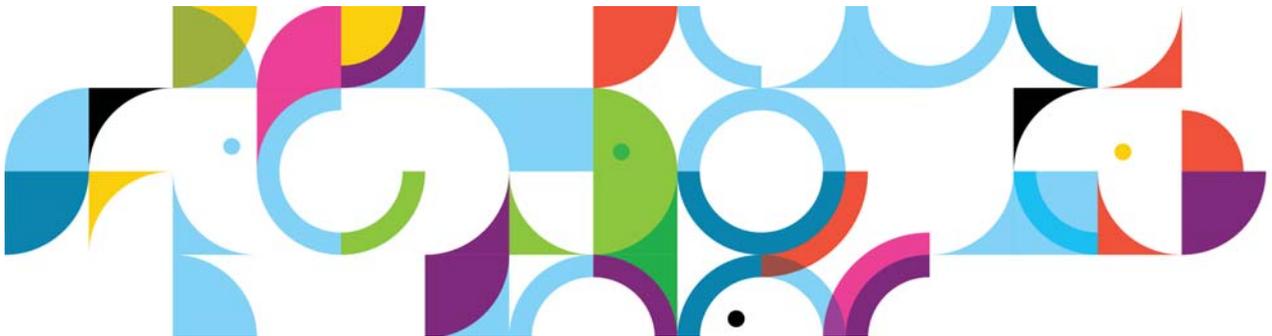


*IBM Connections 4 Public
Deployment Scenarios*

Deployment Scenarios

ERC 1.0



Trademarks

IBM® and the IBM logo are registered trademarks of International Business Machines Corporation.

The following are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide:

AIX®	Cognos®	DB™
DB2 Universal Database™	DB2®	Domino®
Lotus®	LotusScript®	Notes®
Power®	Quickr®	Rational®
Sametime®	System z®	Tivoli®
WebSphere®	400®	

Intel and Xeon are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

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

UNIX is a registered trademark of The Open Group in the United States and other countries.

Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Other product and service names might be trademarks of IBM or other companies.

January 2013 edition

The information contained in this document has not been submitted to any formal IBM test and is distributed on an “as is” basis without any warranty either express or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer’s ability to evaluate and integrate them into the customer’s operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will result elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

© Copyright International Business Machines Corporation 2013.

This document may not be reproduced in whole or in part without the prior written permission of IBM.

Note to U.S. Government Users — Documentation related to restricted rights — Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract with IBM Corp.

IBM Connections 4: PDS SSO configuration

About the author



Xiao Jin Zhao works on the Connections system verification test team and has four years' experience with Connections and six years' experience in testing. She is familiar with Connections product and other ICS portfolio, including installing, configuring, administration, use, and troubleshooting issues. Xiao Jin can be reached at zhaoxjin@cn.ibm.com.

Legend

- connections.example.com: dmgr + http
- node1.example.com: n1
- node2.example.com: n2
- oracleserver.example.com: oracle
- tam.example.com: Tivoli Access Manager server
- quickr.example.com: Quickr domino server
- sametime.example.com: Sametime server
- domino ldap.example.com: LDAP server

Contents

1. Pre-installation tasks
2. Installing IBM Connections 4.0 using LC wizard
3. Post-installation tasks

1. Pre-installation tasks

Installing base software

Install Oracle 10.2.0.5 as database server on Windows 2003

Follow these steps to complete the installation of Oracle 10.2.0.5 as database server on Windows 2003:

1. On the Oracle Database 10g Installation wizard, select Basic Installation as installation method and click **Next**.

Oracle Database 10g Installation - Installation Method

Select Installation Method

Basic Installation
Perform full Oracle Database 10g installation with standard configuration options requiring minimal input. This option uses file system for storage, and a single password for all database accounts.

Oracle Home Location: e:\oracle\product\10.2.0\db_1

Installation Type: Enterprise Edition (1.3GB)

Create Starter Database (additional 720MB)

Global Database Name: orcl

Database Password: ***** Confirm Password: *****

This password is used for the SYS, SYSTEM, SYSMAN, and DBSNMP accounts.

Advanced Installation
Allows advanced selections such as different passwords for the SYS, SYSTEM, SYSMAN, and DBSNMP accounts, database character set, product languages, automated backups, custom installation, and alternative storage options such as Automatic Storage Management.

ORACLE

Figure 1. Installation method screen

2. On the Product-Specific Prerequisite Checks screen, check that there are no requirements to be verified and click **Next**.

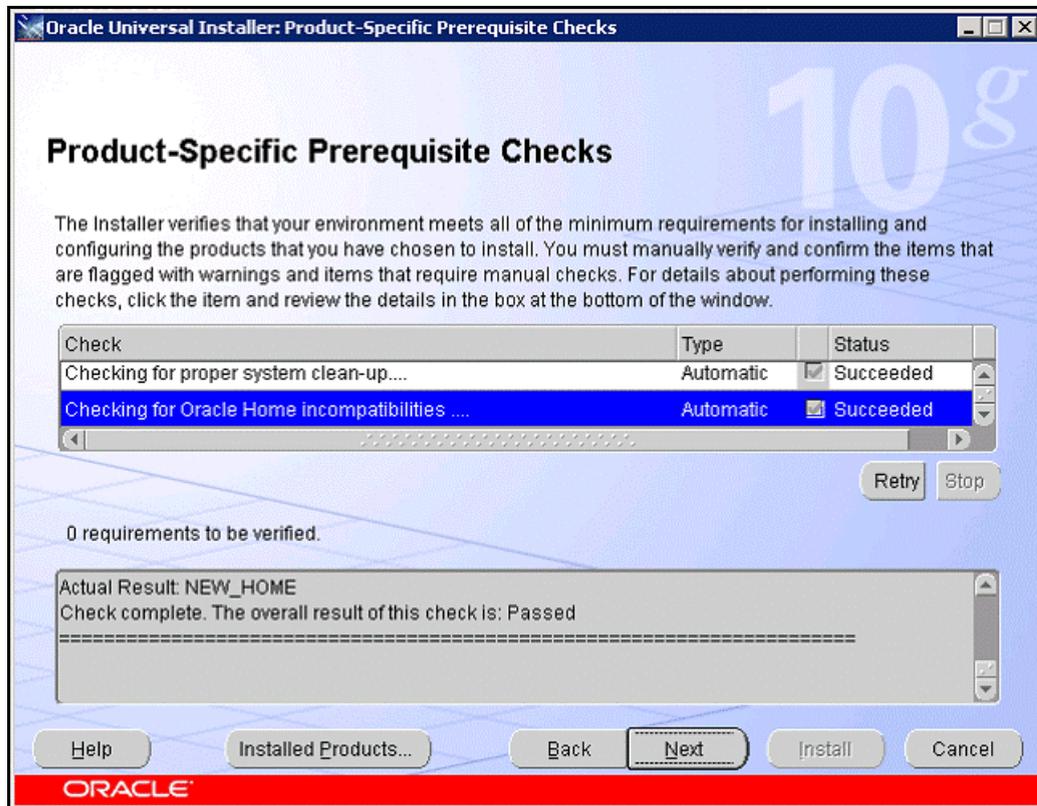


Figure 2. Product-Specific Prerequisite Checks

3. On the Summary screen, click **Install**.

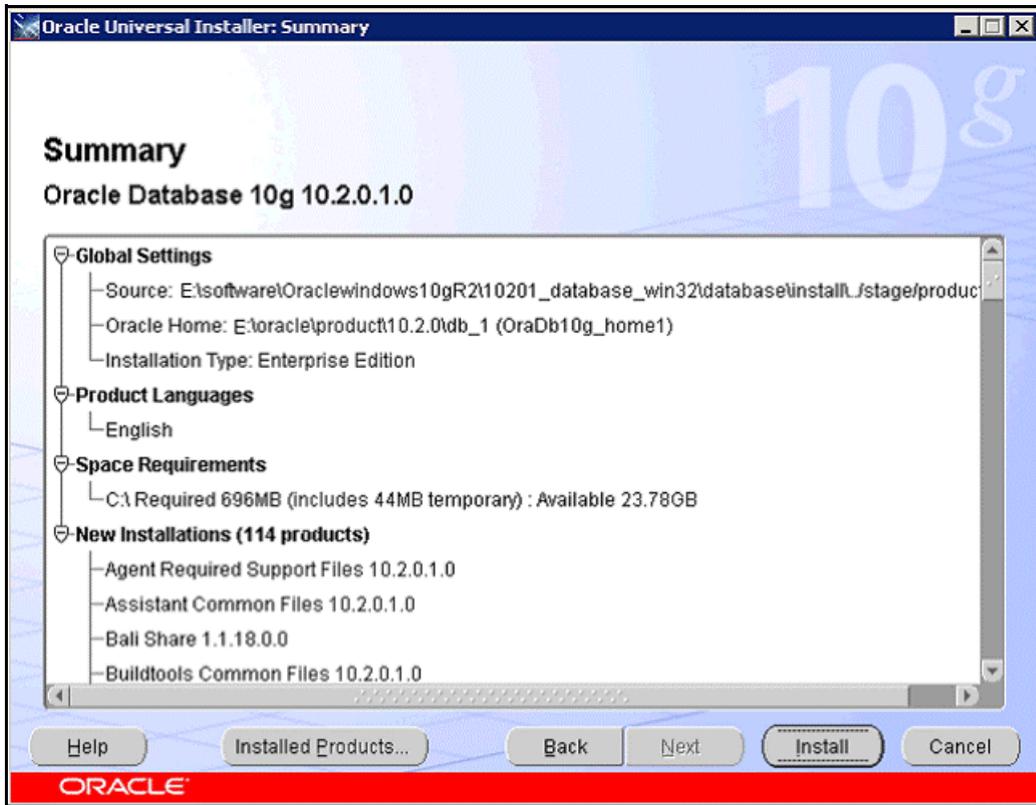


Figure 3. Summary screen

The Database Configuration Assistant screen starts.

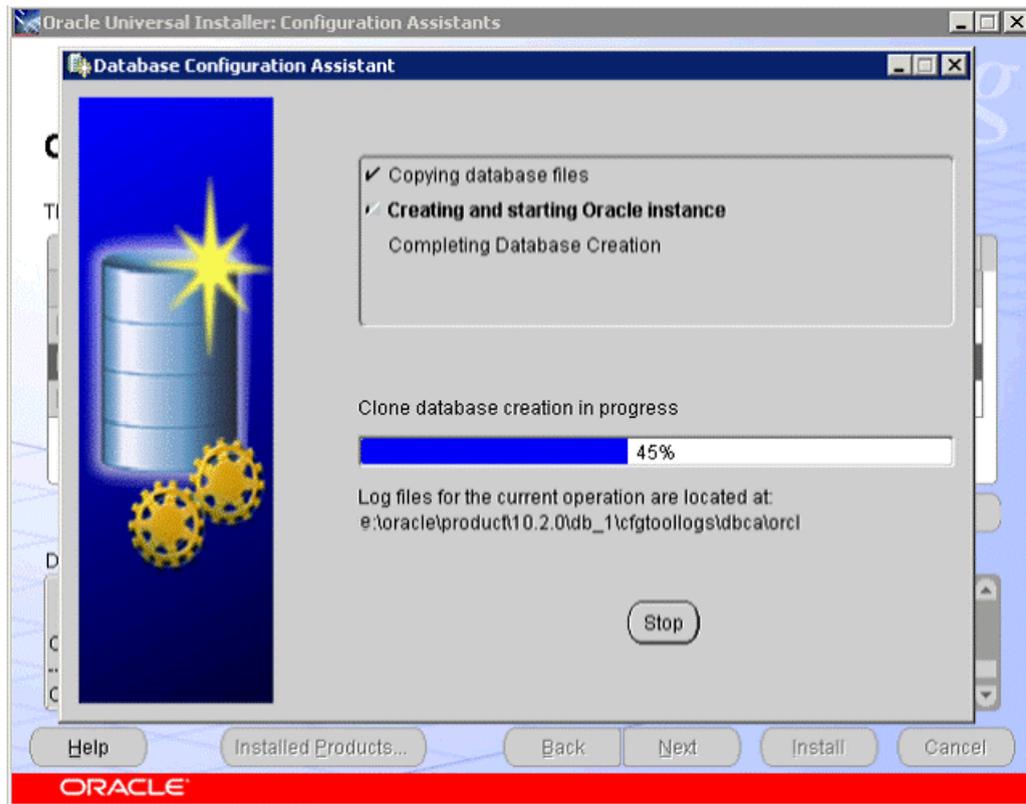


Figure 4. Database Configuration Assistant

___ 4. The End of Installation screen is displayed. Click **Exit**.

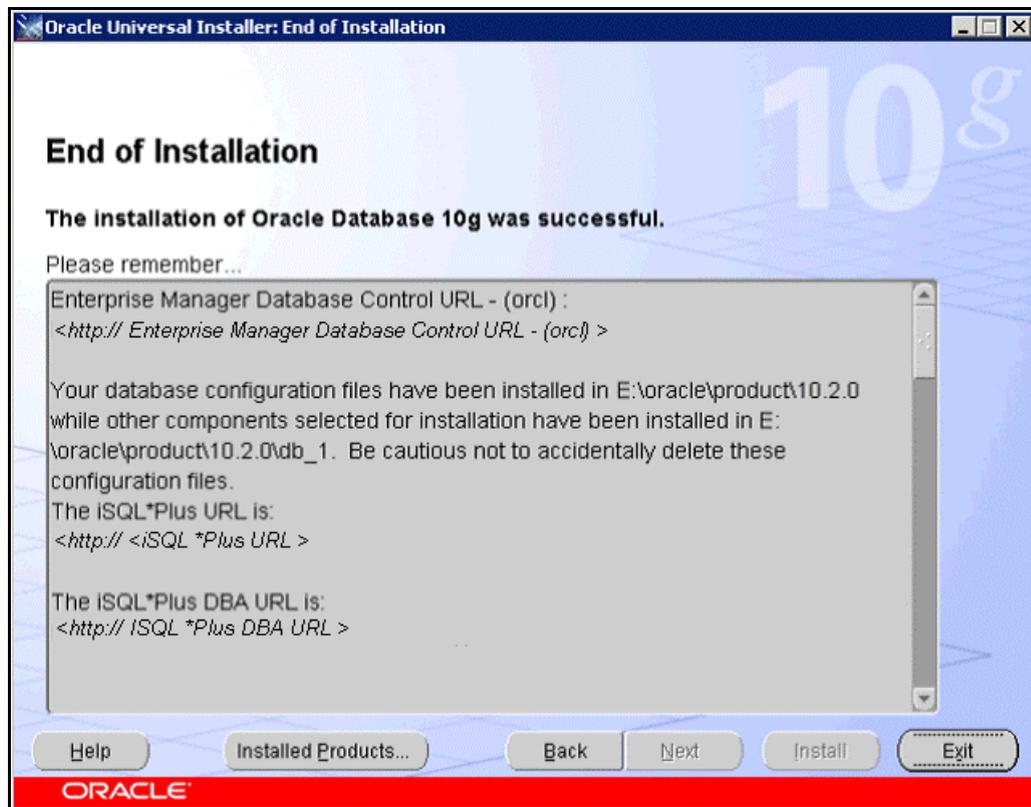


Figure 5. End of Installation screen

___ 5. Apply the 10.2.0.5 fix pack for Oracle.

Preparing to configure the LDAP directory

Determine which Lightweight Directory Access Protocol (LDAP) attributes you want to use as the identifiers for IBM® Connections users.



