Test connection

3. Verify that the test connection was successful (Figure 2-174).

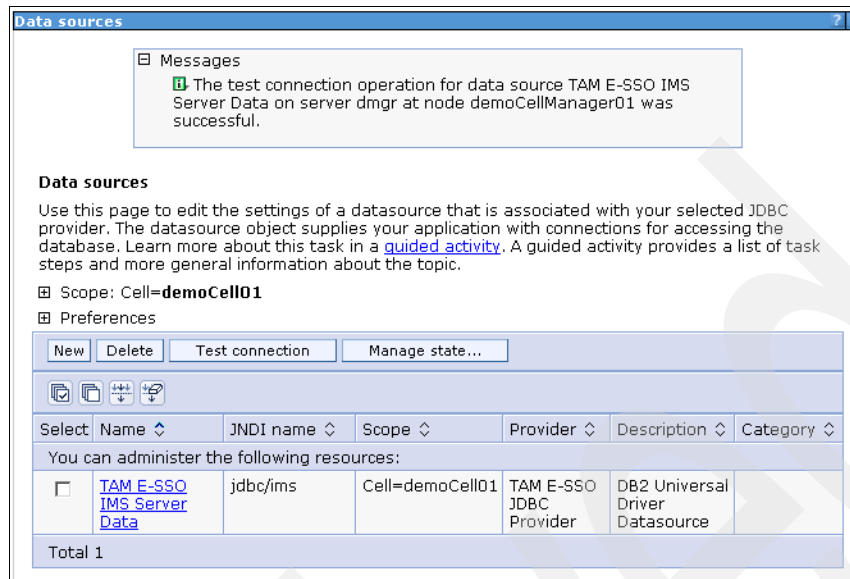


Figure 2-174 Success message

Replacing ClassPath with generic directory

To replace the ClassPath with a generic directory, follow the steps below:

1. From the WebSphere ISC, click **Resources** → **JDBC** → **JDBC Providers** → **TAM E-SSO JDBC Provider** (Figure 2-175).

[JDBC providers](#) > **TAM E-SSO JDBC Provider**

Use this page to edit properties of a Java Database Connectivity (JDBC) provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment.

Configuration

General Properties	Additional Properties
<p>* Scope cells:demoCell01</p> <p>Name TAM E-SSO JDBC Provider</p> <p>Description One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS</p> <p>Class path E:/Program Files/IBM/WebSphere/AppServer/profiles/Dmgr01/config/tamesso/lib/db2jcc.jar</p> <p>Native library path \${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}</p> <p><input type="checkbox"/> Isolate this resource provider</p> <p>* Implementation class name com.ibm.db2.jcc.DB2ConnectionPoolDataSource</p> <p>Apply OK Reset Cancel</p>	<ul style="list-style-type: none">■ Data sources■ Data sources (WebSphere Application Server V4)

Figure 2-175 TAM E-SSO JDBC Provider

2. In the Configuration tab (Figure 2-176), replace the class path to make the path independent of the WebSphere Application Server installation.
3. For DB2, set the CLASSPATH to `${USER_INSTALL_ROOT}/config/tamesso/lib/db2jcc.jar`. Click **OK**.

JDBC providers > TAM E-SSO JDBC Provider

Use this page to edit properties of a Java Database Connectivity (JDBC) provider. The JDBC provider object encapsulates the specific JDBC driver implementation class for access to the specific vendor database of your environment.

Configuration

General Properties	Additional Properties
<p>* Scope cells:demoCell01</p> <p>* Name TAM E-SSO JDBC Provider</p> <p>Description One-phase commit DB2 JCC provider that supports JDBC 3.0. Data sources that use this provider support only 1-phase commit processing, unless you use driver type 2 with the application server for z/OS. If you use the application server for z/OS, driver type 2 uses RRS</p> <p>Class path \${USER_INSTALL_ROOT}/config/tamesso/lib/db2jcc.jar</p> <p>Native library path \${DB2UNIVERSAL_JDBC_DRIVER_NATIVEPATH}</p> <p><input type="checkbox"/> Isolate this resource provider</p> <p>* Implementation class name com.ibm.db2.jcc.DB2ConnectionPoolDataSource</p>	<p>■ Data sources</p> <p>■ Data sources (WebSphere Application Server V4)</p>

Apply OK Reset Cancel

Figure 2-176 Settings

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

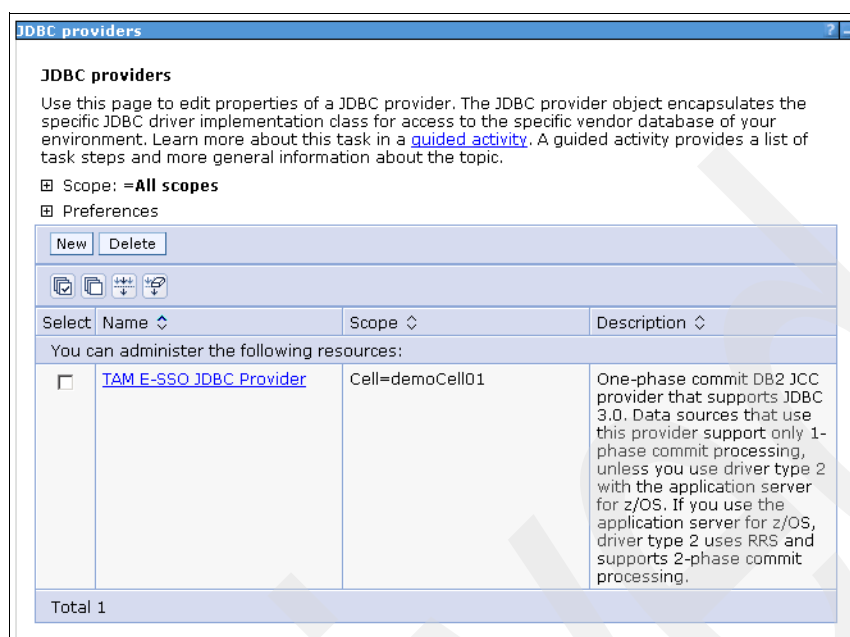


Figure 2-177 JDBC Providers

Synchronizing the nodes

Perform full synchronization of the nodes (Figure 2-178):

1. From the WebSphere ISC, click **System administration** → **Nodes**. Select nodes and click **Full Resynchronize**.

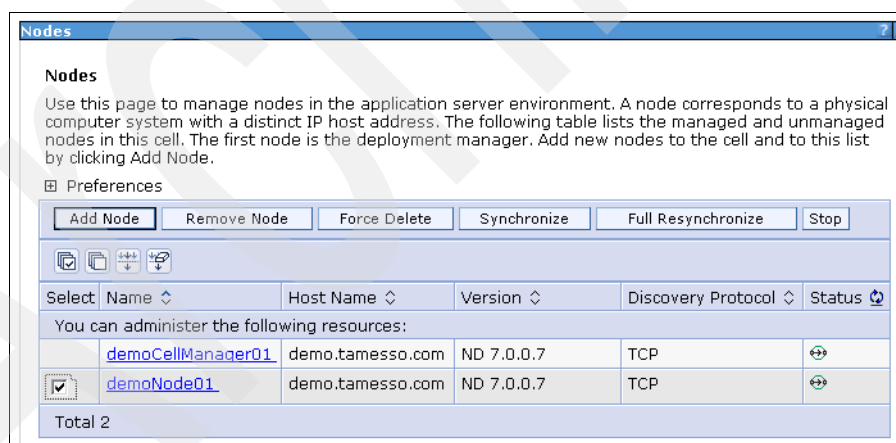


Figure 2-178 Configuration changes

2. Verify that the synchronization was successfully initiated (Figure 2-179).

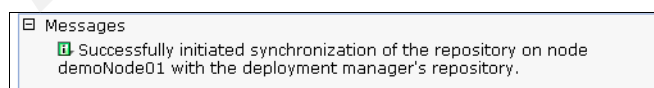


Figure 2-179 Success message

Restarting the cluster

To restart the cluster, follow the steps below:

1. From the WebSphere ISC, click **Servers** → **Clusters** → **WebSphere application server clusters**. Select the **cluster1** checkbox and click **Stop**. Once the cluster has been successfully stopped, select the **cluster1** checkbox again for and click **Start** (Figure 2-180).

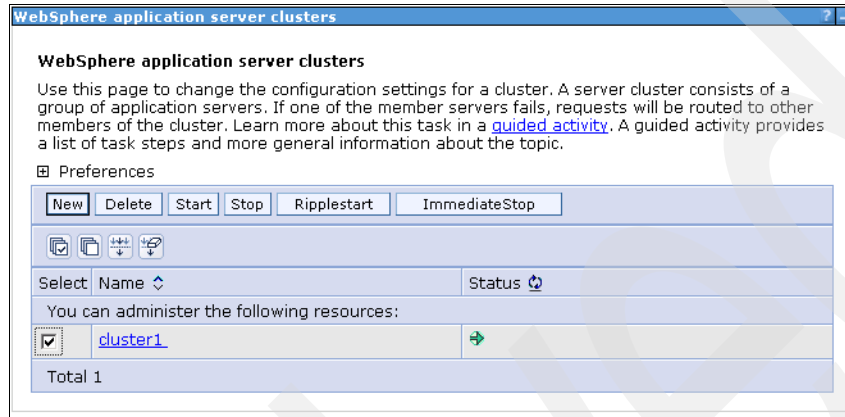


Figure 2-180 WebSphere application server clusters

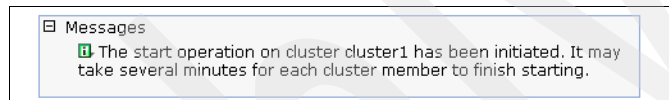


Figure 2-181 Initiation message

2. Verify that the cluster is started (Figure 2-182).



Figure 2-182 Cluster start verification

Starting the IMS Server

From the WebSphere ISC, follow the steps below:

