
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

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

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 ................................................ vii

### 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
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™
- 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](http://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](http://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:
- Stay current on recent Redbooks publications with RSS Feeds:
  http://www.redbooks.ibm.com/rss.html
Chapter 1. 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.

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:

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).

![DB2 Setup Launchpad](image-url)
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](image)

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](image)
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](image)

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](image)
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](image)

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](image)
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](image)

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

![DB2 tools catalog](image1)

**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**.

![Notifications](image2)

**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](image)

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](image)
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.

![Setup complete confirmation](image)

**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.

![Create Database in DB2 Control Centre](image-url)
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 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](image-url)
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.

![Create Database Wizard](image)

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/](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.
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](image)

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

![Installation Summary](image)
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.
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.

**Figure 1-25  Installation verification**

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](image)

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.

22 Setup and Configuration for IBM Tivoli Access Manager for Enterprise Single Sign-On 8.1
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.

![IBM Update Installer for WebSphere Software wizard](image-url)
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 Files\IBM\WebSphere\AppServer). When finished, click Next.

![Image of product selection](image1.png)

**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.

![Image of maintenance package directory selection](image2.png)

**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).

![Image](image1.png)

*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).

![Image](image2.png)

*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.

![Image](image-url)
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](image)

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

![Figure 1-34  Introduction](image)
3. Specify the destination folder for this installer (Figure 1-35). When finished, click **Next**.

![Figure 1-35  Installation destination for the IMS Server](image)

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](image)
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](image)

*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

![WebSphere Application Server administration security information](image)

*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](image)

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](image)

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.

![Pre-installation Summary of IMS Server](image)

**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.

---

![IBM HTTP Server Installation](image.png)

**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](image)

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](image)
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](image)

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](image)
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](image)

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](image)

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

![Image of successful installation](image)

**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 *IBM 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 <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.

   ![Command Prompt](image)

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

![Figure 1-55 Complete WebSphere Application Server configuration file changes](image)

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](image)
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:

```plaintext
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 plugfiles>\<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**

```plaintext
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.

![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-TAMESSO-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](image)

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).

   ![Configuration Wizard Import Configuration](image)

   **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.

![Figure 1-60  Data source information](image)
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 *IBM Tivoli Access Manager for Enterprise Single Sign-On Version 8.1 Installation Guide*, GI11-9309, for further information about creating database schema. In the example presented in this guide, this option has been checked.

Click **Next** to continue.
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.

![Choose Database Type](image)

*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.

![Figure 1-63 Root CA Details](image)
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.

![Figure 1-64 Configure IMS Services URL](image-url)
9. On the Confirm settings page (Figure 1-65), review and verify that the setting information entered looks correct and click **Save**.

![Confirm settings](image)
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](image)

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](image)
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.

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).
6. 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.

Figure 1-72 Password synchronization between users

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

Figure 1-73 Define credentials to be provisioned as an IMS Administrator
8. 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](image)

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](image)

9. 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).

10. 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


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.

![SetupHlp.ini](image)

Figure 1-76 AccessAgent installation and upgrade options defined in SetupHlp.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 the 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.
Installation and configuration in a clustered environment

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.

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](image)

Figure 2-2 Welcome to DB2 Version 9.7

---

Chapter 2. Installation and configuration in a clustered environment 69
2. Click **Install New** to launch the DB2 Setup wizard (Figure 2-3).

![DB2 Setup Launchpad](image1.png)

**Figure 2-3  Install a Product**

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

![Welcome to the DB2 Setup wizard](image2.png)

**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](image)

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](image)
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](image)

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

![Figure 2-8 Select the installation folder](image)
8. Define a DB2 administrator account and specify a password (Figure 2-9). When finished, click Next.

![Figure 2-9 Set user information for the DB2 Administration Server](image)

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.

![Figure 2-10 Configure DB2 instances](image)
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](image)

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](image)
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](Image)

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

![Figure 2-14 Start copying files](Image)
14. Wait for the installation to complete (Figure 2-15).