Note

Ensure that you installed a supported LDAP directory.

To ensure that the Profiles population wizard can return the maximum number of records from your LDAP directory, set the Size Limit parameter in your LDAP configuration to match the number of users in the directory. For example, if your directory has 100,000 users, set this parameter to 100000. For more information, see the documentation for your LDAP directory. If you cannot set the Size Limit parameter, you might run the wizard multiple times. Alternatively, you might write a JavaScript function to split the original LDAP search filter, then run the `collect_dns_iterate.bat` file, and finally run the `populate_from_dns_files.bat` file.

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

1. Identify LDAP attributes to use for the following roles. If no corresponding attribute exists, create one. You can use an attribute for multiple purposes. For example, you can use the mail attribute to perform the login and messaging tasks.

Display name: The `cn` LDAP attribute is used to display a person's name in the product user interface. Ensure that the value you use in the `cn` attribute is suitable for use as a display name.

Log in: Determine which attribute or attributes you want people to be able to use to log in to IBM Connections. For example: `uid`.



Note

The login name must be unique in the LDAP directory.

Messaging: Determine which attribute to use to define the email address of a person. The email address must be unique in the LDAP directory. If a person does not have an email address and does not have an LDAP attribute that represents the email address, that person cannot receive notifications.

Global unique identifier (GUID): Determine which attribute to use as the unique identifier of each person and group in the organization. This value must be unique across the organization.

2. Collect the following information about your LDAP directory before configuring it for WebSphere Application Server:
 - LDAP type: Domino 8.5.2.
 - LDAP host: `domino.ldap.example.com`.
 - Port: 389.
 - Bind user: `cn=Bind User,OU=Person,OU=SharedLDAP,OU=Lotus,o=ibm`.
 - Search base: `OU=SharedLDAP,OU=Lotus,o=ibm`.
 - Search user filter: `(&(uid=*)(objectclass=inetOrgPerson))`.

Installing Tivoli Directory Integrator 7.1 with FP5

Follow these steps to complete the installation of Tivoli Directory Integrator 7.1 with FP5:

- ___ 1. Open the Tivoli Directory Integrator.

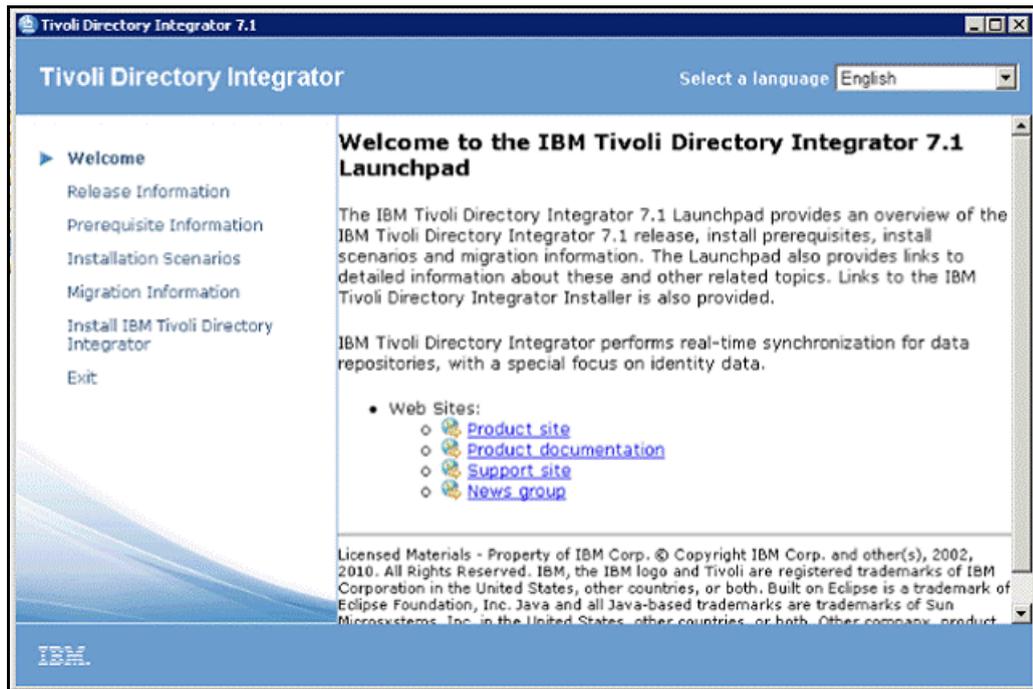


Figure 6. Tivoli Directory Integrator: Welcome screen

- ___ 2. Click **Install IBM Tivoli Directory Integrator**.

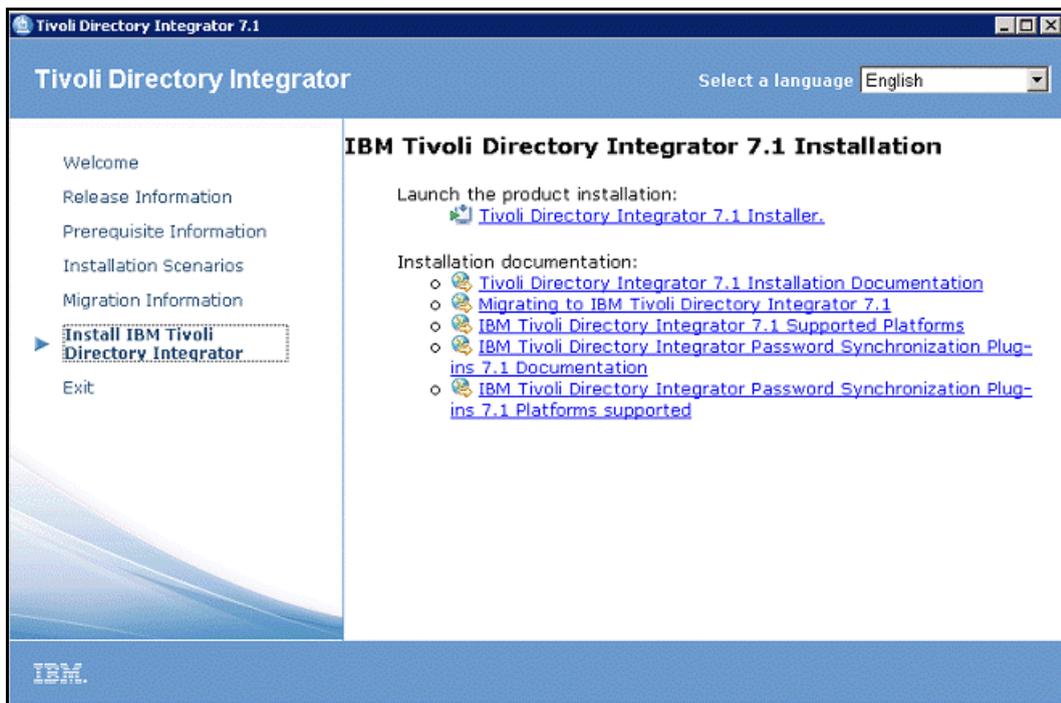


Figure 7. IBM Tivoli Directory Integrator 7.1: Installation screen

- ___ 3. The Directory Integrator 7.1 opens. Click **OK**.

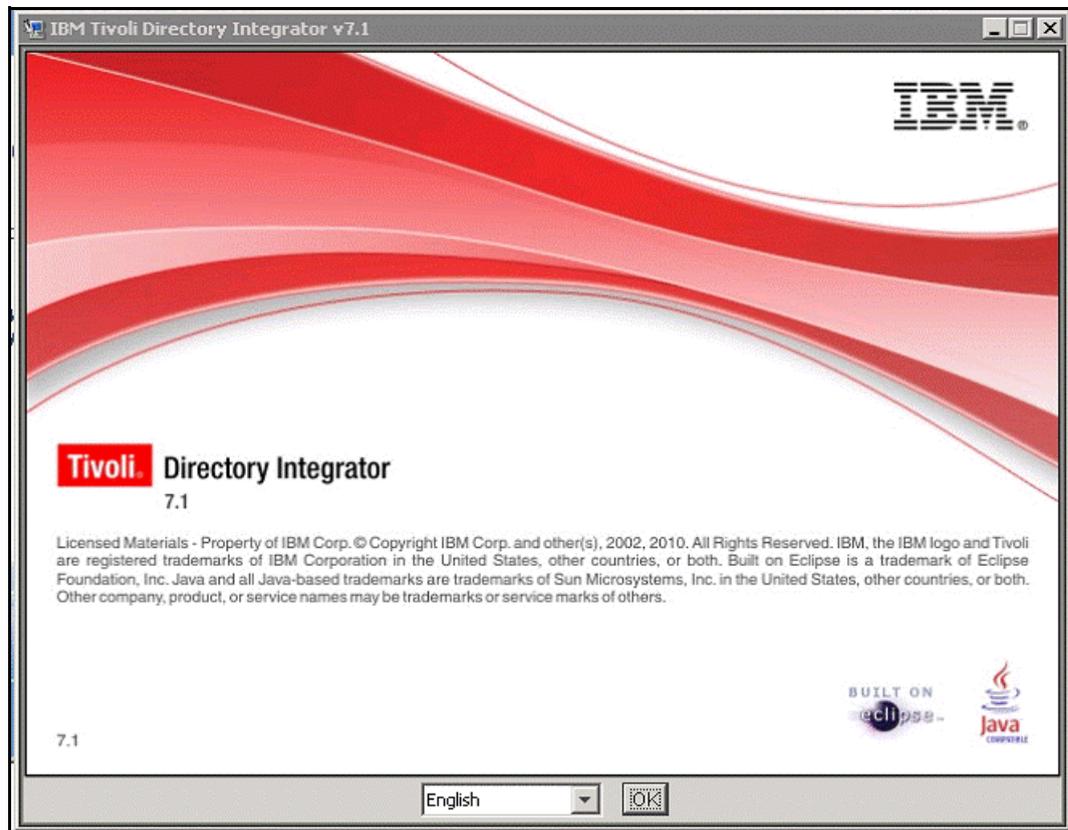


Figure 8. Directory Integrator 7.1: Wizard

4. In the Introduction screen, click **Next**.

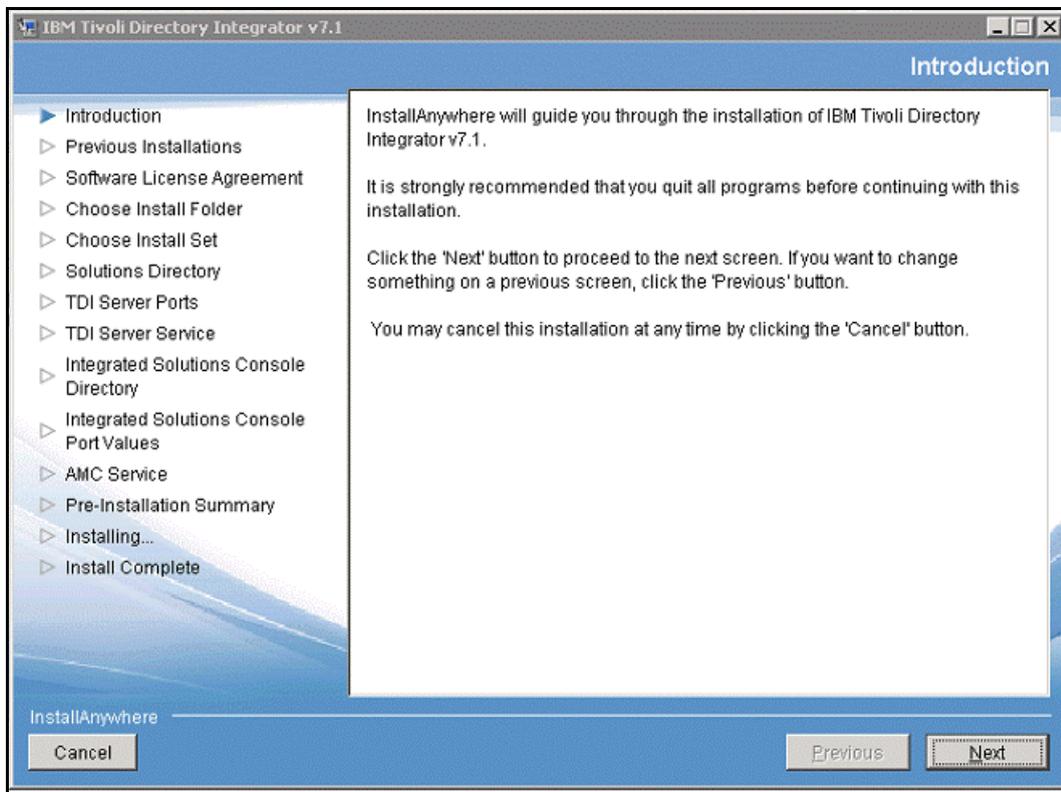


Figure 9. IBM Tivoli Directory Integrator 7.1 installation wizard: Introduction screen

- ___ 5. When the IBM Tivoli Directory Integrator finishes searching previous installations, click **Next**.