1. Start the Tivoli Access Manager for Enterprise Single Sign-On IMS Server (Figure 2-183).

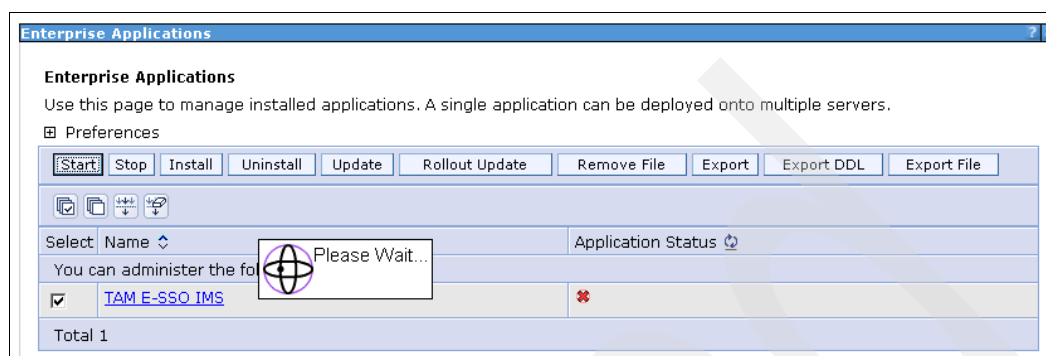


Figure 2-183 Start Tivoli Access Manager for Enterprise Single Sign-On IMS Server

2. Verify that the server is started successfully (Figure 2-184).

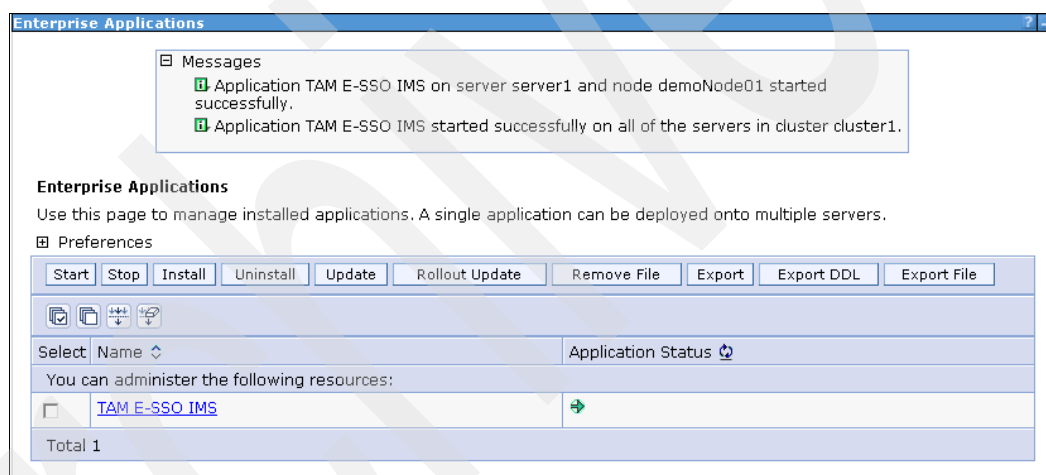


Figure 2-184 Success message

2.6 Configuration for IBM HTTP Server

The following steps guide you to set up the IBM HTTP Server to work with the WebSphere Application Server. Before you begin, ensure that:

- ▶ The WebSphere Application server is installed and running.
- ▶ The IMS Server is successfully installed.
- ▶ Both the IBM HTTP Server and the IBM HTTP Administration Server are running.
- ▶ You have an administrator ID and password for the HTTP Server.
- ▶ Ports 80 and 443 are available (and not being used by another application like IIS).

2.6.1 Running the configurewebserver script

The <Webservername>.bat file is created during the IHS installation and configuration steps carried out earlier. We use this bat file to configure a web server to be managed within the WebSphere ISC.

1. Copy the configurewebserver1.bat file from the <IHS install directory> to the <WAS Install Directory>\bin (for example, from E:\Program Files\IBM\HTTPServer\Plugins\bin to E:\Program Files\IBM\WebSphere\AppServer\bin).
2. Run configure<web server name>.bat from the command prompt, and pass arguments of the profileName, the WebSphere Application Server administration user and password (Figure 2-185). For example, from the E:\Program Files\IBM\WebSphere\AppServer\bin directory, run the following command:

```
configurewebserver1.bat -profileName Dmgr01 -user wasadmin -password p@ssw0rd
```

```
C:\WINDOWS\system32\cmd.exe - configurewebserver1.bat -profileName Dmgr01 -user wasadmin -p...
E:\Program Files\IBM\WebSphere\AppServer\bin>configurewebserver1.bat -profileName
e Dmgr01 -user wasadmin -password p@ssw0rd
Using the profile Dmgr01
Using WebSphere admin userID wasadmin
WASX72091: Connected to process "dmgr" on node demoCellManager01 using SOAP conn
ector; The type of process is: DeploymentManager
WASX8011W: AdminTask object is not available.
WASX73031: The following options are passed to the scripting environment and are
available as arguments that are stored in the argv variable: "webserver1, IHS,
E:\Program Files\IBM\HTTPServer, E:\Program Files\IBM\HTTPServer\conf\h
ttpd.conf, 80, MAP_ALL, E:\Program Files\IBM\HTTPServer\Plugins, unmanaged,
demo.tamesso.com-node, demo.tamesso.com, windows, 8008, httpadmin1"

Input parameters:
Web server name - webserver1
Web server type - IHS
Web server install location - E:\Program Files\IBM\HTTPServer
Web server config location - E:\Program Files\IBM\HTTPServer\conf\httpd.conf

Web server port - 80
Map Applications - MAP_ALL
Plugin install location - E:\Program Files\IBM\HTTPServer\Plugins
Web server node type - unmanaged
Web server node name - demo.tamesso.com-node
Web server host name - demo.tamesso.com
Web server operating system - windows
IHS Admin port - 8008
IHS Admin user ID - httpadmin
IHS Admin password - ""
IHS service name - ""

Web server node definition demoNode01 already exists.
The template version of the web server node is not computed, exception = can't r
ead "AdminTask": no such variable
Web server definition for webserver1 already exists.
Start computing the plugin properties ID.
Plugin properties ID is not computed, exception = com.ibm.ws.scripting.Scripting
Exception: com.ibm.websphere.management.exception.ConfigServiceException
com.ibm.websphere.management.exception.ConnectorException
org.apache.soap.SOAPException: [SOAPException: faultCode=SOAP-ENV:Client; msg=Re
ad timed out; targetException=java.net.SocketTimeoutException: Read timed out]

Start updating the plugin install location.
Plugin install location is not updated, exception = can't read "webserverPluginP
ropertiesID": no such variable
Start updating the plugin log file location.
Plugin log file location is not updated, exception = can't read "webserverPlugin
PropertiesID": no such variable
Start updating the RemoteConfigFilename location.
Plugin remote config file location is not updated, exception = can't read "webs
erverPluginPropertiesID": no such variable
Start updating the RemoteKeyRingFileName location.
Plugin remote keyring file location is not updated, exception = can't read "webs
erverPluginPropertiesID": no such variable
Start saving the configuration.
█
```

Figure 2-185 Running configurewebserver1.bat

3. Exit the command prompt when you see the message Configuration save is completed.

Note: If you want to configure multiple HTTP Servers to the IMS Server, you must specify a unique web server definition name during the IBM HTTP Server/IBM HTTP Server Plug-In installation (for example, webserver1, webserver2).

If you have multiple web servers installed, repeat the above steps for each configure<webservername>.bat file.

2.6.2 Setting up SSL certificates

Create a certificate signed by the WebSphere Application Server CA. This uses the IBM HTTP Server name as the common name (cn) for communication between the client and the HTTP Server.

Deleting the default certificate

From the WebSphere ISC, follow the steps below:

1. Click **SSL certificate and key management** → **Key stores and certificates** → **CMSKeyStore** → **Personal certificates** (Figure 2-186).

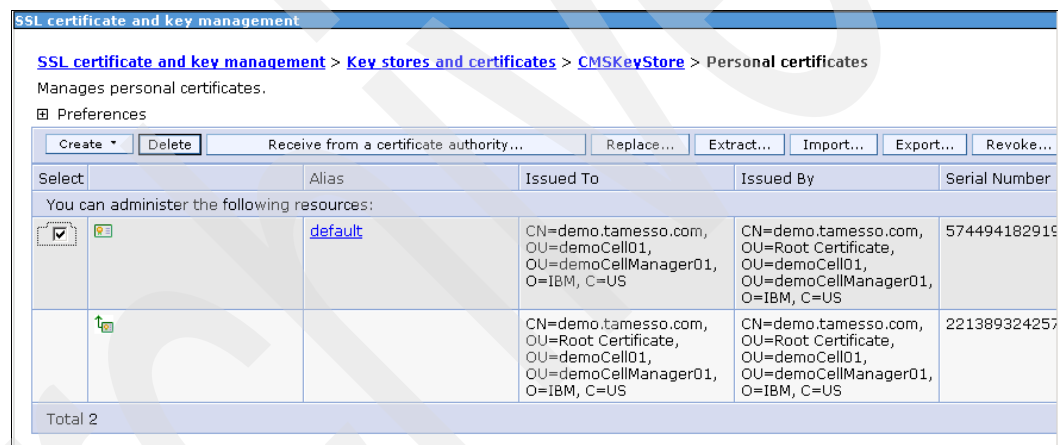


Figure 2-186 Delete default certificate

2. Select the **default** certificate.
3. Click **Delete**.
4. Click **Save** to save the changes to the master configuration.

Creating chained certificate

To create a chained certificate, follow the steps below:

1. Click **Create** → **Chained certificate** and navigate to **SSL certificate and Key management** → **Key stores and certificates** → **CMSKeyStore** → **Personal certificate** → **New**.
2. In the General Properties dialog (Figure 2-187), specify a name for the alias (for example, default) and provide the fully qualified host name for the HTTP Server for the common name (for example, demo.tamesso.com).

SSL certificate and key management > Key stores and certificates > CMSKeyStore > Personal certificates > New

A chained personal certificate is a personal certificate that is created using another certificate's private key to sign it.

General Properties

* Alias
default

Root certificate used to sign the certificate
root

Key size
1024 bits

* Common name
demo.tamesso.com

* Validity period
365 days

Organization
IBM

Organization unit

Locality

State/Province
TX

Zip code

Country or region
US

Apply OK Reset Cancel

Figure 2-187 Setting properties

Note that if you have multiple load balancers set up, specify the fully qualified name of the load balancer here.

3. Enter the other information as necessary (organization, state, and so on). Click **OK**.
4. Save the configuration changes.