![Figure 2-15 Installing DB2 Workgroup Server Edition - DB2COPY1](image)

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](image)
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](image)

*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](image)
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.

![Specify the locale for this database](Image)

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.

![Create Database Wizard](image)

*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.
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](image)

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](image)
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.

![System Prerequisites Check](image)

**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.

![Optional Features Installation](image)

**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.

![Warning](image)

*Figure 2-28 Warning*

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

![Repository](image)

*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](image)

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

![Figure 2-31 Installation Summary](image)
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](image)

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

![Figure 2-35 System Prerequisites Check](image)

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

![Figure 2-37 Installation Complete](image)

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

![Figure 2-39  Product Selection](image)

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

![Figure 2-40  Maintenance Operation Selection](image)
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](image1)

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](image2)
Click **Next** on the Installation Summary page (Figure 2-43) and wait for the installation to complete.

![Figure 2-43 Installation Summary](image)

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](image)

**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).

   ![Welcome to the Profile Management Tool](image)

   **Figure 2-45   Welcome to the Profile Management Tool**
2. Click **Create** to create a new profile (Figure 2-46).

![Profile Management Tool 7.0 - Profiles tab](image)

**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).

![Environment Selection](image)

**Figure 2-47   Environment Selection**
4. On the Server Type Selection page (Figure 2-48), select **Deployment manager** and click **Next**.

![Figure 2-48 Server Type Selection](image)

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

![Figure 2-49 Profile Creation Options](image)
6. 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**.

![Figure 2-50 Administrative Security](image)

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

![Figure 2-51 Profile Creation Summary](image)
Wait for the profile creation to complete (Figure 2-52).

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 2-52 Profile Creation Progress](image)

![Figure 2-53 Profile Creation Complete](image)
9. If you re-launch the WebSphere Profile Management Tool (by clicking **Start → All Programs → IBM WebSphere → Application Server Network Deployment V7.0 → Profile Management Tool**), you will see the Dmgr01 profile has been created (Figure 2-54).

![Figure 2-54 Profile Management Tool 7.0 - Profiles tab](image)

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

![Figure 2-57 Federation](image)

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

![Figure 2-58 Profile Creation Summary](image)
6. 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**.

![Profile Creation Complete](image)

**Figure 2-59  Profile Creation Complete**

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

![Profile Management Tool](image)

**Figure 2-60  Profile Management Tool 7.0 - Profiles tab**

8. 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`).
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.

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

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

   Click New.

\begin{figure}[h]
\centering
\includegraphics[width=\textwidth]{Figure_2-61.png}
\caption{WebSphere Application Server clusters}
\end{figure}

\textbf{Note:} Similarly, create custom profiles for all the nodes to be added to the WebSphere Application Server cluster.
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**.

![Figure 2-62 Create a new cluster](image1)

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).

![Figure 2-63 Create first cluster member](image2)
Click **Next** to continue.

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

![Create a new cluster](image)

**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).
9. 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:

1. 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]

IBM HTTP Server installation

IBM HTTP Server is a Web server that is based on the Apache Web server, developed by the Apache Software Foundation. IBM HTTP Server 7.0 adds several functional enhancements to the Apache base.

- **Launch the installation wizard for IBM HTTP Server**
  - Install IBM HTTP Server using the installation wizard.

  - **WebSphere Application Server Network Deployment**
  - **IBM HTTP Server Installation**
  - **WebSphere Application Server**
  - **Welcome**
  - **Welcome wasadmin**
  - **Welcome to WebSphere Application Server clusters**
  - **Preferences**
  - **Prerequisites**
  - **Start**
  - **Stop**
  - **Ripplestart**
  - **ImmediateStop**
  - **Select Name**
  - **Status**
  - **You can administer the following resources:**
    - **userServlet**
    - **Total 1**

  - **Field help**
    - For field help information, select field label or list, when the help clue is displayed.
  - **Page help**
    - More information.
  - **Command Assistant**
    - View administrative scripting commands.
Click **Next** to continue (Figure 2-67).