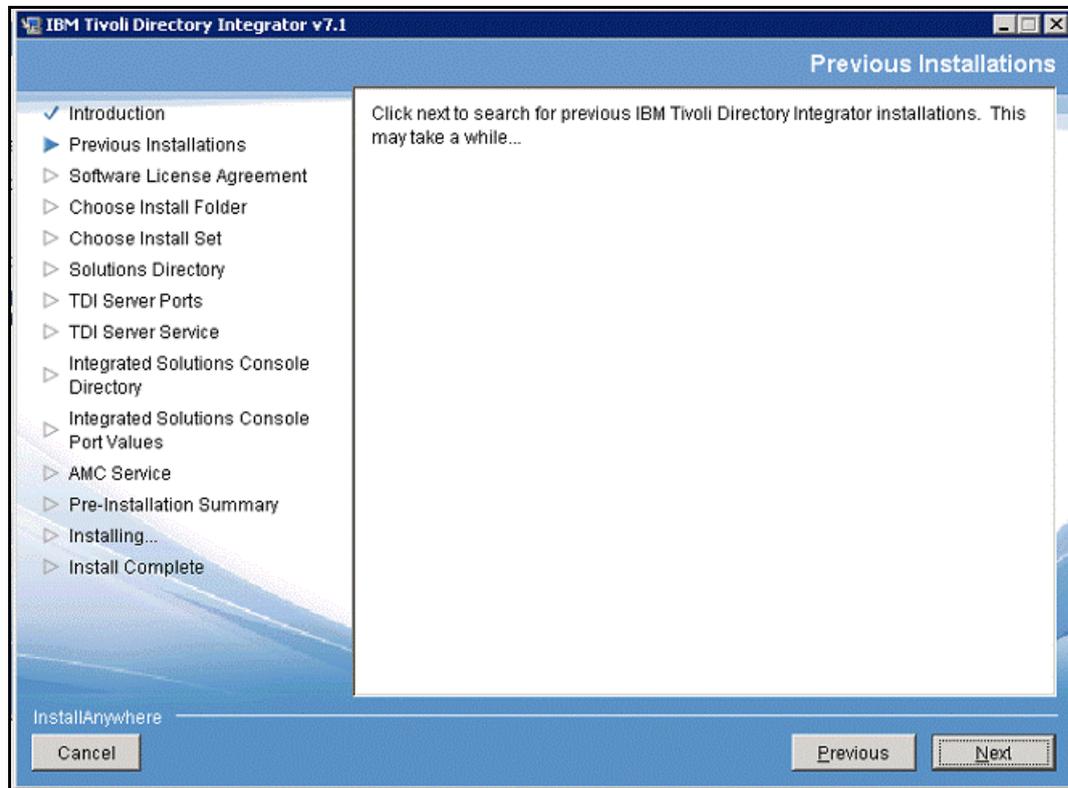


Figure 10. IBM Tivoli Directory Integrator 7.1 installation wizard: Previous installations screen

___ 6. Accept the terms in the license agreement and click **Next**.

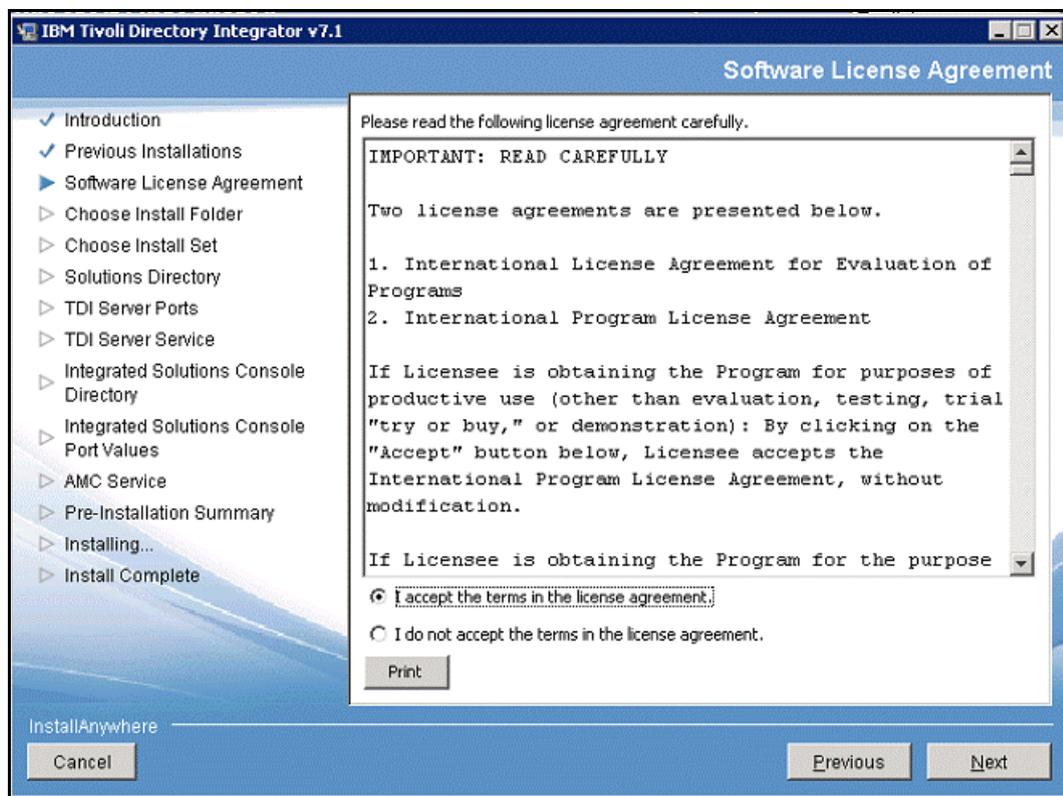


Figure 11. IBM Tivoli Directory Integrator 7.1 installation wizard: Software License Agreement screen

- ___ 7. Look for the path in which you want to install the IBM Tivoli Integrator 7.1 and click **Next**.

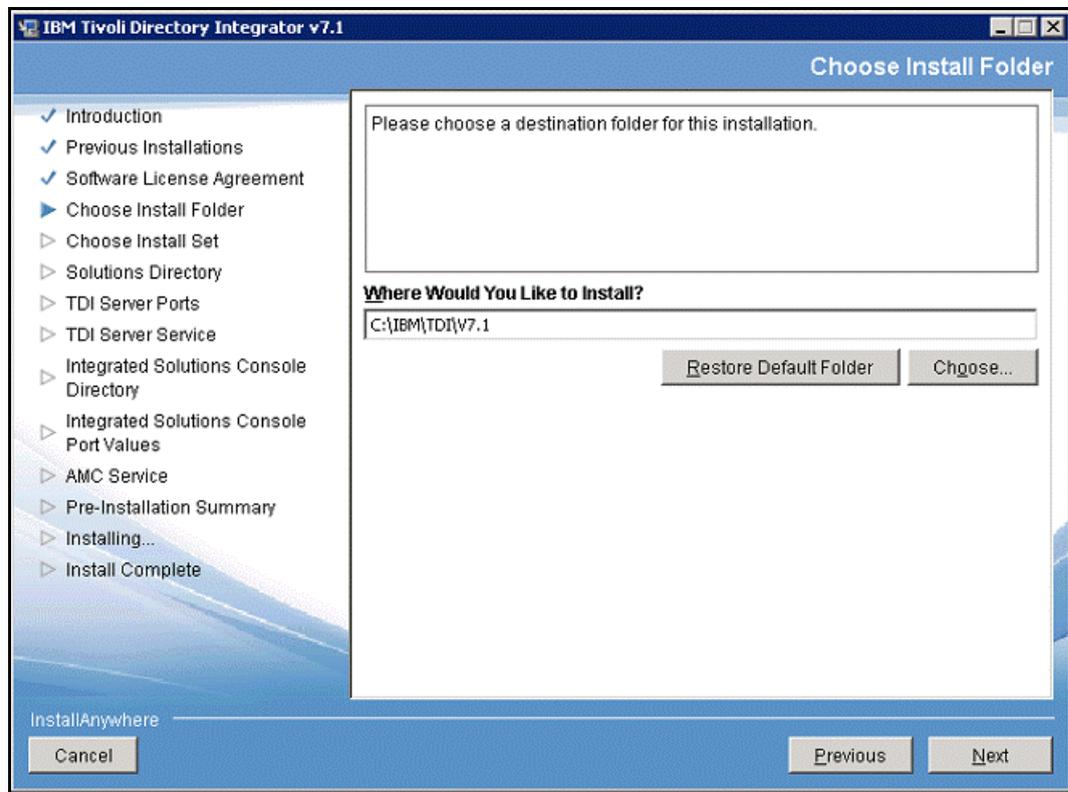


Figure 12. IBM Tivoli Directory Integrator 7.1 installation wizard: Choose Install Folder screen

8. Select **Typical** as the default installation method and click **Next**.

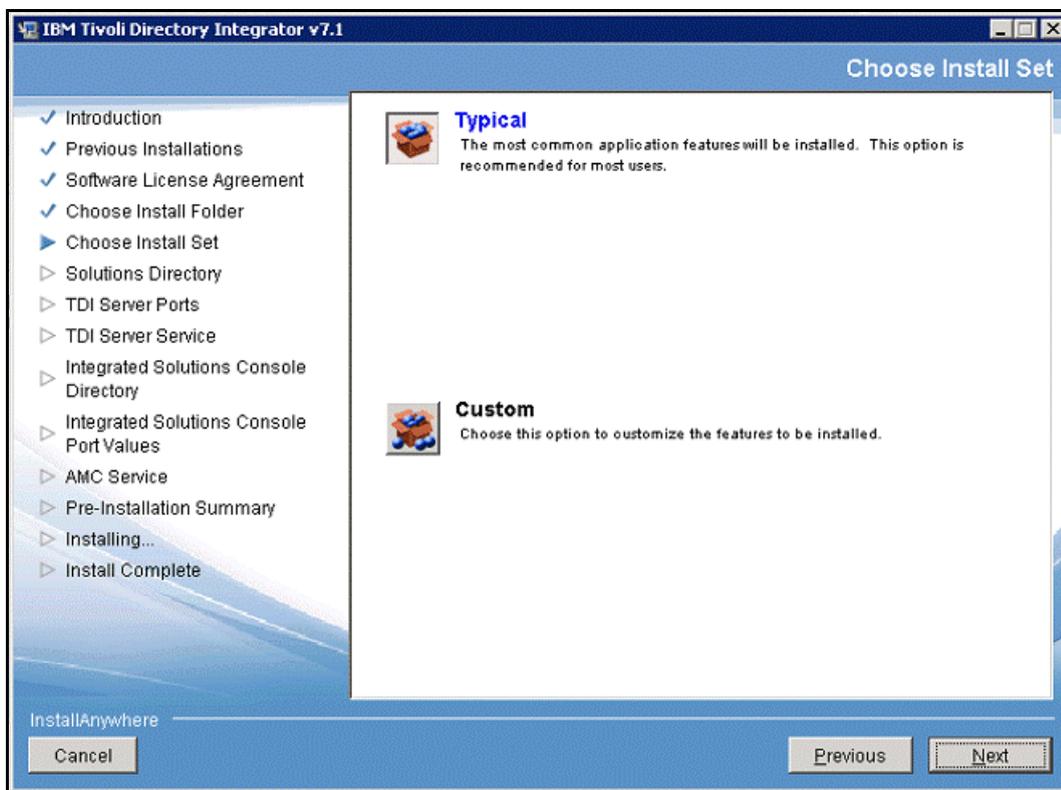


Figure 13. IBM Tivoli Directory Integrator 7.1 installation wizard: Choose Install Set screen

- ___ 9. Notice that the option “Use a subdirectory named Tivoli Directory Integrator under my home directory” is selected and click **Next**.