5. Verify that the new certificate is listed in the Personal certificates section (Figure 2-188).

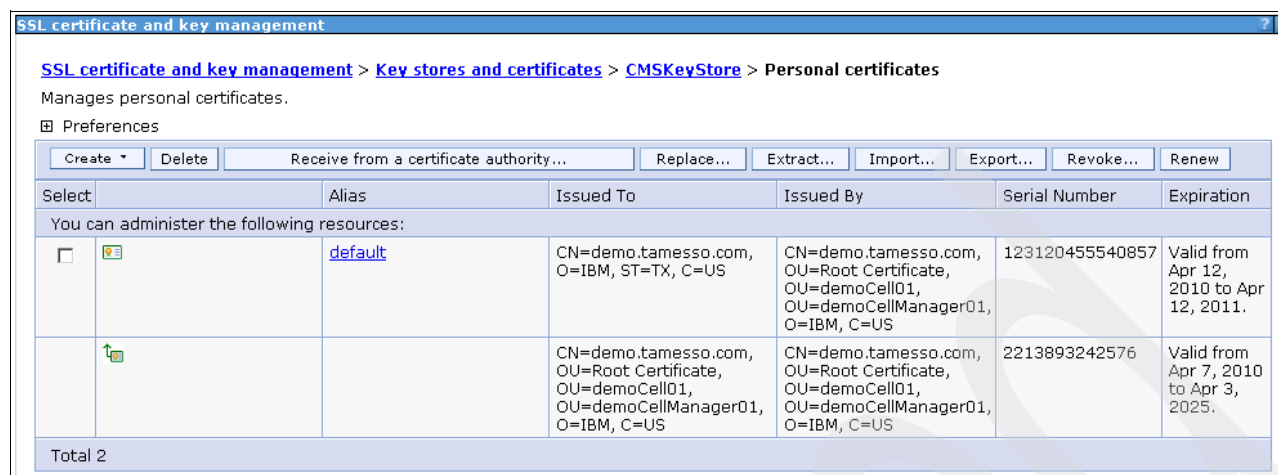


Figure 2-188 Personal certificates section

Note: The above steps need to be performed for each of the IBM HTTP Servers.

Synchronizing WebSphere Application Server keystore

We need to synchronize the WebSphere Application Server keystore with the IBM HTTP Server keystore so that the HTTP plug-in works successfully. First, verify that the IBM HTTP Server is started and running:

1. From the WebSphere ISC, click **Servers** → **Server Types** → **Web Servers**.
2. Select **webserver1**.
3. Select **Additional Properties** → **Plug-In Properties**.

4. Click **Copy to Web server key store directory** (Figure 2-189).

The screenshot shows the 'Configuration' tab of a 'Plug-in properties' dialog. The 'Repository copy of Web server plug-in files' section is expanded, showing the following configuration:

- ☐ Ignore DNS failures during Web server startup
- * Refresh configuration interval: 60 seconds
- * Plug-in configuration file name: plugin-cfg.xml (with a 'View' button)
- ☒ Automatically generate the plug-in configuration file
- ☒ Automatically propagate plug-in configuration file
- * Plug-in key store file name: plugin-key.kdb
- Buttons: 'Manage keys and certificates' and 'Copy to Web server key store directory' (highlighted)

The 'Web server copy of Web server plug-in files' section shows:

- * Plug-in configuration directory and file name: E:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-cfg.xml
- * Plug-in key store directory and file name: E:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb

The 'Plug-in logging' section shows:

- * Log file name: E:\Program Files\IBM\HTTPServer\Plugins\logs\webserver1\http_plugin.log
- Log level: Error (dropdown menu)

Figure 2-189 Copy to web server key store directory

Click **OK** (Figure 2-190).

Runtime Configuration

Plug-in properties

☐ Ignore DNS failures during Web server startup

* Refresh configuration interval
60 seconds

Repository copy of Web server plug-in files:

* Plug-in configuration file name
plugin-cfg.xml View

☒ Automatically generate the plug-in configuration file

☒ Automatically propagate plug-in configuration file

* Plug-in key store file name
plugin-key.kdb

Manage keys and certificates

Copy to Web server key store directory

Web server copy of Web server plug-in files:

* Plug-in configuration directory and file name
E:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-cfg.xml

* Plug-in key store directory and file name
E:\Program Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb

Plug-in logging:

* Log file name
E:\Program Files\IBM\HTTPServer\Plugins\logs\webserver1\http_plugin.log

Log level
Error

Apply OK Reset Cancel

Figure 2-190 Configuration tab

5. Click **Save** in the message box that appears at the top of the page to save changes to the master configuration.

Note: The above steps must be performed for each IBM HTTP Server.

2.6.3 Enabling SSL on the HTTP Server

By default, SSL communication is disabled. We enable SSL on the HTTP server by editing the `httpd.conf` file so that the IMS Server communication is encrypted.

Note: This must be performed for each IBM HTTP Server.

1. From the WebSphere ISC, click **Servers** → **Server Types** → **Web Servers**.
2. Under Web Servers, click **webserver1**.

3. Under Additional Properties, click **Configuration File** (Figure 2-191).

Web servers > webserver1
Use this page to configure a Web server that provides HTTP and HTTPS support to application servers.

Runtime **Configuration**

General Properties

Web server name
webserver1

Type
IBM HTTP Server

* Port
80

* Web server installation location
E:/Program Files/IBM/HTTPServer

* Configuration file name
\${WEB_INSTALL_ROOT}/conf/httpd.conf [Edit](#)

* Service name
IBMHTTPServer7.0

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

Configuration settings

- [Web Server Virtual Hosts](#)
- [Global Directives](#)

Additional Properties

- [Log file](#)
- [Configuration File](#)
- [Process definition](#)
- [Plug-in properties](#)
- [Custom properties](#)
- [Ports](#)

Figure 2-191 Configuration tab

4. Add the following lines of configuration to the end of the configuration file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
# Listen [::]:443
<VirtualHost *:443>
    SSLEnable
    SSLProtocolDisable SSLv2
    SSLServerCert <alias of the IBM HTTP Server SSL certificate>
</VirtualHost>
KeyFile "<absolute path of the plugin-key.kdb>"
SSLDisable
```

For example:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
Listen 0.0.0.0:443
## IPv6 support:
# Listen [::]:443
<VirtualHost *:443>
    SSLEnable
    SSLProtocolDisable SSLv2
    SSLServerCert default
</VirtualHost>
KeyFile "E:\Program
Files\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb"
SSLDisable
```

5. Click **Apply**.
6. Click **OK**.
7. Select **General Properties** → **Apply**.

- Click **Save** in the messages box at the top of the page (Figure 2-192).

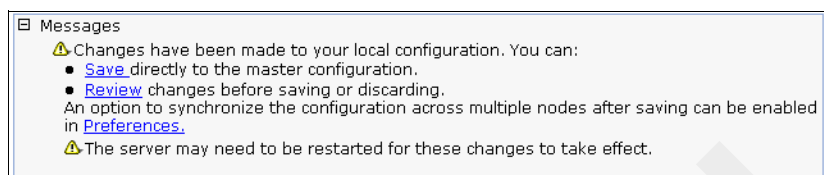


Figure 2-192 Change message

Note: The above steps must be performed for each IBM HTTP Server.

Restarting IBM HTTP Server

From the WebSphere ISC, follow the steps below:

- Click **Servers** → **Server Types** → **Web Servers**.
- Select the check box for webserver (webserver1).
- Click **Propagate Plug-in** (Figure 2-193).

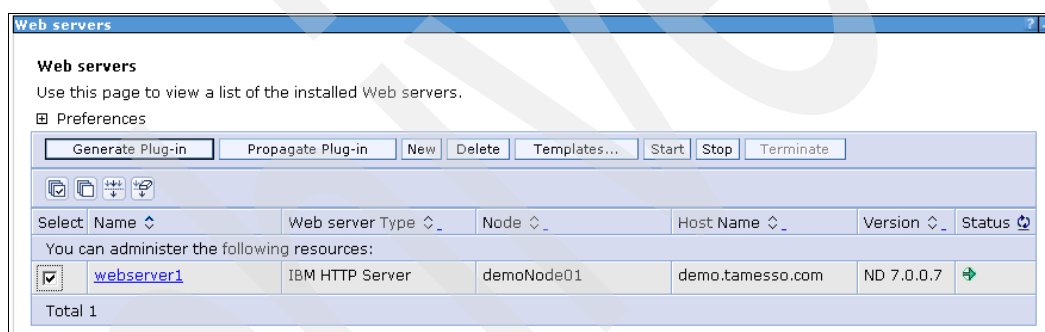


Figure 2-193 Select webserver

- Verify that the plug-in configuration file has been successfully propagated (Figure 2-194).

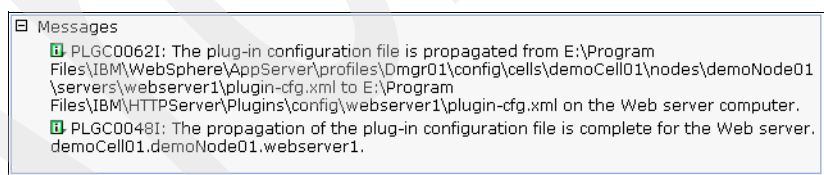


Figure 2-194 Success message

- Select the check box for the webserver (webserver1).
- Click **Stop** to stop the server.
- Select the check box for the webserver (webserver1).

8. Click **Start** to start the server (Figure 2-195).

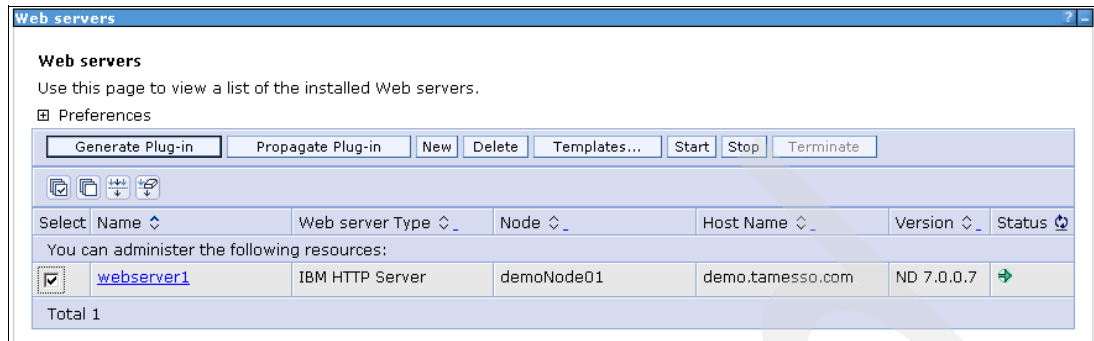


Figure 2-195 Starting the server

Configuring the IMS Server

This section details how to properly configure the IMS Server.