![Figure 2-67 Welcome to IBM HTTP Server 7.0](image)

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

![Figure 2-69 System Prerequisites Check](image)

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

![Figure 2-70 Enter the installation location](image)
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**.

![Port Values Assignment](image)

*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](image-url)
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**.

![HTTP Administration Server Authentication](image)

**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**.

![IBM HTTP Server Plug-in for IBM WebSphere Application Server](image)

**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](image)

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

![Figure 2-76  Success](image)

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](image)

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](image)
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](image)

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

![Available Maintenance Package to Install](image)

**Figure 2-81** Available Maintenance Package to Install

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

![Installation Summary](image)

**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](image)

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](image)

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

![Maintenance Operation Selection](image1.png)

**Figure 2-86  Maintenance Operation Selection**

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

![Maintenance Package Directory Selection](image2.png)

**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](image)

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

![Figure 2-89  Installation Summary](image)
8. Click **Finish** when you see the success message on the Installation Complete page (Figure 2-90).

![Figure 2-90   Installation Complete](image)

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.

1. From the WebSphere Integrated Solutions console, click **Servers → Server Types → Web servers → New**.

2. 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](image)
3. 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**.

![Figure 2-92 Select a node for the Web server and select the Web server type](image)

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

![Figure 2-93 Select a Web server template](image)
5. Verify the installation location (for example, \Program Files\IBM\HTTPServer) and other properties on the Create new Web server definition page (Figure 2-94), and click Next.

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.

Figure 2-95   Confirm new Web server
7. Click **Save** to save to the master configuration (Figure 2-96).

8. Click **OK** (Figure 2-97).
**Starting the web server**

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

**Generating the plug-in**

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

### 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](image)

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

![Figure 2-102 License Agreement](image)
Click **Next** to proceed with the installation (Figure 2-103).

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

---

**Figure 2-103  Introduction**

**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](image)

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

![Figure 2-106  Pre-installation Summary](image)
Wait for the installation to complete (Figure 2-107).

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

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](image1)

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](image2)
4. Select **Install maintenance package** (Figure 2-111) and click **Next**.

![Figure 2-111 Maintenance Operation Selection](image)

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

![Available Maintenance Package to Install](image1.png)

**Figure 2-113** Available Maintenance Package to Install

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

![Installation Summary](image2.png)

**Figure 2-114** Installation Summary
Wait for the installation to complete (Figure 2-115).

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

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

![Configuration tab - General Properties](image)

**Figure 2-119** Configuration tab - General Properties
5. Click **Save** to save the changes to the master configuration (Figure 2-120).
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](image-url)
3. Click **New** (Figure 2-122).
4. 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.
5. Click **Save** to save the changes to the master configuration (Figure 2-124).

**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.

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\TAME-SSO\IMS Server\com.ibm.tamesso.ims-delhi.deploy.all.ear). Click Next.

Figure 2-126  Enterprise Applications

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](image)

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

![Figure 2-129 Select installation options](image)
### 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 dispersed among several application servers. Also, specify the Web servers as targets that serve as root requests to this application. The plug-in configuration file (plug-in.figxml) for each Web server is generated on the application server(s) that are routed through.

#### Clusters and servers:
- WebSphere cell=demoCell1 cluster=demoCell1
- WebSphere cell=demoCell1 node=demoNode1 server=webserver1

<table>
<thead>
<tr>
<th>Module (Version)</th>
<th>URL</th>
<th>Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>TAM ESSO IMS Static Assets (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-static-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS Frontdoor (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-front-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS WebConfiguration (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-webConfiguration-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS AccessAdmin (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-accessAdmin-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS Legacy Runtime (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-runtime-war/access1-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS AccessAssistantWebWorkplace (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-accessAssistant-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS AccessAssistant Help (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-help-accessAdmin-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
<tr>
<td>TAM ESSO IMS AccessAssistant Help (0.1.0.0.281)</td>
<td>com.ibm.tamesso.imss-hole-webapp-help-accessAdmin-war/WEB-INF/web.xml</td>
<td>WebSphere cell=demoCell1,cluster=demoCell1</td>
</tr>
</tbody>
</table>

*Figure 2-130  Map modules to servers*
7. 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.