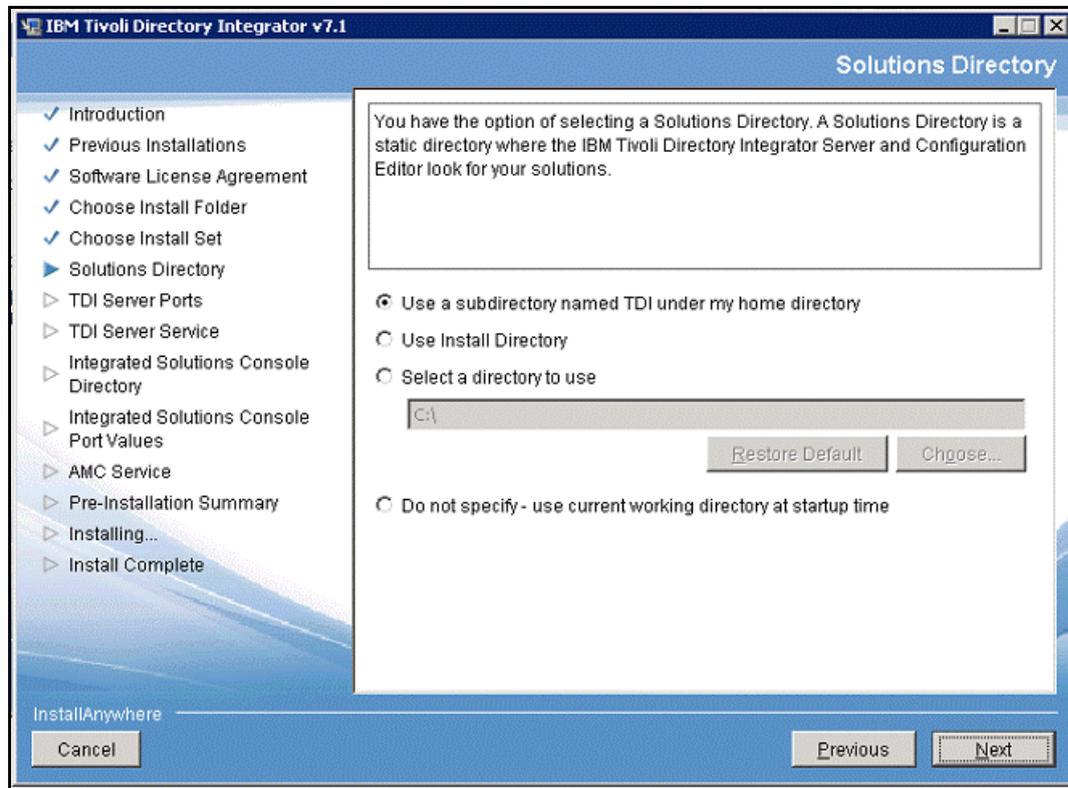


Figure 14. IBM Tivoli Directory Integrator 7.1 installation wizard: Solutions Directory screen

___ 10. Enter the port values as shown in the figure and click **Next**.

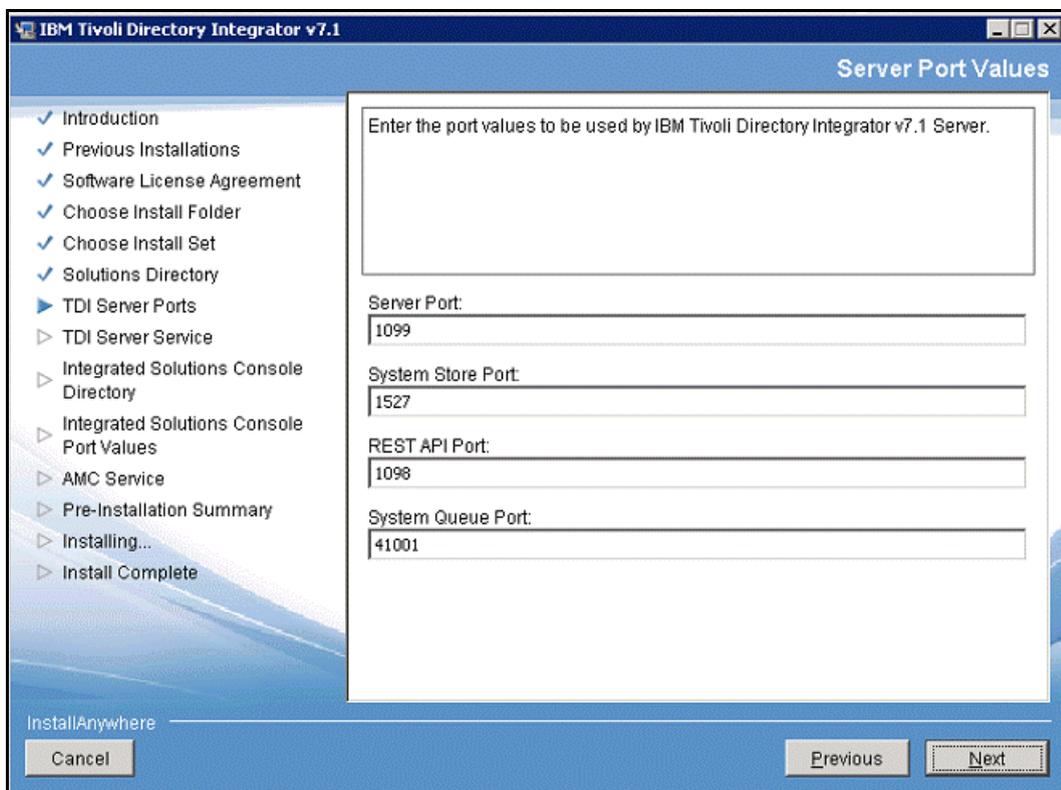


Figure 15. IBM Tivoli Directory Integrator 7.1 installation wizard: Server Port Values screen

- ___ 11. It is not necessary that you register IBM Tivoli Directory Integrator v7.1 as a system service. Click **Next**.

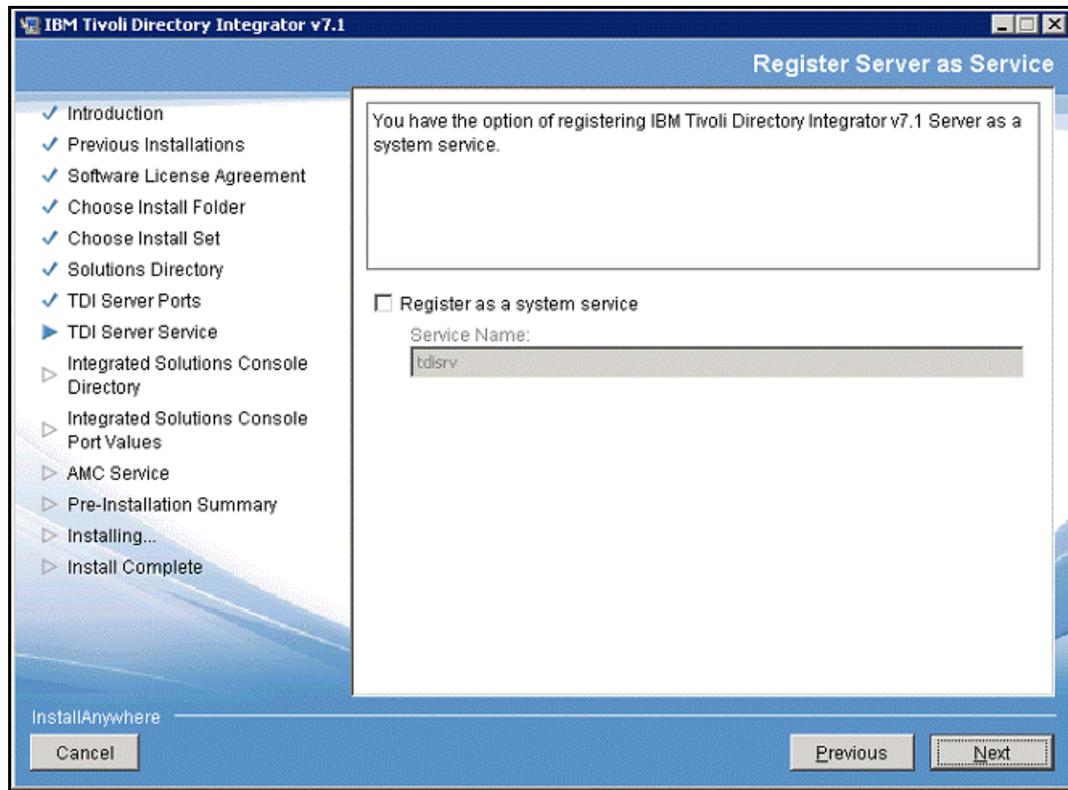


Figure 16. IBM Tivoli Directory Integrator 7.1 installation wizard: Register Server as Service screen

- ___ 12. Enter the port values for Integrated Solutions Console SE to use as shown in the figure and click **Next**.

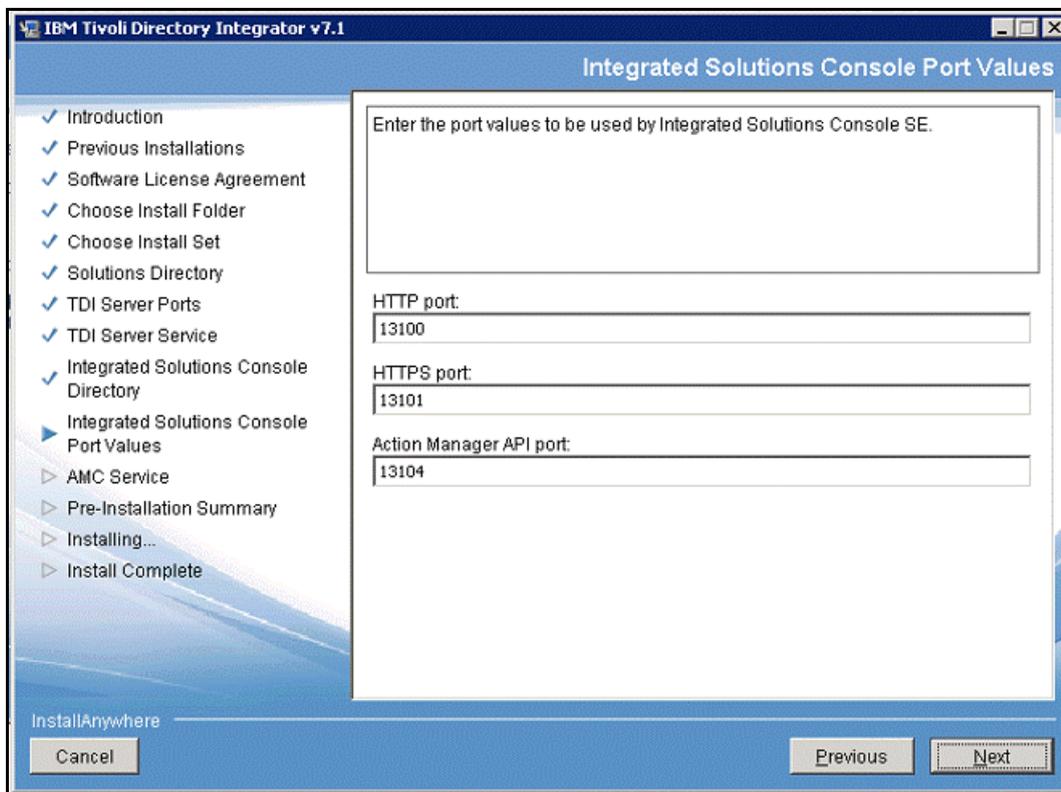


Figure 17. IBM Tivoli Directory Integrator 7.1 installation wizard: Integrated Solutions Console Port Values screen

- ___ 13. It is not necessary that you register the Administration and Monitoring Console as a system service. Click **Next**.

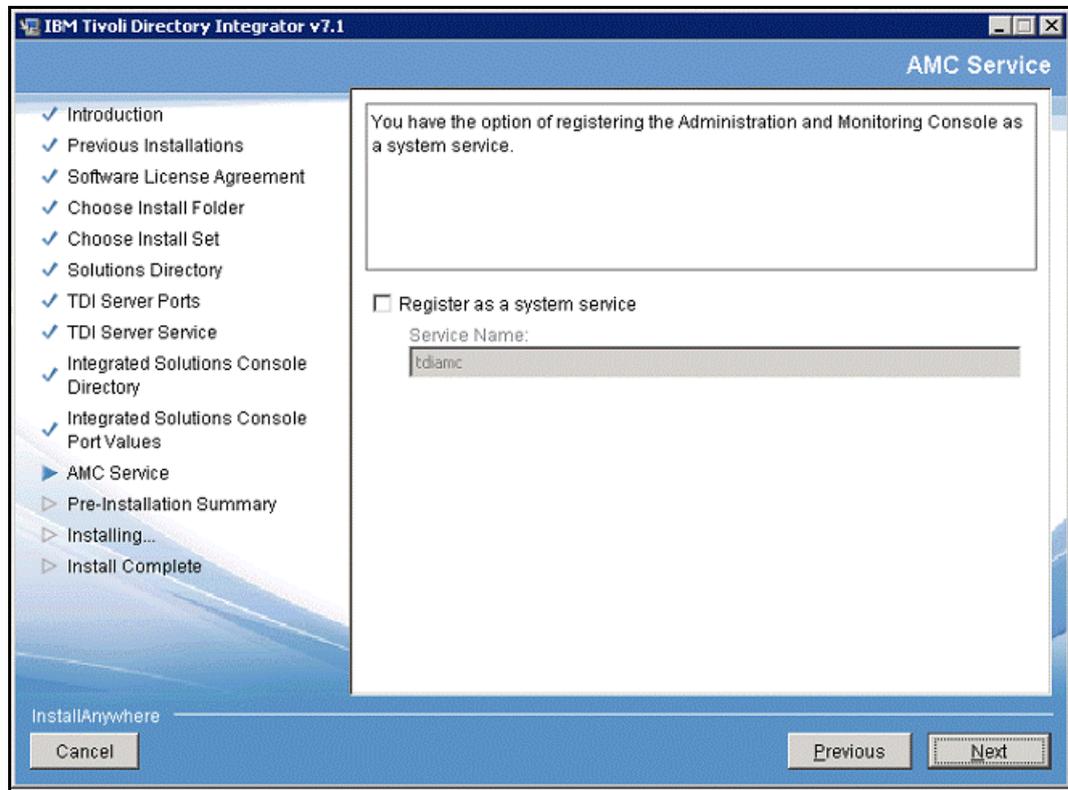


Figure 18. IBM Tivoli Directory Integrator 7.1 installation wizard: AMC Service screen