Starting the IMS Server

If the IMS Server is not already started:

1. Start it via the WebSphere ISC (Figure 2-196).

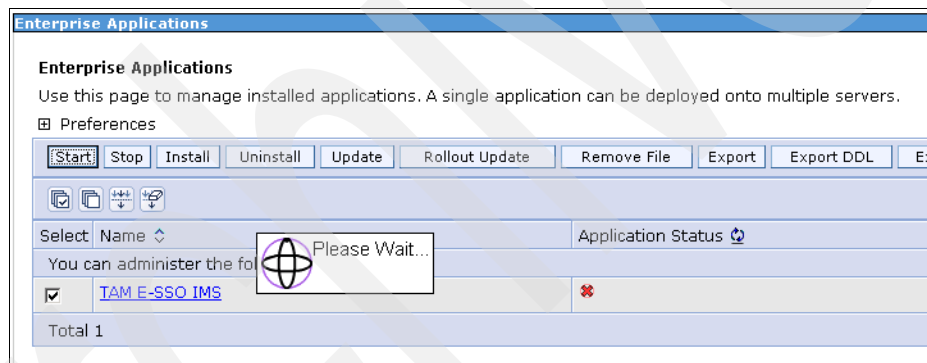


Figure 2-196 Enterprise Applications

2. Verify that the server is started successfully (Figure 2-197).

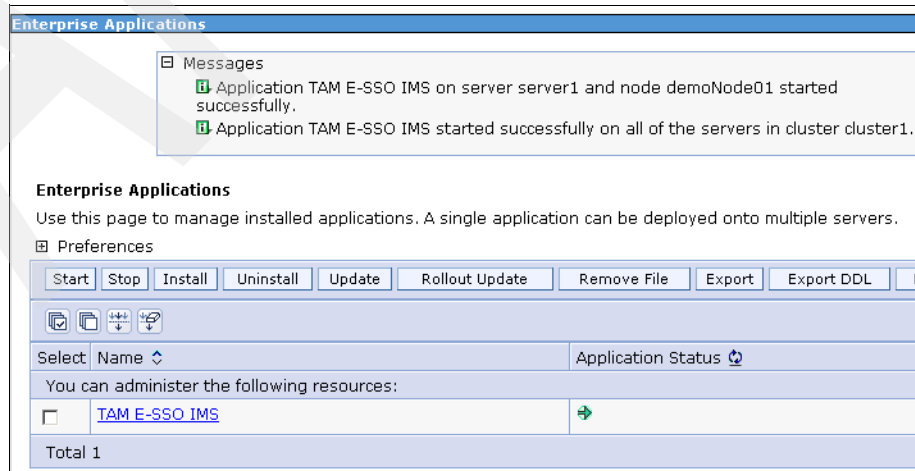


Figure 2-197 Success message

Running the IMS configuration

To do this:

1. Access the following URL:

`https://<fully qualified hostname>:9443/ims`

For example:

`https://demo.tamesso.com:9443/ims`

2. Accept the default setting (do not import the configuration from the old IMS installation), and click **Begin** (Figure 2-198).

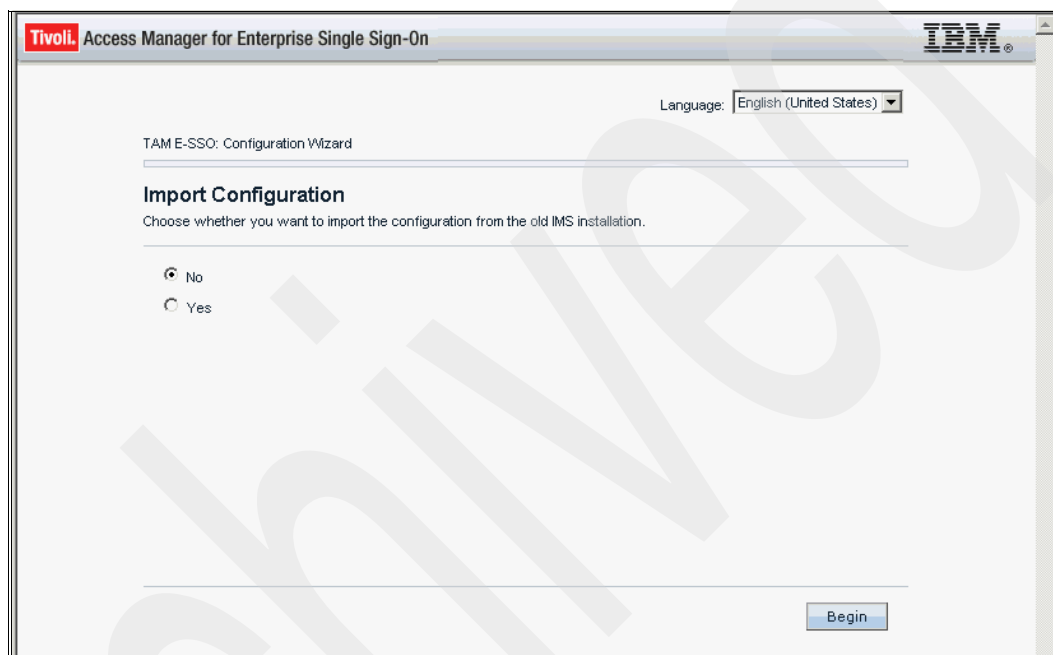


Figure 2-198 Import Configuration

3. Select the Create IMS Server database schema check box and click **Next** (Figure 2-199).

The screenshot shows a web-based configuration wizard titled 'TAM E-SSO: Configuration Wizard' with the IBM logo in the top right. A language dropdown menu is set to 'English (United States)'. The main heading is 'Create IMS Database Schema', followed by the instruction 'Mark the checkbox to use this wizard to create the IMS Server database schema.' Below this, there is a checkbox labeled 'Create IMS Server database schema.' which is checked. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

Figure 2-199 Create IMS Database Schema

4. Select **DB2 Server** as the database type and click **Next** (Figure 2-200).

The screenshot shows the next step in the wizard, titled 'Choose Database Type', with the instruction 'Choose the database type the IMS Server will use.' There are three radio button options: 'DB2 Server' (which is selected), 'Microsoft SQL Server', and 'Oracle Server'. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next'.

Figure 2-200 Choose Database Type

5. Enter/verify the database configuration information. Click **Next** (Figure 2-201).

The screenshot shows the 'Database Configuration - DB2' screen of the Tivoli Access Manager for Enterprise Single Sign-On configuration wizard. The window title is 'Tivoli Access Manager for Enterprise Single Sign-On' with the IBM logo. A language dropdown is set to 'English (United States)'. The wizard progress bar is at the 'Database Configuration - DB2' step. The instructions state: 'Provide the database configuration information.' The form contains the following fields: 'Host Name' with value 'demo.tamesso.com', 'Port' with value '50000', 'Database Name' with value 'imscdb', 'User Name' with value 'db2admin', and 'User Password' with masked characters '*****'. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

Figure 2-201 Database Configuration - DB2

6. Enter CellDefaultKeyStore for the keystore name, enter WebAS as the keystore password, and enter root for the root CA alias name. Click **Next** (Figure 2-202).

The screenshot shows the 'Provide Root CA Details' screen of the Tivoli Access Manager for Enterprise Single Sign-On configuration wizard. The window title is 'Tivoli Access Manager for Enterprise Single Sign-On' with the IBM logo. A language dropdown is set to 'English (United States)'. The wizard progress bar is at the 'Provide Root CA Details' step. The instructions state: 'Enter the keystore name, password, and certificate alias of the root CA that will be used to sign the IMS Server intermediate CA.' The form contains the following fields: 'Keystore name' with value 'CellDefaultKeyStore', 'Keystore password' with masked characters '*****', and 'Root CA alias name' with value 'root'. At the bottom are 'Cancel', 'Back', and 'Next' buttons.

Figure 2-202 Provide Root CA Details

7. On the Configure IMS services URL page (Figure 2-203), enter the fully qualified server name for the HTTP Server, enter 443 for the HTTPS port number, and click **Next**.

The screenshot shows the 'Configure IMS services URL' page of the Tivoli Access Manager for Enterprise Single Sign-On configuration wizard. The page title is 'TAM E-SSO: Configuration Wizard'. A progress bar is visible. The language is set to 'English (United States)'. The page instructs the user that the IMS Server services URL is required for AccessAssistant to connect to the IMS Server. There are two input fields: 'Fully qualified web server name' with the value 'demo.tamesso.com' and 'HTTPS port number' with the value '443'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.

Figure 2-203 Configure IMS services URL

8. On the Confirm settings page (Figure 2-204), verify the settings and click **Save**.

The screenshot shows the 'Confirm settings' page of the Tivoli Access Manager for Enterprise Single Sign-On configuration wizard. The page title is 'TAM E-SSO: Configuration Wizard'. A progress bar is visible. The language is set to 'English (United States)'. The page instructs the user that the following settings will be applied and to confirm the settings before proceeding to the next step. If the settings are correct, the user should click 'Save'. There are two sections with green checkmarks: 'Provide Root CA Details' with sub-items 'Keystore name: CellDefaultKeyStore' and 'Root CA alias name: root', and 'Configure IMS services URL' with sub-items 'Fully qualified web server name: demo.tamesso.com' and 'HTTPS port number: 443'. At the bottom, there are 'Cancel', 'Back', and 'Save' buttons.