![Map modules to servers](image)

**Figure 2-131 Map modules to servers**
8. Review the installation summary (Figure 2-132) and click **Finish**.
9. Click **Save** (Figure 2-133) to save changes directly to the master configuration.

If there are enterprise beans in the application, the EJB deployment process can take several minutes. Do not save the configuration until the process completes.

Check the SystemOut log on the deployment manager or server where the application is deployed for specific information about the EJB deployment process as it occurs.

**ADMA5016I:** Installation of TAM E-SSO IMS started.

**ADMA5067I:** Resource validation for application TAM E-SSO IMS completed successfully.

**ADMA5068I:** Application and module versions are validated with versions of deployment targets.

**ADMA5006I:** The application TAM E-SSO IMS is configured in the WebSphere Application Server repository.

**ADMA5035I:** The library references for the installed optional package are created.

**ADMA5006I:** The application TAM E-SSO IMS is configured in the WebSphere Application Server repository.

**ADMA5006I:** The application binaries are saved in C:\Program Files\IBM\WebSphere\AppServer\profiles\Demo01\wswtemp\S14984E14\workspace\calloutdemo01\applications\TAM E-SSO IMS.tar\TAM E-SSO IMS.ear

**ADMA5006I:** The application TAM E-SSO IMS is configured in the WebSphere Application Server repository.

**SECI400I:** Successfully updated the application TAM E-SSO IMS with the appContextIDForSecurity information.

**ADMA5006I:** The application TAM E-SSO IMS is configured in the WebSphere Application Server repository.

**ADMA5013I:** Activation plan created successfully.

**ADMA5011I:** The cleanup of the temp directory for application TAM E-SSO IMS is complete.

**ADMA5013I:** Application TAM E-SSO IMS installed successfully.

**Application TAM E-SSO IMS installed successfully.**

To start the application, first save changes to the master configuration.

Changes have been made to your local configuration. You can:
- **Save** directly to the master configuration.
- **Review** changes before saving or discarding.

To work with installed applications, click the "Manage Applications" link.

**Manage Applications**
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](image-url)
3. Under Web Module Properties, click **Session management** (Figure 2-135).

![Figure 2-135  Tivoli Access Manager for Enterprise Single Sign-On IMS](image)

<table>
<thead>
<tr>
<th>General Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
</tr>
<tr>
<td>TAM E-SSO IMS</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Detail Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Target specific application status</td>
</tr>
<tr>
<td>Startup behavior</td>
</tr>
<tr>
<td>Application binaries</td>
</tr>
<tr>
<td>Class loading and update detection</td>
</tr>
<tr>
<td>Request dispatcher properties</td>
</tr>
<tr>
<td>Security role to user/group mapping</td>
</tr>
<tr>
<td>View Deployment Descriptor</td>
</tr>
<tr>
<td>Last participant support extension</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>References</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared library references</td>
</tr>
<tr>
<td>Shared library relationships</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Modules</th>
</tr>
</thead>
<tbody>
<tr>
<td>Manage Modules</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Web Module Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session management</td>
</tr>
<tr>
<td>Context Foot For Web Modules</td>
</tr>
<tr>
<td>JSP and JSF options</td>
</tr>
<tr>
<td>Virtual hosts</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Enterprise Java Bean Properties</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default messaging provider references</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Database Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>SQL profiles and pure/query bind files</td>
</tr>
</tbody>
</table>
4. Under General Properties (Figure 2-136), check the Override session management check box to select it. Click **Apply**.

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

**Figure 2-136  Session management**
5. Click **Save** (Figure 2-137).

![Configuration tab](image)

**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**.

![General Properties](image1.png)

**Figure 2-138** General Properties

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

![Preferences](image2.png)

**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](image)

**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 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](image)
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).

![SSL certificate and key management](image)

---

Chapter 2. Installation and configuration in a clustered environment  155
2. Click **CellDefaultKeyStore** (Figure 2-143).