14. Check the pre-installation summary information and click **Install**.

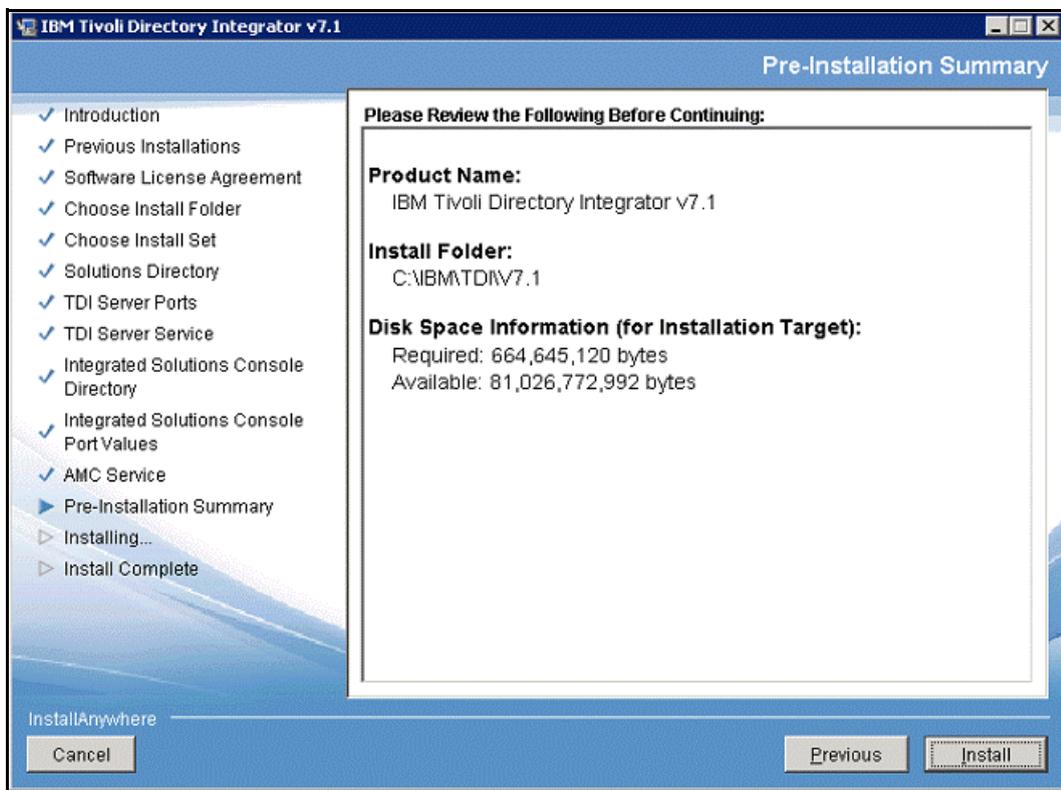


Figure 19. IBM Tivoli Directory Integrator 7.1 installation wizard: Pre-installation Summary screen

The IBM Tivoli Directory Integrator v7.1 starts installing.

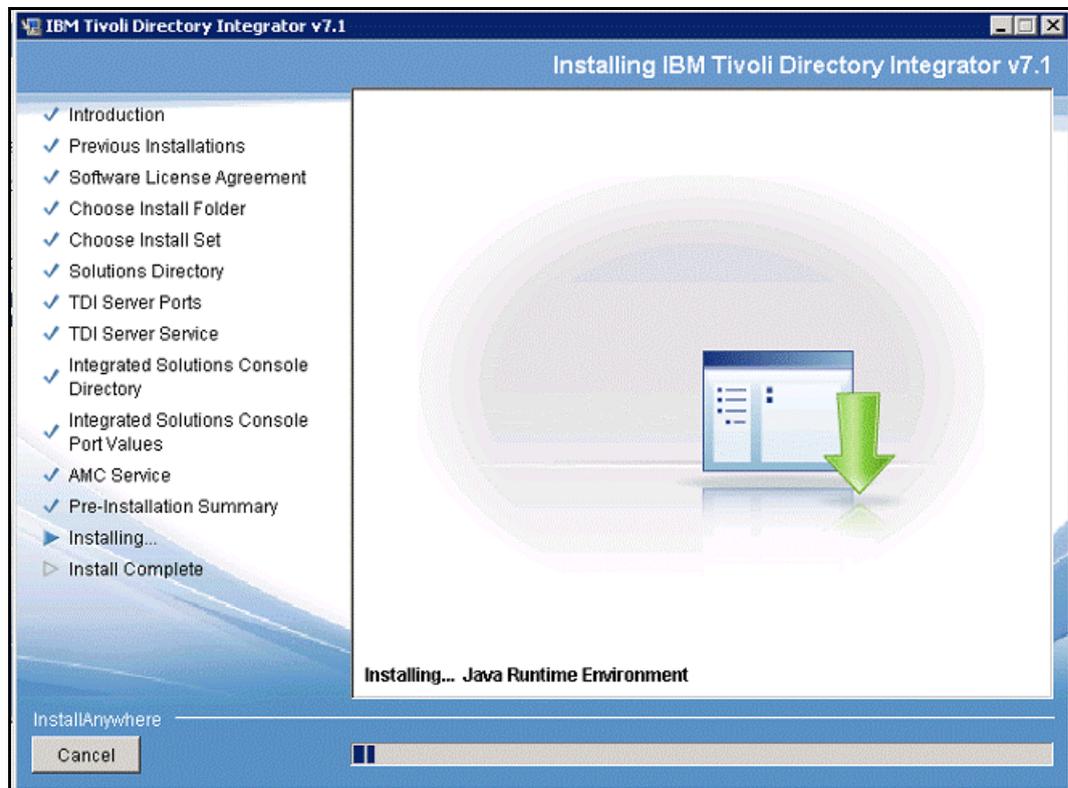


Figure 20. IBM Tivoli Directory Integrator 7.1 installation wizard: Installing IBM Tivoli Directory Integrator v7.1 screen

___ 15. When the installation is completed, click **Done**.

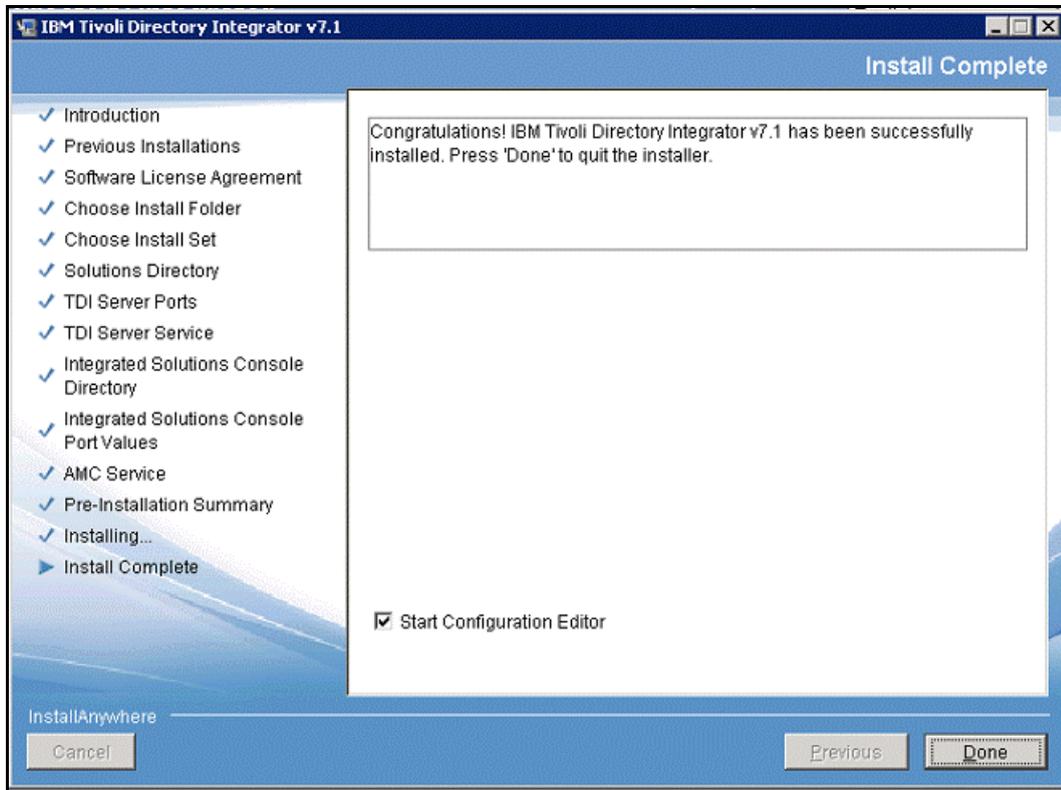


Figure 21. IBM Tivoli Directory Integrator 7.1 installation wizard: Install Complete screen

___ 16. To apply FP5 to Tivoli Directory Integrator 7.1, extract the 7.1.0-TIV-TDI-FP0005.zip, read the file 7.1.0-TIV-TDI-FP0005.README.html carefully to understand how to apply FP5. Here is the command that is used to apply FP5:

```
C:\IBM\TDI\U7.1\bin>applyUpdates.bat -update TDI-7.1-FP0005.zip
CTGDK0023I Applying fix 'TDI-7.1-FP0005' using backup directory 'C:\IBM\TDI\U7.1
\maintenance\BACKUP\TDI-7.1-FP0005'.
CTGDK0027I Updating SERVER.
CTGDK0027I Updating CE.
CTGDK0027I Updating EXAMPLES.
C:\IBM\TDI\U7.1\bin>
```

Figure 22. Command to apply FP5

Installing IBM WebSphere Application Server 7.0 and IBM HTTP Server 7.0 on Windows 2008

Installing Deployment Manager

Follow these steps to install the Deployment Manager:

1. Open **WebSphere Application Server Network Deployment**.

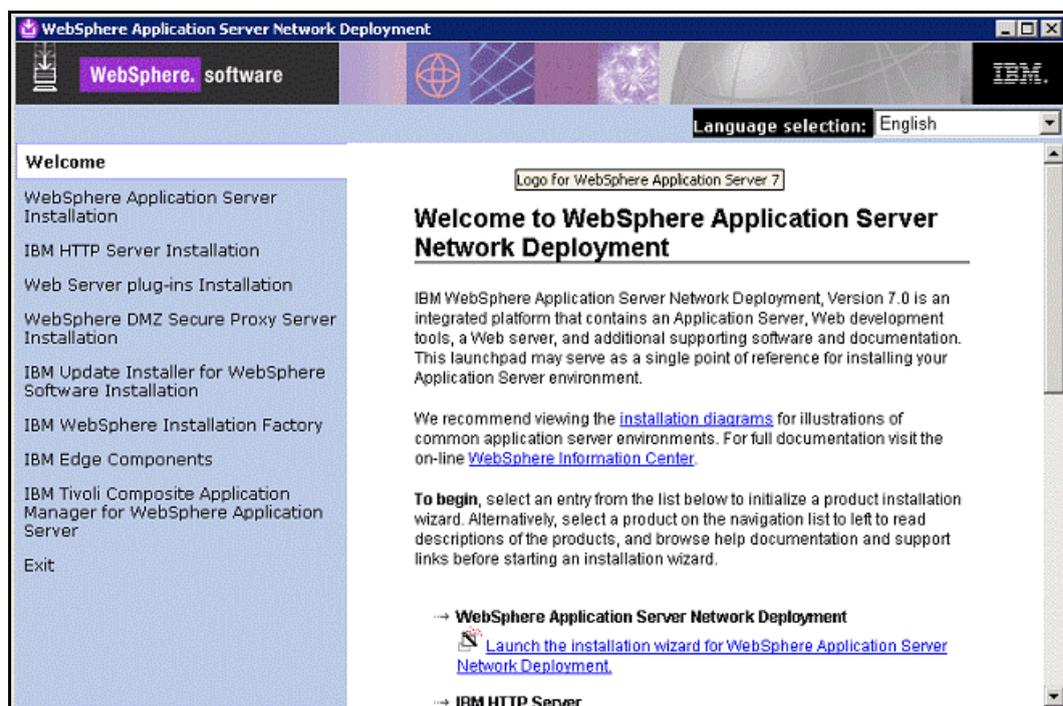


Figure 23. WebSphere Application Server Network Deployment

- ___ 2. Under Deployment Installation, click **Launch the installation wizard for the WebSphere Application Server Network Deployment**.

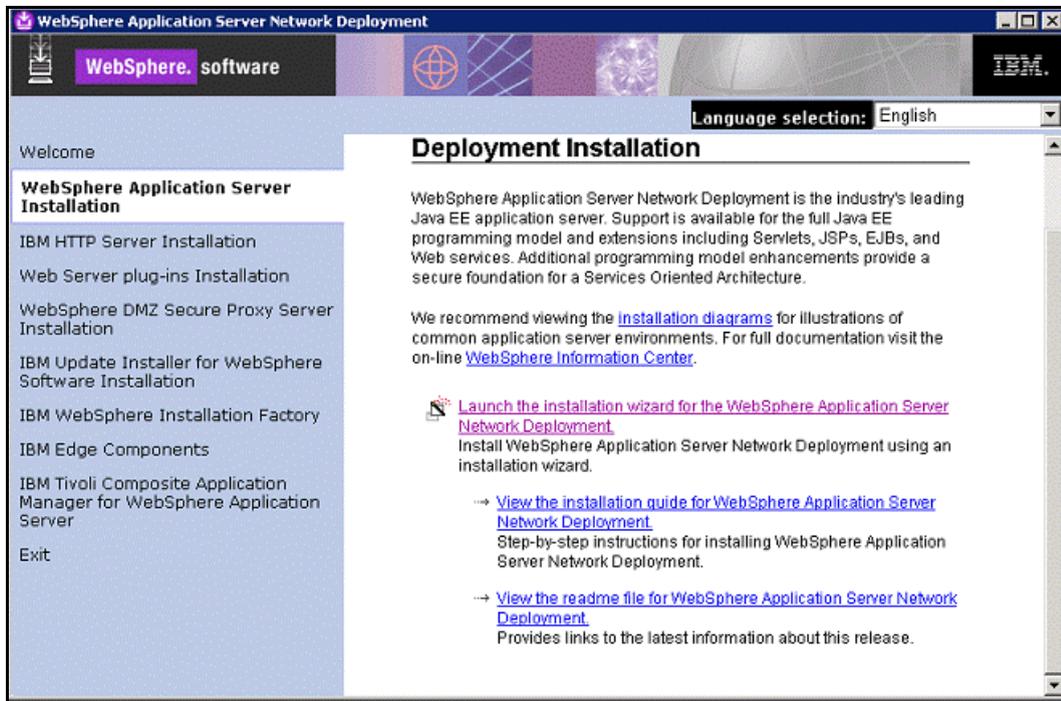


Figure 24. WebSphere Application Server Network Deployment: Deployment installation screen

- ___ 3. In the Welcome screen of the installation wizard, click **Next**.