Figure 2-204 Confirm settings

9. Wait for the process to complete (Figure 2-205).

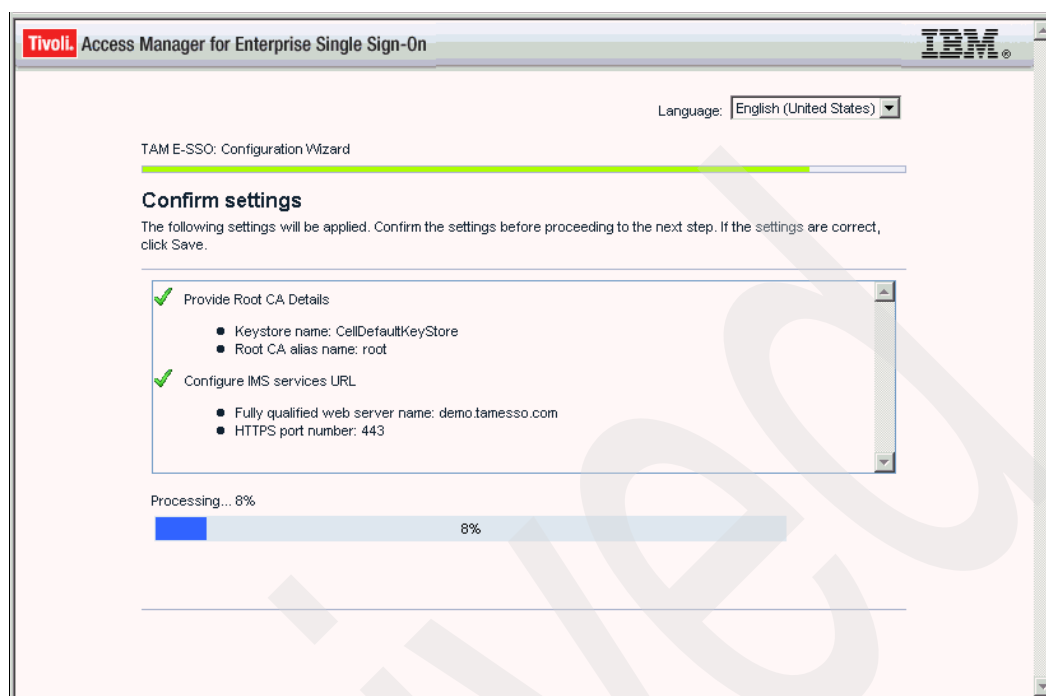


Figure 2-205 Confirm settings

Deleting root certificate from CellDefaultKeyStore

To do this:

1. From the WebSphere ISC, click **Security** → **SSL Certificate and Key Management**.
2. Under Related Items, click **Key stores and certificates**.
3. Click **CellDefaultKeyStore**.
4. Under Additional Properties, select **Personal Certificates**.
5. Select the check box of the root certificate to be deleted.
6. Click **Delete**.
7. Click **Save** to save to the master configuration.

Synchronizing all managed nodes

To do this:

1. Go to **System Administration** → **Nodes**.
2. Select all the nodes and click **Full resynchronize** (Figure 2-206).

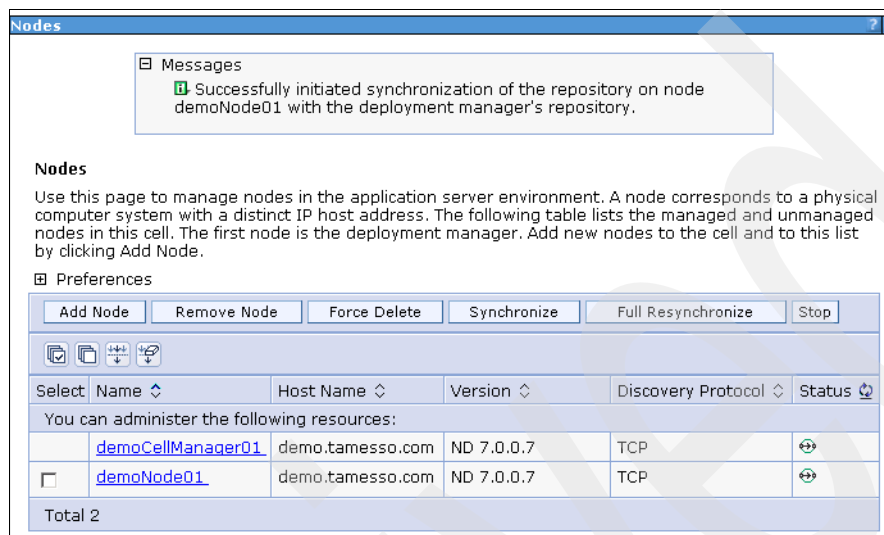


Figure 2-206 Success message

Restarting the WebSphere cluster

Restart the WebSphere Cluster (Figure 2-207).

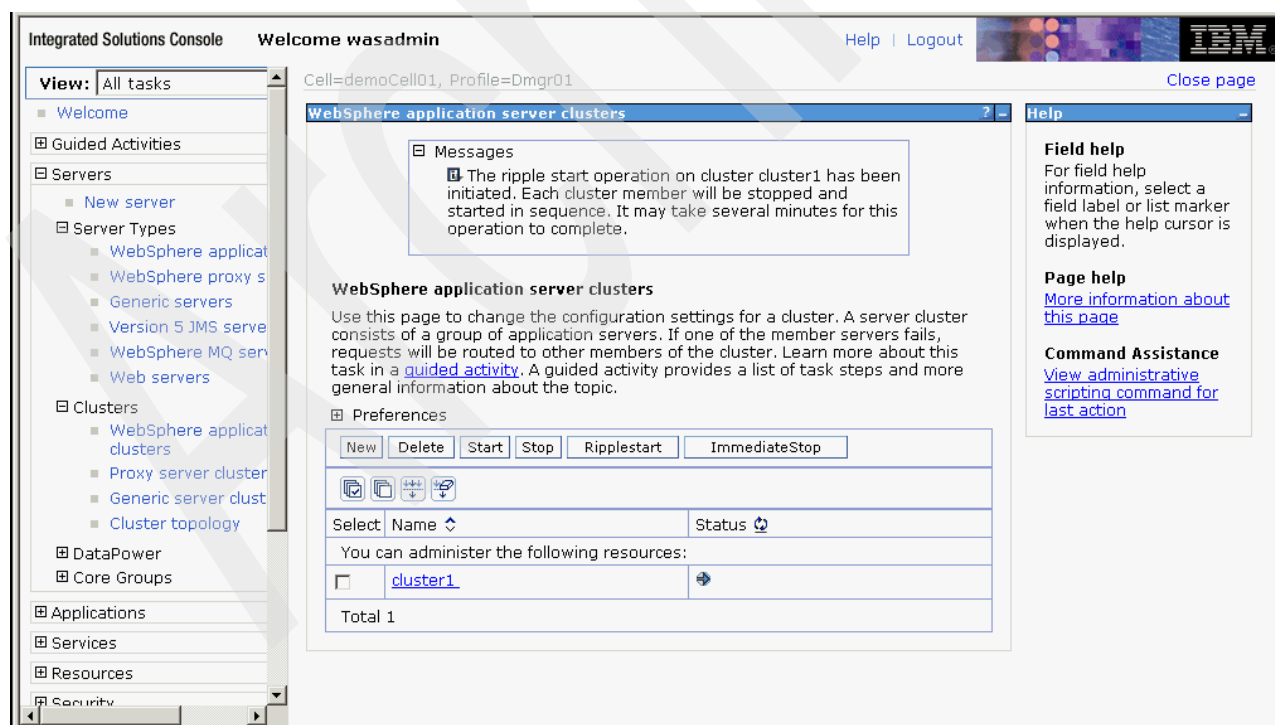


Figure 2-207 WebSphere Application Server clusters

Note: You might have to manually start the nodeagent before starting the cluster.

Restarting the IMS Server

Stop and start the IMS Server from the WebSphere ISC.

1. To stop the IMS Server:
 - a. From the ISC, select **Applications** → **Application Types** → **WebSphere Enterprise Applications**.
 - b. Select the **TAM E-SSO IMS** check box.
 - c. Click **Stop**. Once the application is stopped, the status is displayed (Figure 2-208).

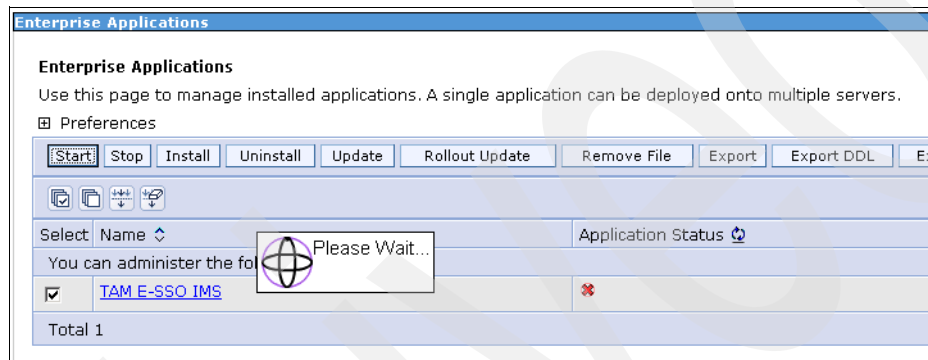


Figure 2-208 Application successfully stopped

2. To restart the IMS Server:
 - a. From the ISC, select **Applications** → **Application Types** → **WebSphere Enterprise Applications**.
 - b. Select the **TAM E-SSO IMS** check box.
 - c. Click **Start**. Once the application is restarted, the status is displayed (Figure 2-209).

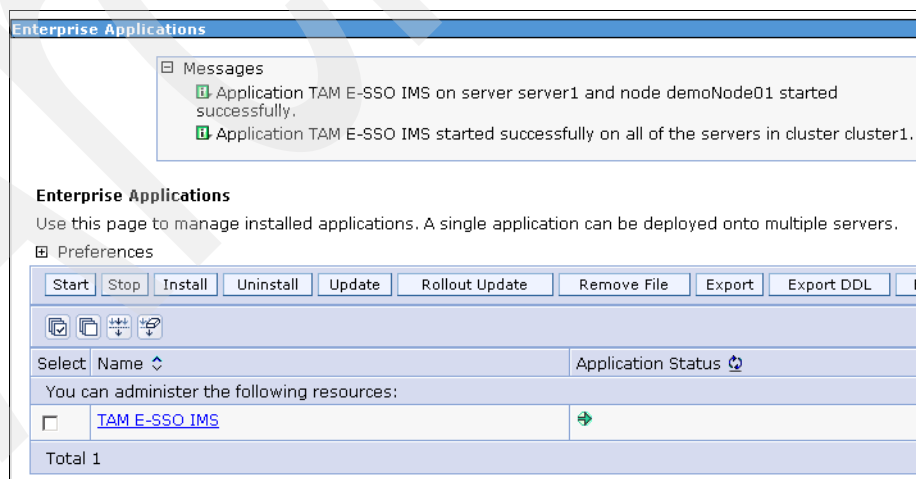


Figure 2-209 Application successfully started

2.7 Adding nodeagent and server to Windows services

Run the WebSphere wasservice application to add the nodeagent and server to the Windows startup. This allows the services to start automatically when the server is rebooted.