![Key stores and certificates](image)

**Figure 2-143  Key stores and certificates**

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

![CellDefaultKeyStore](image)

**Figure 2-144  CellDefaultKeyStore**
4. Click **Import** (Figure 2-145).

![Figure 2-145](image)

Figure 2-145  Personal certificates

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

![Figure 2-146](image)

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**.

![Figure 2-147 Import certificates from a key file or key store](image)

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

![Figure 2-148 Import certificates from a key file or key store](image)
8. Click **Save** to save directly to the master configuration (Figure 2-149).

![Figure 2-149 Personal certificates](image)

**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](image)

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](image)
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](image)

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

![Figure 2-156  Message - Changes](image)

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).

![General Properties list](image1)

**Figure 2-157   General Properties list**

8. 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.

![Enter user ID and password](image2)

**Figure 2-158   Enter user ID and password**
9. Click **Save** to save changes to the master configuration (Figure 2-159).

![Figure 2-159   Save changes to master configuration](image)

### 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).

![Figure 2-160   Data sources](image)
**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**.

![Figure 2-161 Enter basic data source information](image-url)
**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**.

![Create a data source](image)

*Figure 2-162  Create new JDBC provider*
**Entering database class path information**

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

![Figure 2-163 Enter database class path information](image)
**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**.

![Figure 2-164 Enter database specific properties for the data source](image)

**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**.

![Figure 2-165  Setup security aliases](image)
**Summary**

In summary:

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

---

### Figure 2-166  Summary of actions

<table>
<thead>
<tr>
<th>Summary</th>
<th>Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Options</td>
<td>Values</td>
</tr>
<tr>
<td>Scope</td>
<td>cells:demoCell1</td>
</tr>
<tr>
<td>Data source name</td>
<td>TAM E-SSO IMS Server Data</td>
</tr>
<tr>
<td>JDBC provider name</td>
<td>jdbc/jms</td>
</tr>
<tr>
<td>Description</td>
<td>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 PRS and supports 2-phase commit processing.</td>
</tr>
<tr>
<td>Class path</td>
<td></td>
</tr>
</tbody>
</table>
  - `jdbc:db2:db2icJar`  
  - `jdbc:db2icJar`  
  - `jdbc:db2icJar`  
  - `jdbc:db2icJar`  
  - `jdbc:db2icJar` |
| Native path | `jdbc:db2icJar` |
| 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) |

2. Click **Save** to save to the master configuration.
3. 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).

![Figure 2-167 Data sources](image-url)
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**.

![Figure 2-168 Connection pools](image-url)
10. Click **Save** to save to the master configuration.

![Image: Save to the master configuration](image)

**Figure 2-169  Save to the master configuration**

<table>
<thead>
<tr>
<th>Data sources</th>
</tr>
</thead>
<tbody>
<tr>
<td>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 connectiors 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.</td>
</tr>
</tbody>
</table>

**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 section here.

  ![Cell-demoCell01](cell-demoCell01)

**Preferences**

<table>
<thead>
<tr>
<th>New</th>
<th>Delete</th>
<th>Test connection</th>
<th>Manage state</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>JDBC name</th>
<th>Scope</th>
<th>Provider</th>
<th>Description</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="select" alt="Select" /></td>
<td><img src="name" alt="Name" /></td>
<td><img src="jdbcname" alt="JDBC name" /></td>
<td><img src="scope" alt="Scope" /></td>
<td><img src="provider" alt="Provider" /></td>
<td><img src="description" alt="Description" /></td>
<td><img src="category" alt="Category" /></td>
</tr>
</tbody>
</table>

You can administer the following resources:

- **TAM E-550**
  - **DB2 Server Data**
  - **jdbcJms**
  - **Cell-demoCell01**
  - **TAM E-550 JDBC Provider**
  - **DB2 Universal Driver**
  - **Datasource**