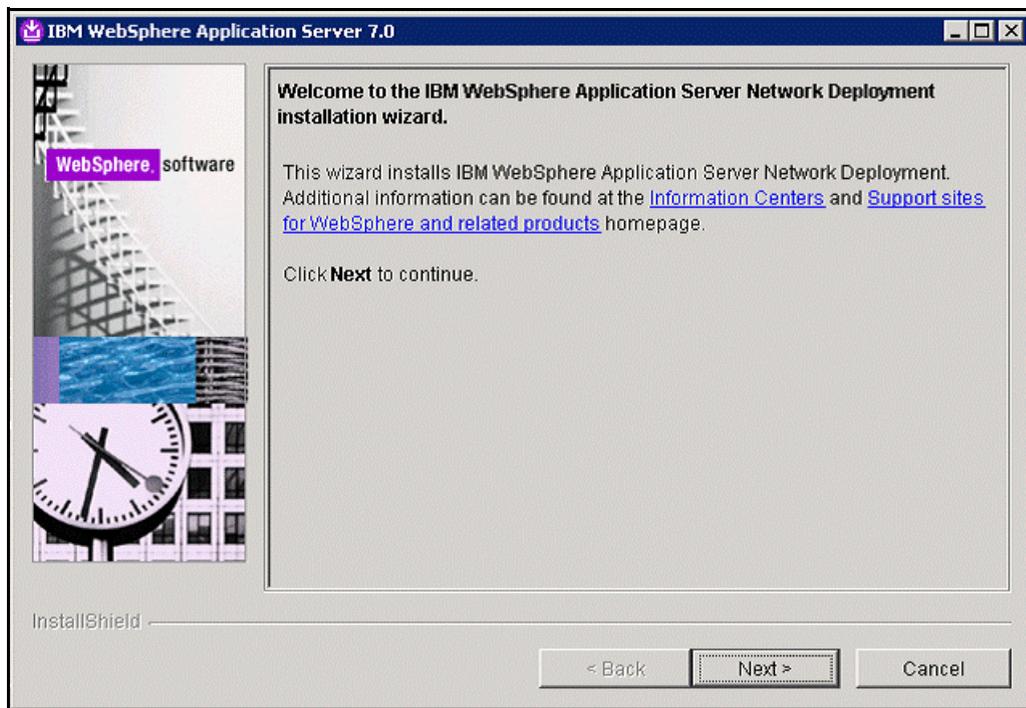


Figure 25. IBM WebSphere Application Server Network Deployment wizard

- ___ 4. Accept both the IBM and the non-IBM terms and click **Next**.

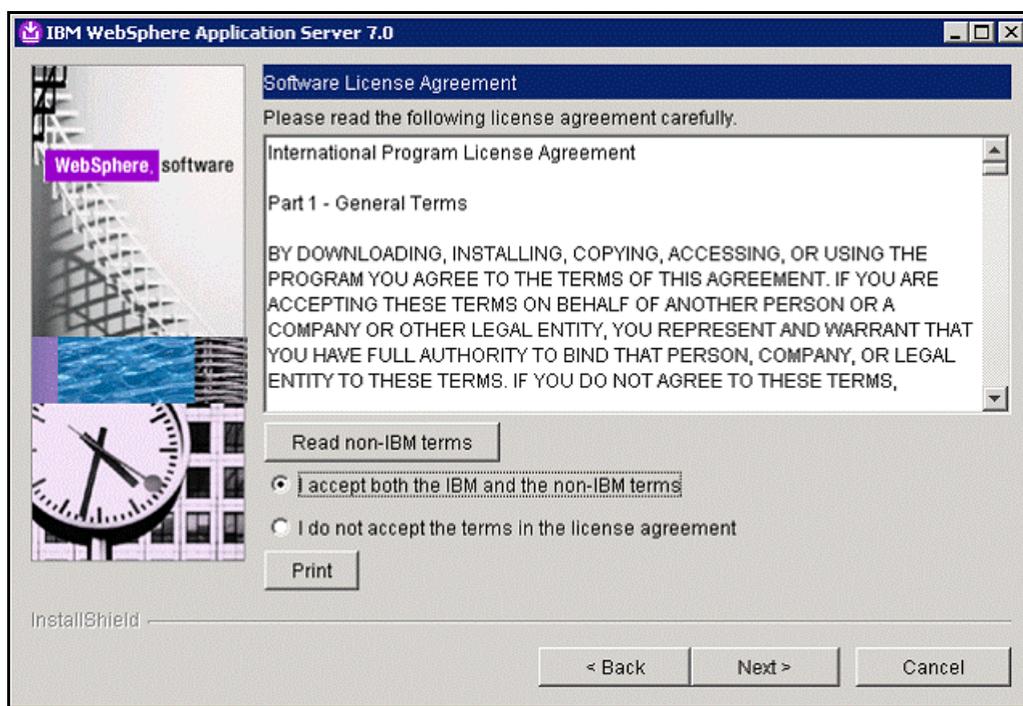


Figure 26. IBM WebSphere Application Server 7.0: Software License Agreement screen

- ___ 5. Notice that your operating system passed the prerequisites check. Click **Next**.

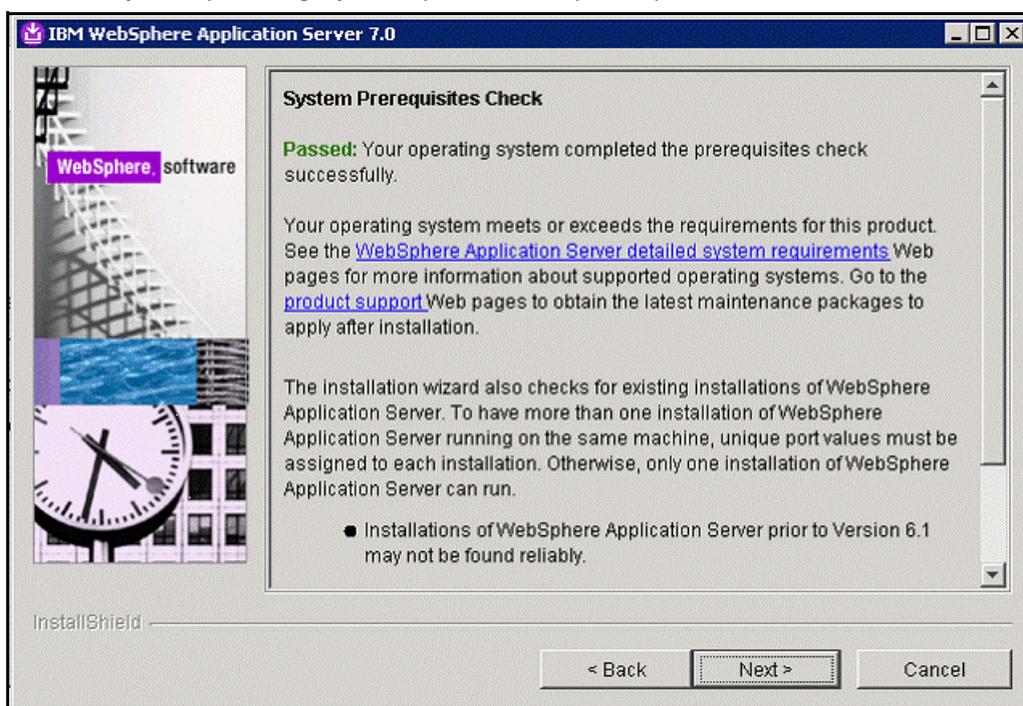


Figure 27. IBM WebSphere Application Server 7.0: System Prerequisites Check screen

6. You can optionally install optional features. Click **Next**.

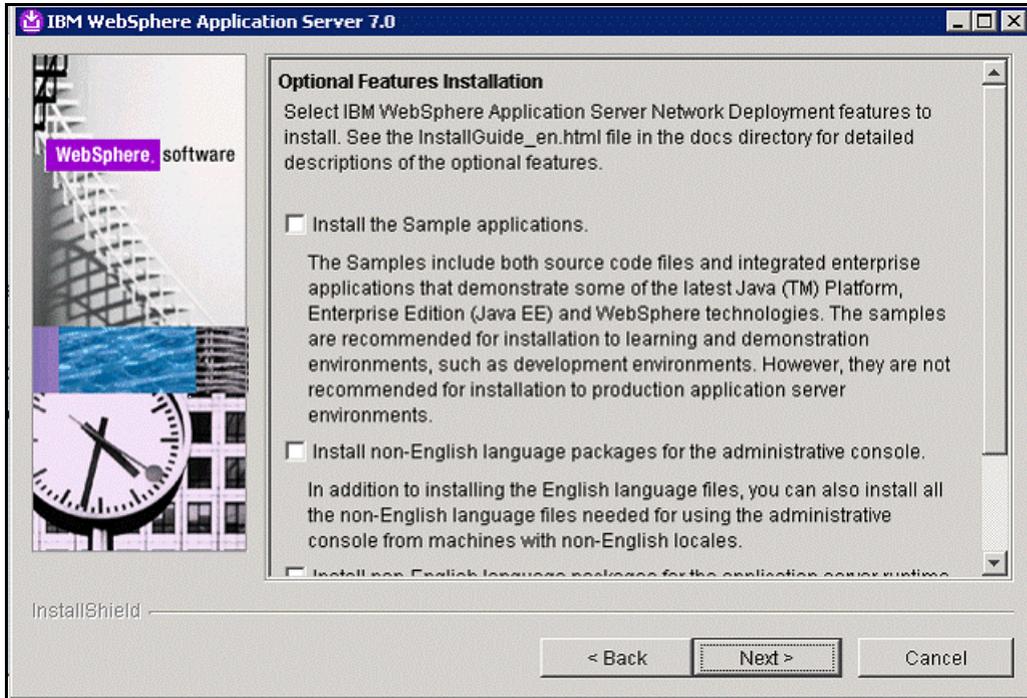


Figure 28. IBM WebSphere Application Server 7.0: Operational Features Installation screen

7. Specify the directory where you want to install the IBM WebSphere Application Server 7.0 and click **Next**.

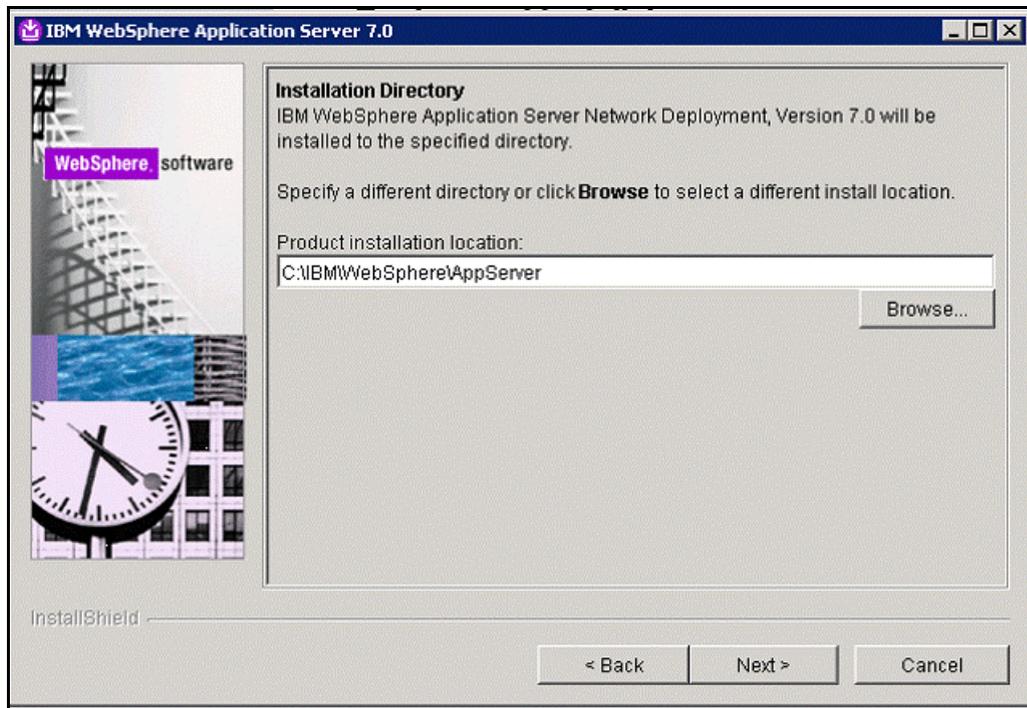


Figure 29. IBM WebSphere Application Server 7.0: Installation Directory screen

- ___ 8. Select **Management** as the WebSphere Application Server environment and click **Next**.