2.7.1 nodeagent

Take the following steps:

1. Open a command prompt window and enter the following commands:

```
>cd E:\Program Files\IBM\WebSphere\AppServer\bin
```

```
>E:\Program Files\IBM\WebSphere\AppServer\bin>wasservice -add Custom01NodeAgent  
-serverName nodeagent -profilePath "E:\Program  
Files\IBM\WebSphere\AppServer\profiles\Custom01" -wasHome "E:\Program  
Files\IBM\WebSphere\AppServer" -logRoot "E:\Program  
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\nodeagent" -logFile  
"E:\Program  
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\nodeagent\startServer.log"  
-restart true -startType automatic
```

```
Adding Service: Custom01NodeAgent
```

```
Config Root: E:\Program
```

```
Files\IBM\WebSphere\AppServer\profiles\Custom01\config
```

```
Server Name: nodeagent
```

```
Profile Path: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
```

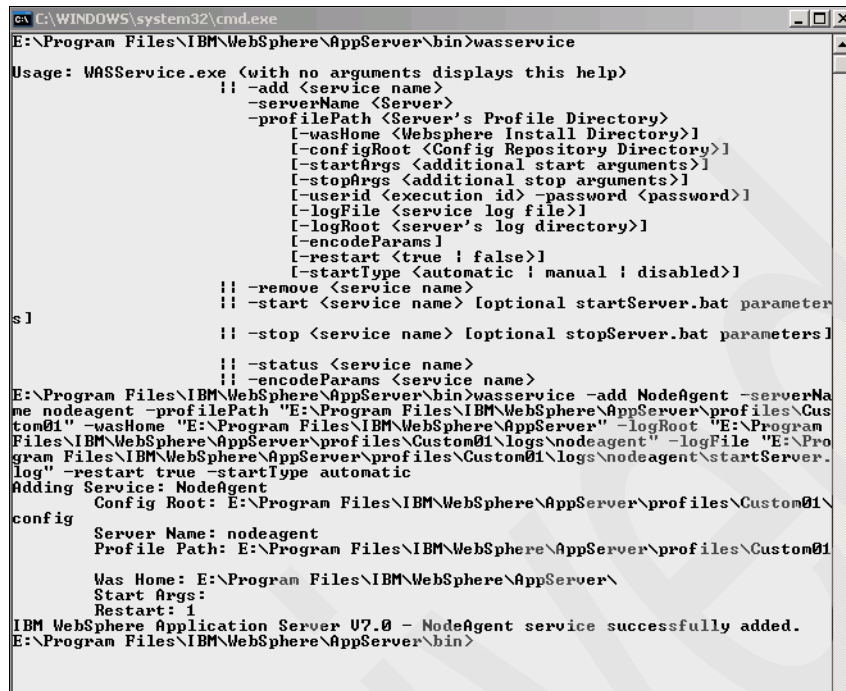
```
Was Home: E:\Program Files\IBM\WebSphere\AppServer\
```

```
Start Args:
```

```
Restart: 1
```

```
IBM WebSphere Application Server V7.0 - Custom01NodeAgent service successfully  
added.
```

Figure 2-210 depicts the command prompt output.



```

C:\WINDOWS\system32\cmd.exe
E:\Program Files\IBM\WebSphere\AppServer\bin>wasservice

Usage: WASService.exe <with no arguments displays this help>
    || -add <service name>
    || -serverName <Server>
    || -profilePath <Server's Profile Directory>
    || [-wasHome <WebSphere Install Directory>]
    || [-configRoot <Config Repository Directory>]
    || [-startArgs <additional start arguments>]
    || [-stopArgs <additional stop arguments>]
    || [-userid <execution id> -password <password>]
    || [-logFile <service log file>]
    || [-logRoot <server's log directory>]
    || [-encodeParams]
    || [-restart <true ! false>]
    || [-startType <automatic ! manual ! disabled>]
    || -remove <service name>
    || -start <service name> [optional startServer.bat parameter
s]
    || -stop <service name> [optional stopServer.bat parameters]
    || -status <service name>
    || -encodeParams <service name>
E:\Program Files\IBM\WebSphere\AppServer\bin>wasservice -add NodeAgent -serverName
nodeagent -profilePath "E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01"
-wasHome "E:\Program Files\IBM\WebSphere\AppServer" -logRoot "E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\nodeagent" -logFile "E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\nodeagent\startServer.
log" -restart true -startType automatic
Adding Service: NodeAgent
Config Root: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\
config
Server Name: nodeagent
Profile Path: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
Was Home: E:\Program Files\IBM\WebSphere\AppServer\
Start Args:
Restart: 1
IBM WebSphere Application Server U7.0 - NodeAgent service successfully added.
E:\Program Files\IBM\WebSphere\AppServer\bin>
  
```

Figure 2-210 Output for adding a nodeagent

2. Edit the registry settings to make the CellManager service dependent on the nodeagent starting first.
3. Open the key via the registry editing tool (regedit) by clicking **My Computer** → **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Services** → **IBMwas70Service - demoCellManager01**.
4. Create a MultiString value named **DependOnService** and enter the value **IBMwas70Service - Custom01NodeAgent**.

This makes the CellManager service dependent on the nodeagent service starting first (Figure 2-211).

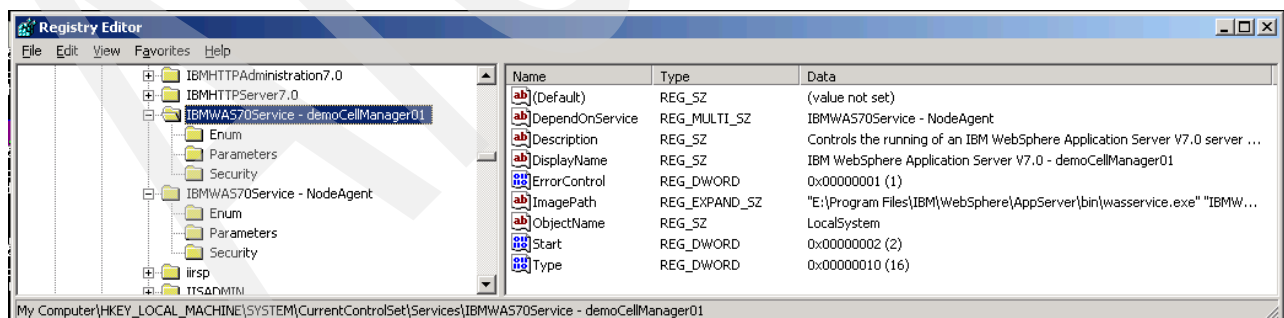


Figure 2-211 Registry editor

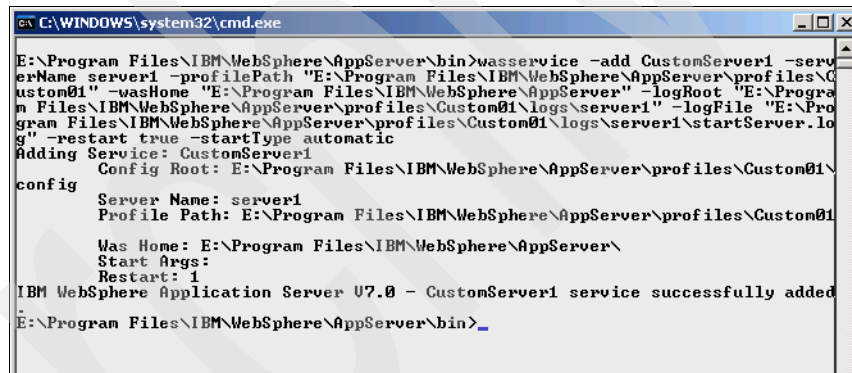
2.7.2 server1

Take the following steps:

1. Open a command prompt window and enter the following commands:

```
E:\Program Files\IBM\WebSphere\AppServer\bin>wasservice -add CustomServer1
-serverName server1 -profilePath "E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom01" -wasHome "E:\Program
Files\IBM\WebSphere\AppServer" -logRoot "E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\server1" -logFile
"E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\server1\startServer.log"
-restart true -startType automatic
Adding Service: CustomServer1
    Config Root: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\
config
    Server Name: server1
    Profile Path: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
Was Home: E:\Program Files\IBM\WebSphere\AppServer\
Start Args:
Restart: 1
IBM WebSphere Application Server V7.0 - CustomServer1 service successfully
added.
```

Figure 2-212 depicts the command prompt output.



```
C:\WINDOWS\system32\cmd.exe
E:\Program Files\IBM\WebSphere\AppServer\bin>wasservice -add CustomServer1 -serv
erName server1 -profilePath "E:\Program Files\IBM\WebSphere\AppServer\profiles\C
ustom01" -wasHome "E:\Program Files\IBM\WebSphere\AppServer" -logRoot "E:\Progra
m Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\server1" -logFile "E:\Progr
am Files\IBM\WebSphere\AppServer\profiles\Custom01\logs\server1\startServer.log"
-g" -restart true -startType automatic
Adding Service: CustomServer1
    Config Root: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01\
config
    Server Name: server1
    Profile Path: E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom01
Was Home: E:\Program Files\IBM\WebSphere\AppServer\
Start Args:
Restart: 1
IBM WebSphere Application Server V7.0 - CustomServer1 service successfully added
E:\Program Files\IBM\WebSphere\AppServer\bin>_
```

Figure 2-212 Output for adding server1

2. Edit the registry settings to make the server1 service dependent on the nodeagent starting first.
3. Open the key via the registry editing tool (regedit) by selecting **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Services** → **IBMWAS70Service - CustomServer1**.