**Total: 1**
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).

<table>
<thead>
<tr>
<th>JDBC providers</th>
</tr>
</thead>
<tbody>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Scope:</td>
</tr>
<tr>
<td>Show scope selection drop-down list with the all scopes option</td>
</tr>
<tr>
<td>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.</td>
</tr>
<tr>
<td>Preferences</td>
</tr>
<tr>
<td>New</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Select</th>
<th>Name</th>
<th>Scope</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cell=DemoCell1, Profile=DemoProfile</td>
<td>TAM E-SSO JDBC Provider</td>
<td>Cell=DemoCell1</td>
<td>One-phase commit DB2 JDBC provider that supports DB2 9.7. 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.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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.
Testing data source connection

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

1. From the WebSphere ISC, click Resources → JDBC → Data Sources.
2. Under Preferences, select the TAM E-SSO IMS Server Data Source check box. Click Test connection (Figure 2-173).
3. Verify that the test connection was successful (Figure 2-174).

![Figure 2-174  Success message](image)
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).
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.

![Figure 2-176 Settings](image-url)
4. Click **Save** to save the configuration changes.

![Figure 2-177  JDBC Providers](image)

**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](image)

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

![Figure 2-179  Success message](image)
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** check box and click **Stop**. Once the cluster has been successfully stopped, select the **cluster1** check box again and click **Start** (Figure 2-180).

![Figure 2-180 WebSphere application server clusters](image1)

![Figure 2-181 Initiation message](image2)

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

![Figure 2-182 Cluster start verification](image3)
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](image)

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

![Figure 2-184 Success message](image)

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:

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

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

Figure 2-185  Running configurewebserver1.bat
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](image)

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).

   ![Figure 2-187 Setting properties](image)

   * 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

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

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).

![Figure 2-191 Configuration tab](image)

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

   ![Figure 2-192 Change message](image)

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

**Restarting IBM HTTP Server**

From the WebSphere ISC, follow the steps below:

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

![Figure 2-193 Select webserver](image)

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

   ![Figure 2-194 Success message](image)

5. Select the check box for the webserver (webserver1).
6. Click **Stop** to stop the server.
7. Select the check box for the webserver (webserver1).
8. Click **Start** to start the server (Figure 2-195).

![Figure 2-195   Starting the server](image)

**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](image)

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

![Figure 2-197   Success message](image)
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).

![Import Configuration](image)

*Figure 2-198  Import Configuration*
3. Select the Create IMS Server database schema check box and click Next (Figure 2-199).

![Figure 2-199  Create IMS Database Schema](image1)

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

![Figure 2-200  Choose Database Type](image2)
5. Enter/verify the database configuration information. Click Next (Figure 2-201).

![Figure 2-201 Database Configuration - DB2](image)

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).

![Figure 2-202 Provide Root CA Details](image)
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**.

![Figure 2-203 Configure IMS services URL](image)

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

![Figure 2-204 Confirm settings](image)
9. Wait for the process to complete (Figure 2-205).

![Figure 2-205  Confirm settings](image)

**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 **CellDefaulKeyStore**.
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).
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.
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** → **IBMWS70Service - demoCellManager01**.

4. Create a MultiString value named **DependOnService** and enter the value **IBMWS70Service - Custom01NodeAgent**.

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

   ![Output for adding server1](image)

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).

![Registry Editor](image)

**Figure 2-213** Create multi-string 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.
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
  

- For MS SQL Server 2005
  

- For MS SQL Server 2008 we refer to the following tech note:
  
  [link](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.
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.


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

```xml
<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="*.jsv"/>
  <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="*.jsw"/>
  <Uri AffinityCookie="JSESSIONID" AffinityURLIdentifier="jsessionid" Name="/i_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.
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.

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/encentuate.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:


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:


There are two options for cleaning up WebSphere Application Server:

- Delete the profile. See the instructions here:


- 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, TAMESOIMSKeystore, 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.
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.
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 →
      IBMWAS70Service -demoCellManager01**.

   b. Create a MultiString value named DependOnService with a value IBMWAS70Service -
      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:

Online resources

These websites are also relevant as further information sources:

- How to use Microsoft SQL Server 2008 as the database server
  

- 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:
  

Help from IBM

IBM Support and downloads

ibm.com/support

IBM Global Services

ibm.com/services

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.