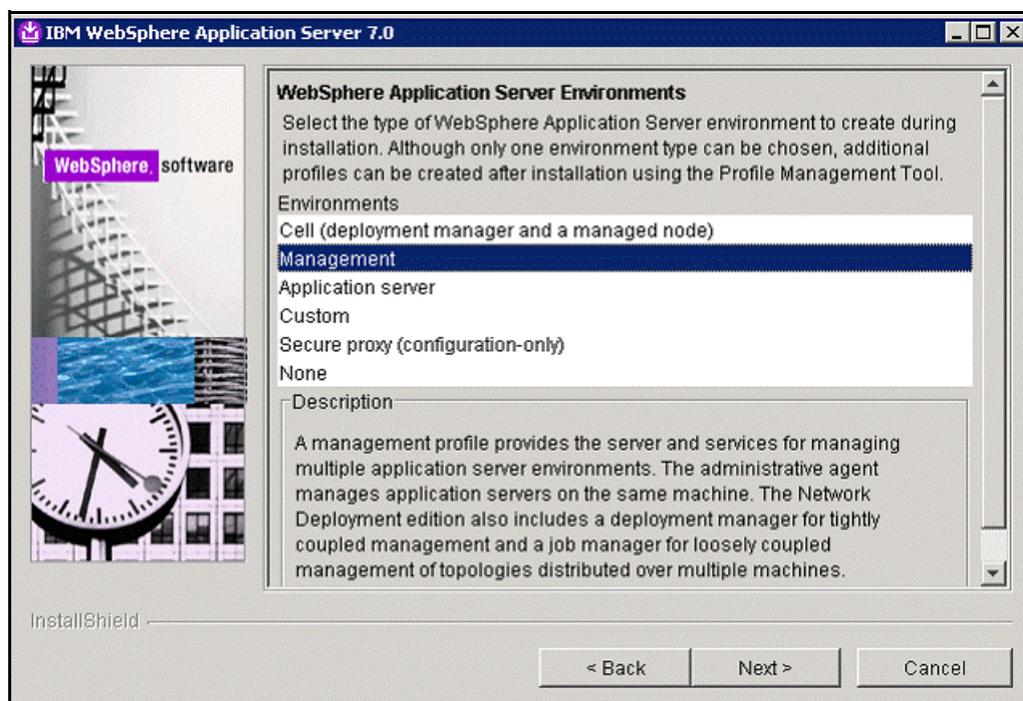


Figure 30. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments screen

- ___ 9. In the Server Type Selection screen, click **Deployment manager** and click **Next**.

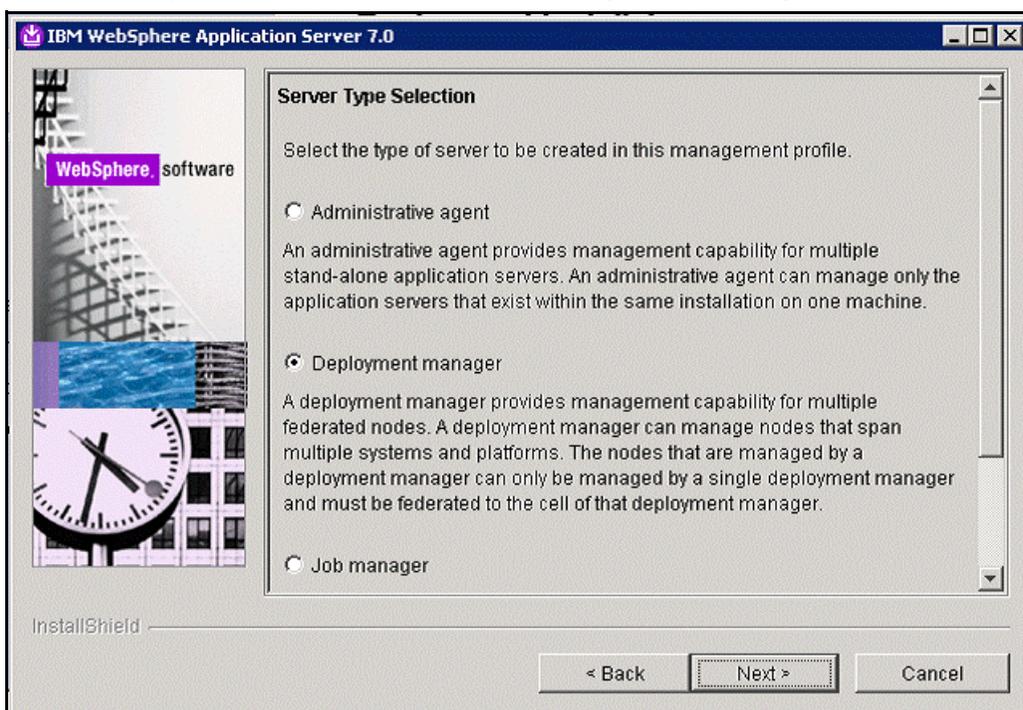


Figure 31. IBM WebSphere Application Server 7.0: Server Type Selection screen

___ 10. Select **Enable administrative security**, enter the user name and password, and click **Next**.



Figure 32. IBM WebSphere Application Server 7.0: Enable Administrative Security screen

___ 11. You can optionally create a repository for Centralized Installation Managers. Click **Next**.

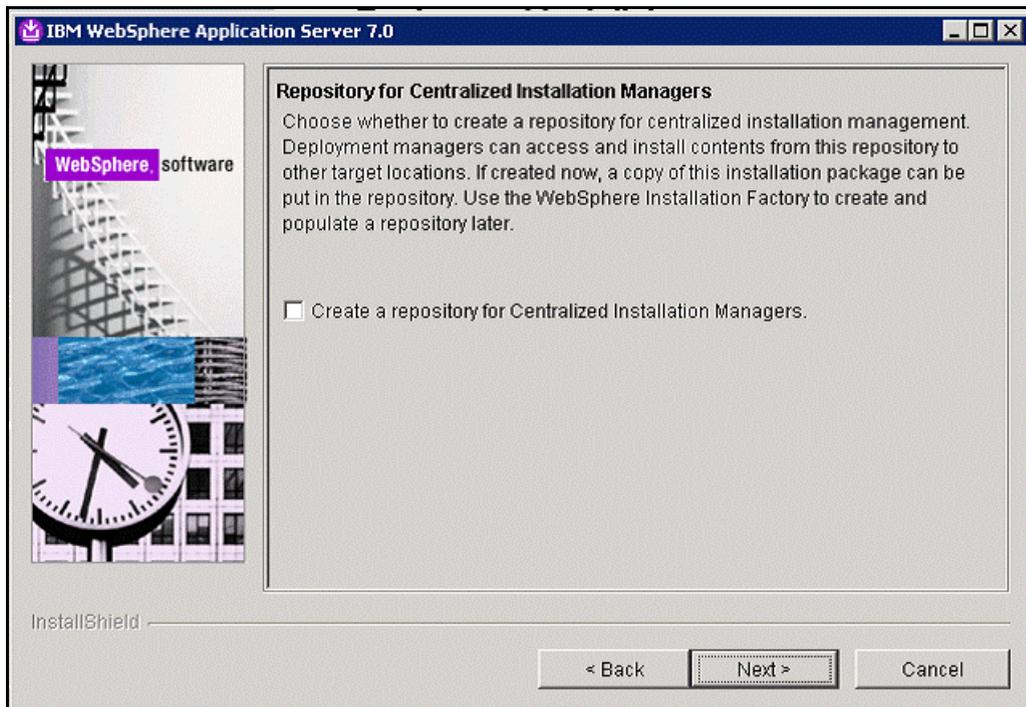


Figure 33. IBM WebSphere Application Server 7.0: Repository for Centralized Installation Managers screen

___ 12. Review the installation summary and click **Next**.

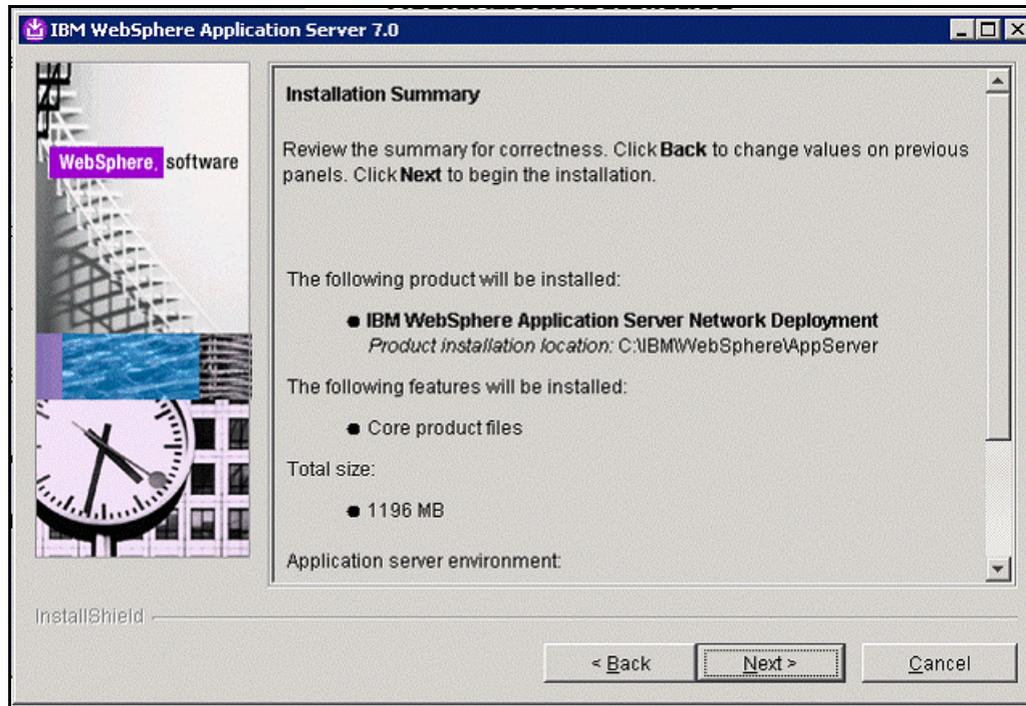


Figure 34. IBM WebSphere Application Server 7.0: Installation Summary screen

___ 13. Check the installation results and click **Finish**.

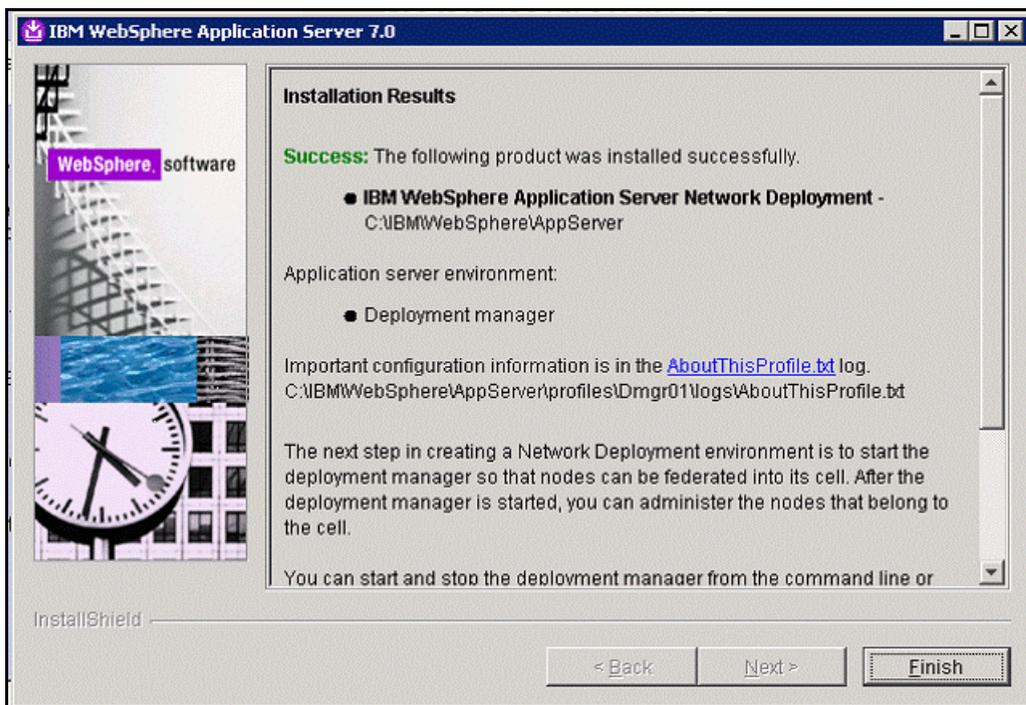


Figure 35. IBM WebSphere Application Server 7.0: Installation Results screen

Installing application server

To install the IBM WebSphere Application Server 7.0, follow these steps:

1. Open the IBM WebSphere Application Server Network Deployment installation wizard and click **Next**.

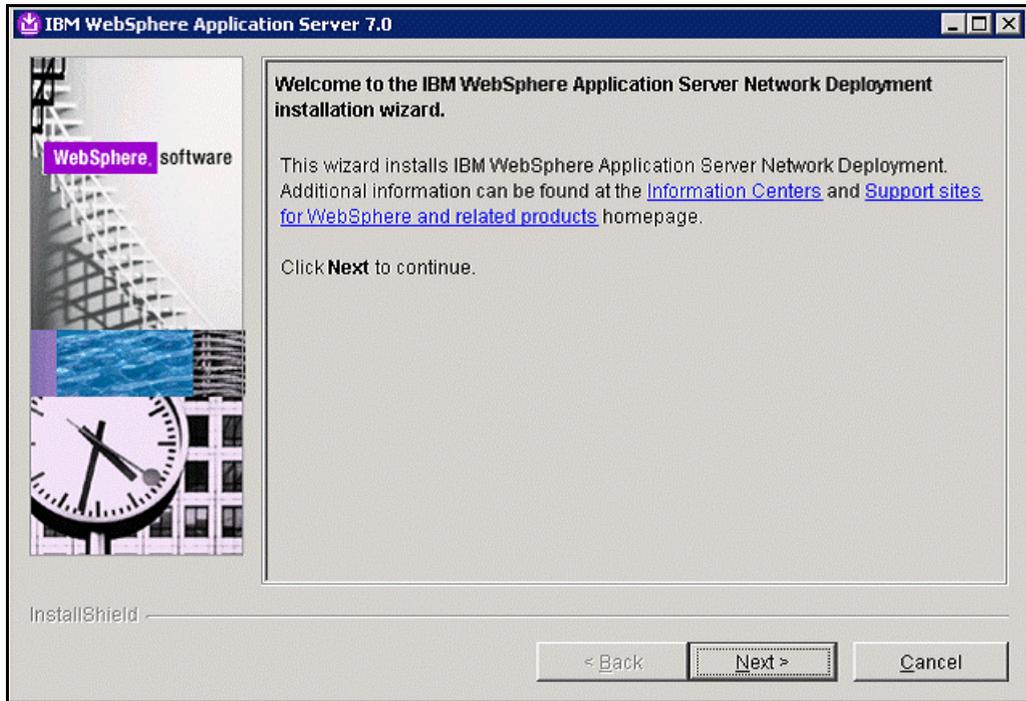


Figure 36. IBM WebSphere Application Server Network Deployment wizard

- ___ 2. In the Software License Agreement screen, accept both the IBM and non-IBM terms and click **Next**.