4. Create a multi-string value named DependOnService with a value IBMWAS70Service - Custom01NodeAgent (Figure 2-213).

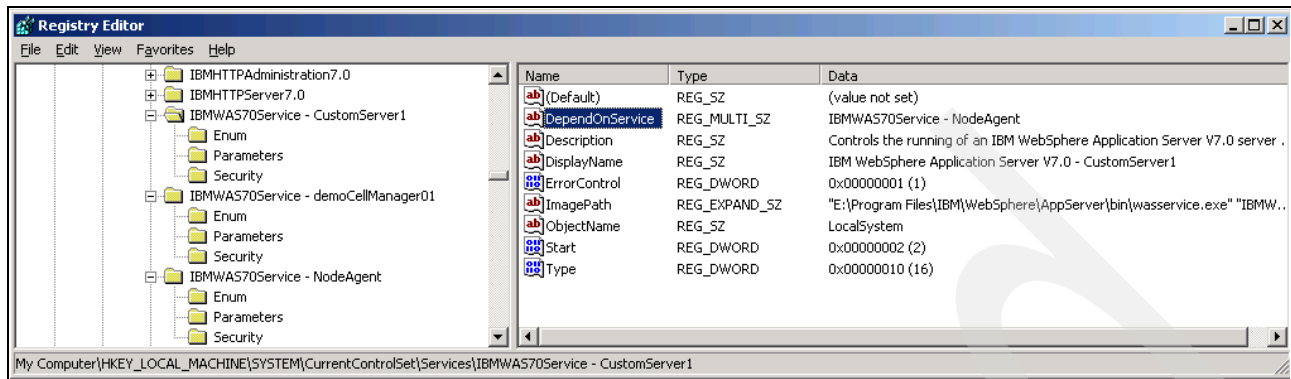


Figure 2-213 Create multi-strong value name

To provision the IMS administrator and to set up the Tivoli Access Manager for Enterprise Single Sign-On IMS enterprise directory, see 1.5.4, “Provisioning IMS administrator and defining enterprise directory” on page 57.

This concludes the configuration of the WebSphere Application Server cluster environment.

Database type configuration for IMS Server

On the Database Configuration page you are prompted for the DB configuration information relevant to the server. Figure A-1 on page 204 shows the settings for DB2:

- ▶ Hostname: host name (or IP address) where the DB server resides.
- ▶ Port: DB server listening port. This was an option during the DB2 install, and 50000 is the default. It might be different if you have multiple DB2s on the one server.
- ▶ Database Name: the name of the IMS Server database to configure as defined during the DB2 install (see 1.1.2, “Creating a database” on page 12).
- ▶ User Name: DB2 administrator account defined during DB2 install (db2admin is the default).
- ▶ User Password: DB2 administrator password defined during DB2 install.

If you are using Oracle or Microsoft SQL Server, the values will be different. For example, with Microsoft SQL Server, you are prompted for the instance (optional) when a non-default Microsoft SQL Server instance has been created. See “Microsoft SQL Server configuration for IMS Server” on page 204 for more details.

Figure A-1 Database configuration

If you are using MS SQL Server, the next page asks whether you want to create a new database. See “Microsoft SQL Server configuration for IMS Server” on page 204 for the ramifications of this. If you have already created the (empty) database, leave this option unselected and click **Next** to continue.

Microsoft SQL Server configuration for IMS Server

There are certain requirements for MS SQL Server when used as the IMS Server datastore. These are not clear in the *Installation Guide*, but the Release Notes and Setup Guide contain pertinent information.

The relevant sections of the Setup Guide are:

- For MS SQL Server 2000

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc/common/database_prerequisites_SQL_Server_2000.html

- For MS SQL Server 2005

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itamesso.doc/common/database_prerequisites_SQL_Server_2005.html

- For MS SQL Server 2008 we refer to the following tech note:

<http://www.ibm.com/support/docview.wss?uid=swg21420688>

There are, according to our reading of the documentation, two ways to create the database and IMS schema after you have installed MQ SQL Server itself:

- During the IMS Server Database Configuration step, select **Create new database** and specify the system administrator (SA) account/password as the **User Name/Password**. This creates the database instance and loads the ESSO schema/initial data.
- Before running the IMS Server configuration, create an empty database instance using the MS SQL Server admin UI. Also create a database owner and set the appropriate

rights/settings. Then during the IMS Server Database Configuration do *not* select (or de-select) **Create new database**, then specify the database owner/password as the **User Name/Password**.

We have not tried the first approach, however most for most customer deployments you do not want the top-level system administrator account information stored in an application outside of the DBA teams control. Thus, most deployments use the second option.

It is important that you follow the requirements in the links above, particularly the one about not having the database owner as an administrator. If you do (as we found), then the schema is created with an owner of dbo (for example, dbo.IMSTrustedCA) but when IMS talks to the database the calls are against a prefix of owner (for example, fred.IMSTrustedCA).

The safest way that we found to have a working database is to have the database name and owner name the same (for example, a database name of "Tamesso" and an owner of Tamesso). Theoretically, if you have both the default schema of the DB owner being the IMS DB name and the default DB for the DB owner being the IMS DB, then it should all work, but it did not for us.

One final note is that when creating the DB in the MS SQL Server admin UI, make sure that the correct collation is used (SQL_Latin1_General_CP1_CS_AS). If not, you see error messages during the configuration.

Archived

Diagnosing installation problems

Many separate components and prerequisite steps are required to fully achieve the installation and configurations of Tivoli Access Manager for Enterprise Single Sign-On 8.1, WebSphere Application Server, IBM HTTP Server, Database Server Type installation, fix packs, and so on. Due to the complexity and many installation and configuration steps involved, there is a chance that problems will be encountered during the install, as there are more points of failure.

There is limited information about diagnosing problems in the *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309. The *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Troubleshooting and Support Guide*, GC23-9693, has a far more comprehensive coverage of installation issues and how to debug them.

This appendix contains additional information accumulated during Tivoli Access Manager for Enterprise Single Sign-On installations.

AccessAgent connection to IMS Server

The main challenge encountered is when installing the AccessAgent and its unsuccessful attempt to contact the IMS Server. To diagnose these types of problems you need to understand the organization and interaction between the AccessAgent and the IMS Server application running on WebSphere Application Server. This is covered in Appendix C, “Using ports and networks” on page 211.

One particular reason why AccessAgent is not able to connect to the IMS Server might be that the Windows firewall is turned on. Disable the firewall to troubleshoot AccessAgent when it is not functioning as expected behind a firewall.

The following sections provide steps to help diagnose connection problems. For the sake of the discussion, the IMS Server (and HTTP Server) host name is `imsserver.demo.com`, the IHS ports are standard (80, 443), and WebSphere Application Server ports are standard (9080, 9443). We also assume that you are trying to connect to IMS using https and the https port.

Is the HTTP server/port accessible

The first thing to check is whether a browser can resolve the IMS Server host name. Enter a URL of `http://imsserver.demo.com:80`. You will see the standard IBM HTTP Server page. If this works, you have proven that the host name is resolvable, the HTTP server is running, and port 80 is accessible. If it does not work, check name resolution and http port configuration, and that the http server is running.

Is the HTTPS port accessible

Repeat the above steps with https: `https://imsserver.demo.com:443`. You should get a dialog complaining about the certificate that the server has presented. On validating the certificate you should get to the standard IBM HTTP Server page. If this works, you have proven that the HTTPS configuration in the `httpd.conf` is correct and that there is a certificate. If it does not work, re-check the SSL configuration in the `httpd.conf` file.

Does the host name match the SSL Cert DN

Note the host name in the CN of the SSL certificate. It should be the same as the fully qualified host name that you are specifying in the AccessAgent config.

If the host name that you are specifying is different from that in the CN of the certificate, try again with the correct host name.

Is the WebSphere Application Server available for SOAP requests

The AccessAgent uses a ping service of `/ims/services/encentuate.ims.service.ServerInfo`. In the browser, try:

- ▶ For http
<http://imsserver.demo.com:9080/ims/services/encentuate.ims.service.ServerInfo>
- ▶ For https
<https://imsserver.demo.com:9080/ims/services/encentuate.ims.service.ServerInfo>

This should resolve and give you a welcome message.

If this works you have proven that WebSphere Application Server is running and that the IMS application is installed and responding to SOAP requests. If not, check that WebSphere Application Server is running and that the IMS application is running in WebSphere Application Server.

Is WebSphere Application Server plug-in configured correctly

You should be able to send requests to the HTTP Server ports, and the WebSphere Application Server plug-in will route the request to the WebSphere Application Server server. In the browser, try:

- For http:

`http://imsserver.demo.com/ims.services/encentuate.ims.service.ServerInfo`

- For https:

`https://imsserver.demo.com/ims.services/encentuate.ims.service.ServerInfo`

This should resolve and give you the same welcome message. If this works you have proven that the HTTP Server is taking requests on port 80, identifying the /ims portion of the URL, and routing them (as per the WebSphere Application Server plug-in) to WebSphere Application Server. If not, check the URIGroup settings in the plugin-cfg.xml file. Example B-1 shows a sample correct plugin-cfg.xml file.

Example B-1 plugin-cfg.xml example

```
<UriGroup Name="default_host_server1_IMS81Node01_Cluster_URIs">
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/snoop/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/hello"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/hitcount"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsp"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsw"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsw"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/j_security_check"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ibm_security_logout"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/servlet/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/static/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/front/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/webconf/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/admin/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ims/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/aawwp/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/help/admin/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/help/aawwp/*"/>
<Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/ivt/*"/>
</UriGroup>
```

The key entries are those from /static/ through /help/aawwp/. If these are missing, the WebSphere Application Server plug-in needs to be re-generated.

Archived

Using ports and networks

With the change of middleware with the current Tivoli Access Manager for Enterprise Single Sign-On, there is potential for confusion over what ports are being used between the AccessAgent and the IMS Server.

Figure C-1 shows the key components in the communication flow between the AccessAgent and the IMS Server.

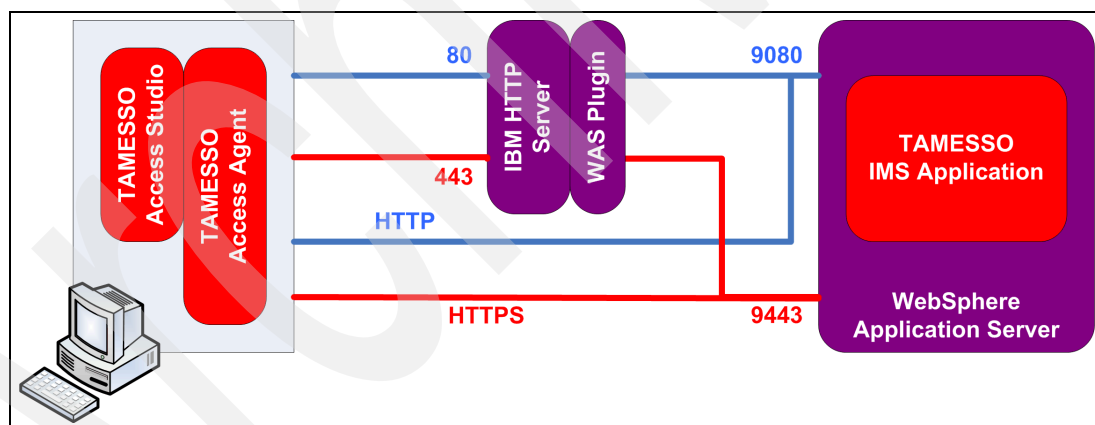


Figure C-1 Database configuration

The IMS application is running on WebSphere Application Server using the embedded WebSphere Application Server HTTP Server. This is listening on ports 9080 (HTTP) and 9443 (HTTPS). WebSphere Application Server invokes the appropriate IMS Server code based on the URLs received at the embedded HTTP Server (for example, `/ims/services/encntuate.ims.service.ServerInfo`).

For troubleshooting purposes only, the AccessAgent can communicate with the IMS server application directly using the 9080/9443 ports based on the above diagram in Figure C-1.

Default ports: By default, WebSphere Application Server port numbers are set to 9080 and 9443 during the installation, but it can be configured differently for each environment.

If the default ports (80/443) are used, the AccessAgent communicates with the IBM HTTP Server (IHS). The HTTP Server looks up the URL against the URI definitions loaded from the WebSphere Application Server plug-in `plugin-cfg.xml` file. If configured correctly, it routes all requests with URLs of the following forms to WebSphere Application Server:

- ▶ `static/*`
- ▶ `/front/*`
- ▶ `/webconf/*`
- ▶ `/admin/*`
- ▶ `/ims/*`
- ▶ `/aawwp/*`
- ▶ `/help/admin/*`
- ▶ `/help/aawwp/*`

The communication between the AccessAgent is all SOAP over HTTP/HTTPS.

Uninstalling Tivoli Access Manager for Enterprise Single Sign-On

This appendix covers the uninstallation of Tivoli Access Manager for Enterprise Single Sign-On 8.1. There is an uninstall program, but this does not cover all components that are installed.

This section is not concerned with removing WebSphere Application Server or database components, only the Tivoli Access Manager for Enterprise Single Sign-On components, under the assumption that there will be a re-install.

Standard uninstall

You can use the standard Windows add/remove programs utility to remove the Access Studio, Access Agent, and IMS Server components.

Make sure that you restart the system as advised.

Additional WebSphere Application Server cleanup

Removing IMS is essentially deleting the WebSphere Application Server profile. You might see the following link for information about how to delete a profile:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/tasks/IMS_Troubleshoot_Delete_Profile.html

There is also a Technote document available that offers more steps for what needs to be performed to do a WebSphere Application Server cleanup. This article was written to troubleshoot when a problem arises during the IMS Installation process, when a configuration failure happens using the IMS Configuration Utility, and results in being unable to return to the IMS configuration page. The article is available at:

<http://www.ibm.com/support/docview.wss?uid=swg21438690>

There are two options for cleaning up WebSphere Application Server:

- ▶ Delete the profile. See the instructions here:
http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/tasks/IMS_Troubleshoot_Delete_Profile.html
- ▶ Do a manual cleanup.

The steps for performing a manual clean up for WebSphere Application Server are:

1. Remove the JDBC settings:
 - a. Open the WebSphere Application Server ISC. Navigate to **Resources** → **JDBC** → **JDBC Providers**.
 - i. Delete the JDBC providers named TAM E-SSO JDBC Provider.
 - ii. Navigate to **Security** → **Global Security**.
 - iii. Under **Authentication**, go to **Java Authentication and Authorization Service**. Click **J2C Authentication data**.
 - b. Delete **imsauthdata**.
2. Remove the IMS KeyStore:
 - a. Click **Security** → **SSL certificate and key management** → **Key Stores and Certificates** on the right (under Related Items).
 - b. Select the check box for the IMS Entry, TAMESSOIMSKeystore, and click **Delete**.
 - c. Navigate to **Environment** → **Naming** → **Name space bindings**.
 - d. Delete the IMS Runtime URL.
 - e. Save the changes to the master configuration.

- f. Open Windows Explorer and delete the keystore file
 <PROFILE_ROOT>\config\cells\<CELL_NAME>\TAMESSOIMSKeystore.jks.
- g. Delete the <PROFILE_ROOT>\config\tamesso folder.
3. Restart the server (restart Dmgr and the cluster if you are using clustered IMS).
4. Delete the IMS database.

File system cleanup

The install leaves a lot of files and directories around. The uninstall utility does not remove all of them. First, make sure that the Tivoli Access Manager for Enterprise Single Sign-On directory is deleted (C:\Program Files\IBM\TAMESSO). Next run a search across the WebSphere AppServer directory (C:\Program Files\IBM\WebSphere\AppServer) looking for IMS. You will probably find a lot of cache and temporary entries for empty folders that can be cleaned up. We also found a KeyStore file that was causing problems with the install and had to delete it.

Archived

Creating WebSphere Application Server

To create a new WebSphere Application Server for your cluster, navigate to the WebSphere Administration Console, then:

1. Navigate to **Servers** → **New Server**.
2. For the server type, select **WebSphere Application Server** and click **Next**.
3. Select the node from the drop-down menu.
4. Enter a server name (for example, server2) and click **Next**.

Note: Specify a unique name for the server in the WebSphere Application Server cluster.

5. Ensure that **Generate Unique Ports** is selected for the server-specific properties. Click **Next**.
6. Review the Summary of actions and click **Finish**.
7. Click **Save** to save the changes to the master configuration. Click **OK**.
8. Also add the application server to the WebSphere Application Server cluster.

Archived

Adding an IMS Server to the cluster

In this appendix we describe the necessary steps to add an additional IMS Server to the WebSphere Application Server cluster:

1. Create a new custom profile (for example, Custom02) for the node that you are adding to the WebSphere Application Server cluster.
2. Create a new application server (for example, server2) from the WebSphere Application Server Admin Console:
 - a. Navigate to **Servers** → **new Server**.
 - b. Select **WebSphere Application Server** and click **Next**.
 - c. Select **target node** and enter a name for the new server and click **Next** → **Next**.
 - d. Select **Generate Unique Ports** and click **Next**.
 - e. Click **Finish** and **Save**.

3. Add the newly created server to the WebSphere cluster from the ISC.
4. Add the nodeagent/application server to Windows automatic services. Run the **wasservice -add** command from the AppServer\bin directory:

```
Eg: wasservice -add Custom02NodeAgent -serverName nodeagent -profilePath
"E:\Program Files\IBM\WebSphere\AppServer\profiles\Custom02" -wasHome
"E:\Program Files\IBM\WebSphere\AppServer" -logRoot "E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom02\logs\nodeagent" -logFile
"E:\Program
Files\IBM\WebSphere\AppServer\profiles\Custom02\logs\nodeagent\startServer.log"
-restart true
startType automatic
```

Similarly, add the application server.

5. Update the Windows services for the proper startup sequence:
 - a. Edit the CellManager service registry to edit the dependency of the node agent starting up first. Run regedit and navigate to the CellManager key by clicking **My Computer** → **HKEY_LOCAL_MACHINE** → **SYSTEM** → **CurrentControlSet** → **Services** → **IBMVAS70Service -demoCellManager01**.
 - b. Create a MultiString value named DependOnService with a value IBMVAS70Service - Custom02NodeAgent.

Similarly, edit the registry settings to make the new server service dependent on the nodeagent starting up first.
6. Install the NLI.rar file on the new node (refer to 2.5.1, “Installing Native Library Invoker rar file” on page 135).
7. Generate/propagate the plug-in and restart the HTTP Server.
8. Select all nodes and run a full synchronize.
9. Restart the IMS Server.

Related publications

The publications listed in this section are considered particularly suitable for a more detailed discussion of the topics covered in this paper.

IBM Redbooks publications

The following IBM Redbooks publications provide additional information about the topic in this document. Note that certain publications referenced in this list might be available in softcopy only.

- ▶ *Deployment Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7350
- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On v8.0 Migration Guide for Encentuate 3.4 and 3.5*, REDP-4615
- ▶ *Certification Study Guide Series: IBM Tivoli Access Manager for Enterprise Single Sign-On 8.0*, SG24-7784

You can search for, view, or download Redbooks publications, Redpapers publications, Technotes, draft publications and Additional materials, as well as order hardcopy Redbooks publications, at this website:

ibm.com/redbooks

Other publications

These publications are also relevant as further information sources:

- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309
- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Setup Guide*, GC23-9692
- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Deployment Guide*, SC23-9952
- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Troubleshooting and Support Guide*, GC23-9693
- ▶ *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Policies Definition Guide*, SC23-9694

Online resources

These websites are also relevant as further information sources:

- ▶ How to use Microsoft SQL Server 2008 as the database server
<http://www.ibm.com/support/docview.wss?uid=swg21420688>
- ▶ How to replace the IBM HTTP Server SSL certificate with an SSL certificate signed by a third-party CA.
http://www.ibm.com/support/docview.wss?rs=0&q1=1424371&uid=swg21424371&loc=en_US
- ▶ The IBM Tivoli Access Manager for Enterprise Single Sign-On reference manuals on the online information center:
<http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?topic=/com.ibm.itamesso.doc/welcome.htm>

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services



Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 for Single-Server and Cluster Environments



Covers the detailed setup and configuration for all infrastructure components

Provides thorough explanations of key components

Discusses a step-by-step installation approach

This IBM Redpaper publication covers the detailed step-by-step installation of IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 onto a single-server as well as a clustered environment.

This paper supplements the *IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 Installation Guide* and *IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1 Setup Guide*. Do not use this document in isolation. Check the relevant guides in the Tivoli Access Manager for Enterprise Single Sign-On Information Center as you perform the install.

There might be various reasons to install Tivoli Access Manager for Enterprise Single Sign-On into either a single server or a clustered environment. A small-scale deployment, a typical proof of technology, or a proof of concept might be the best examples for a single server installation, whereas larger scale deployments or requirements for high availability and scalability might be reasons to deploy in a clustered environment.

This IBM Redpaper is targeted towards administrators and engineers who are facing a Tivoli Access Manager for Enterprise Single Sign-On deployment on either a single IBM WebSphere Application Server or a clustered IBM WebSphere Application Server Network Deployment configuration.

INTERNATIONAL TECHNICAL SUPPORT ORGANIZATION

BUILDING TECHNICAL INFORMATION BASED ON PRACTICAL EXPERIENCE

IBM Redbooks are developed by the IBM International Technical Support Organization. Experts from IBM, Customers and Partners from around the world create timely technical information based on realistic scenarios. Specific recommendations are provided to help you implement IT solutions more effectively in your environment.

For more information:
ibm.com/redbooks