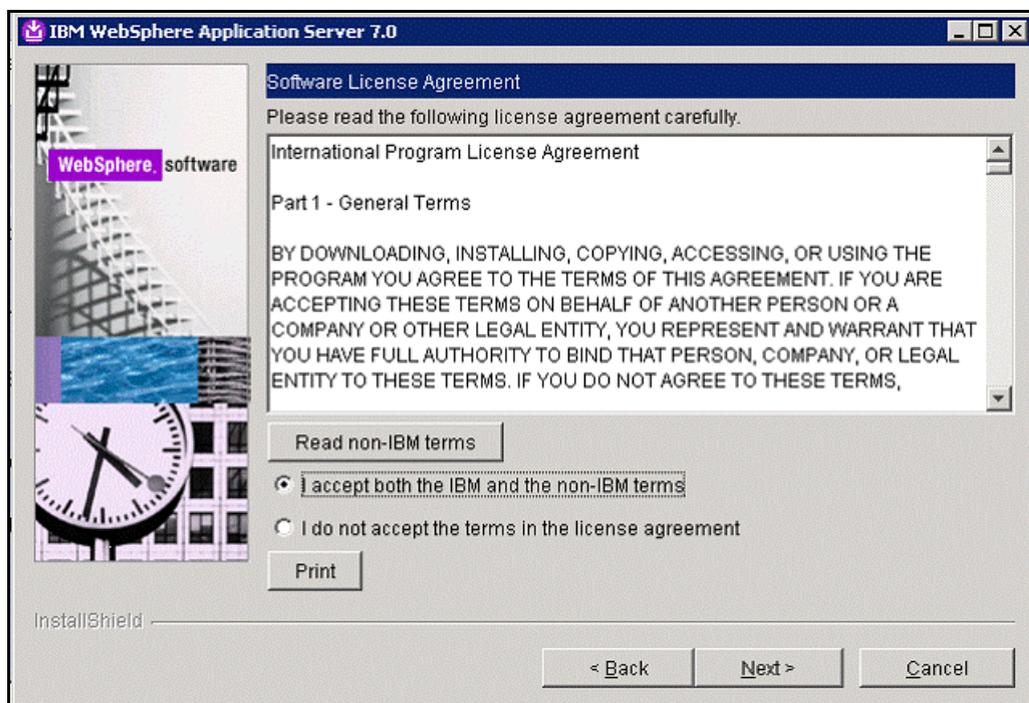


Figure 37. IBM WebSphere Application Server 7.0: Software License Agreement screen

- ___ 3. Notice that your operating system completed the prerequisites check. Click **Next**.

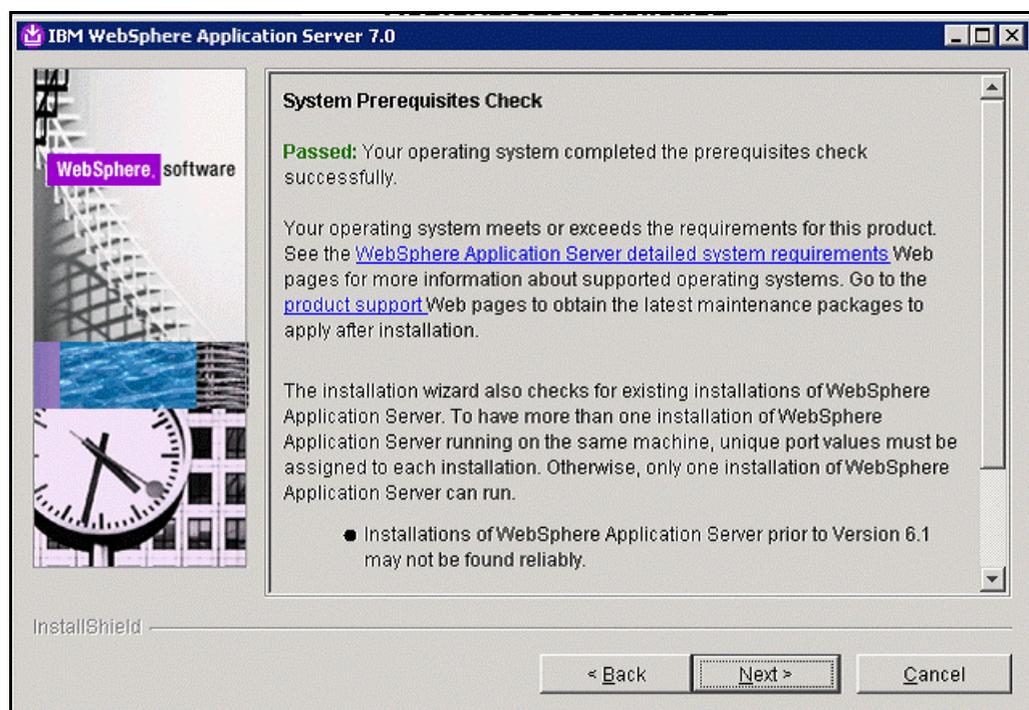


Figure 38. IBM WebSphere Application Server 7.0: System Prerequisites Check screen

4. Choose whether to install optional features. Click **Next**.

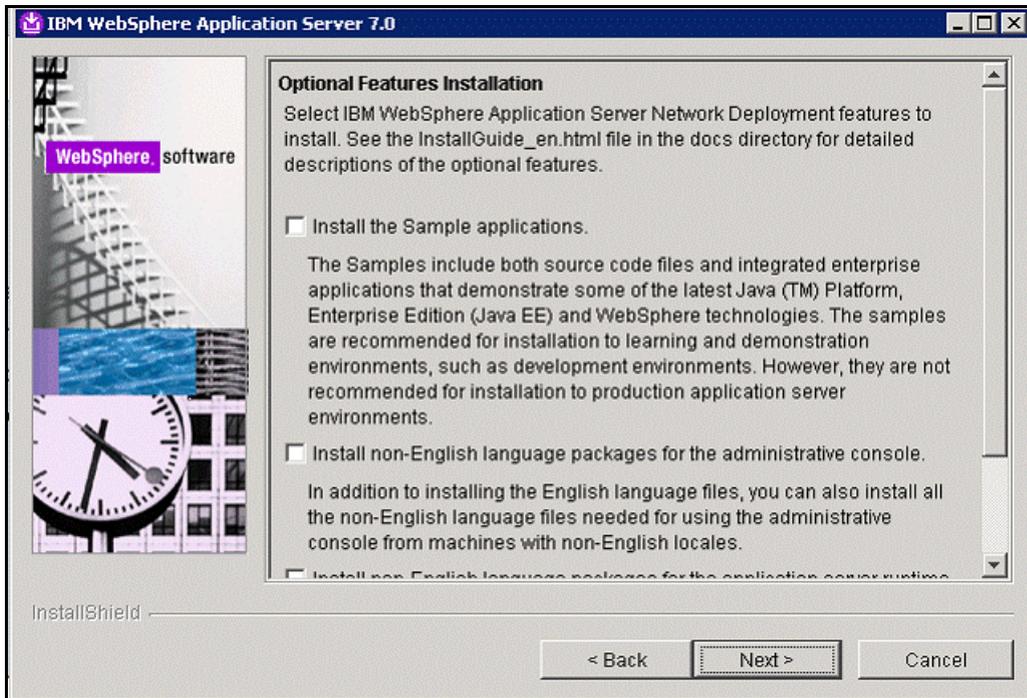


Figure 39. IBM WebSphere Application Server 7.0: Optional Features Installation screen

5. Specify the directory where you want to install the IBM WebSphere Application Server 7.0 and click **Next**.

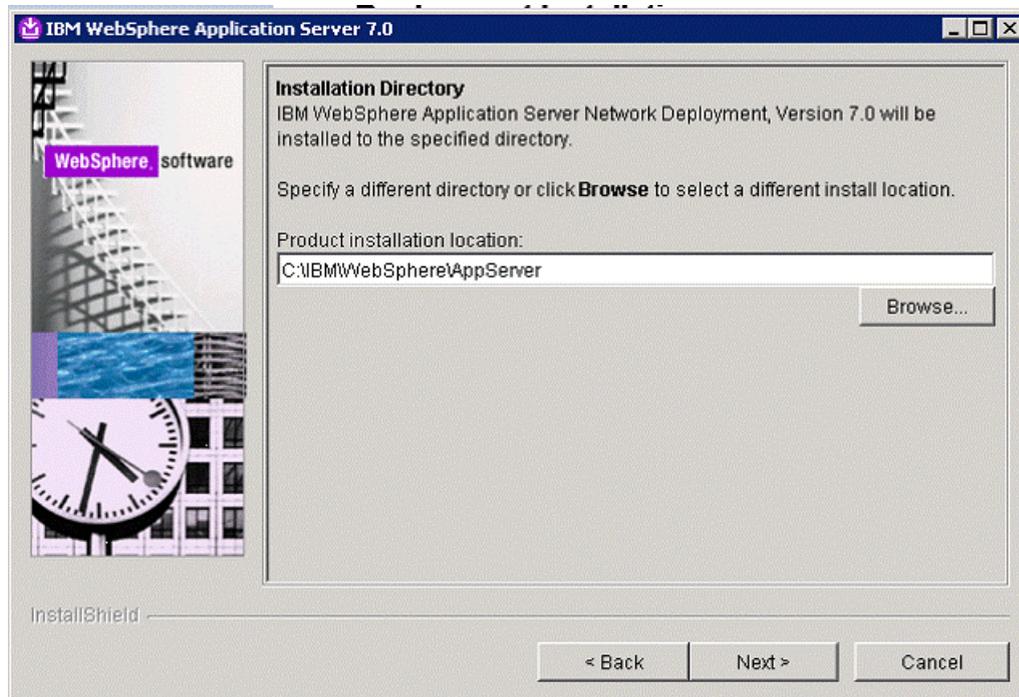


Figure 40. IBM WebSphere Application Server 7.0: Installation Directory screen

- ___ 6. Select **Application server** as the WebSphere Application Server environment and click **Next**.

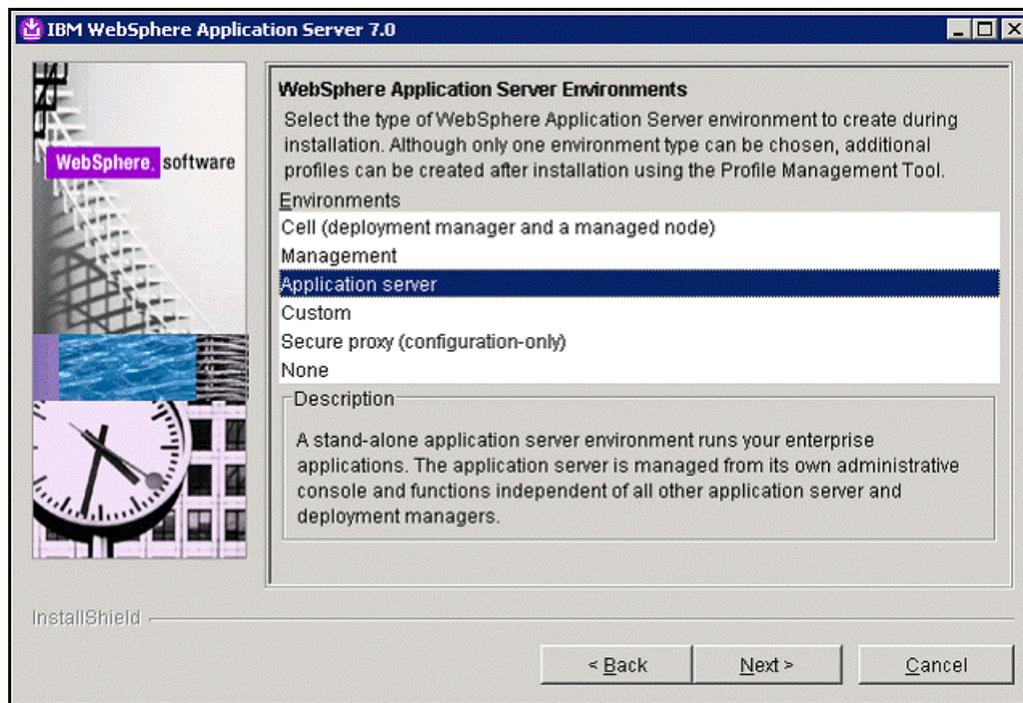


Figure 41. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments screen

- ___ 7. Select **Enable administrative security**, enter the user name and password, and click **Next**.



Figure 42. IBM WebSphere Application Server 7.0: Enable Administrative Security screen

8. Review the installation summary and click **Next**.

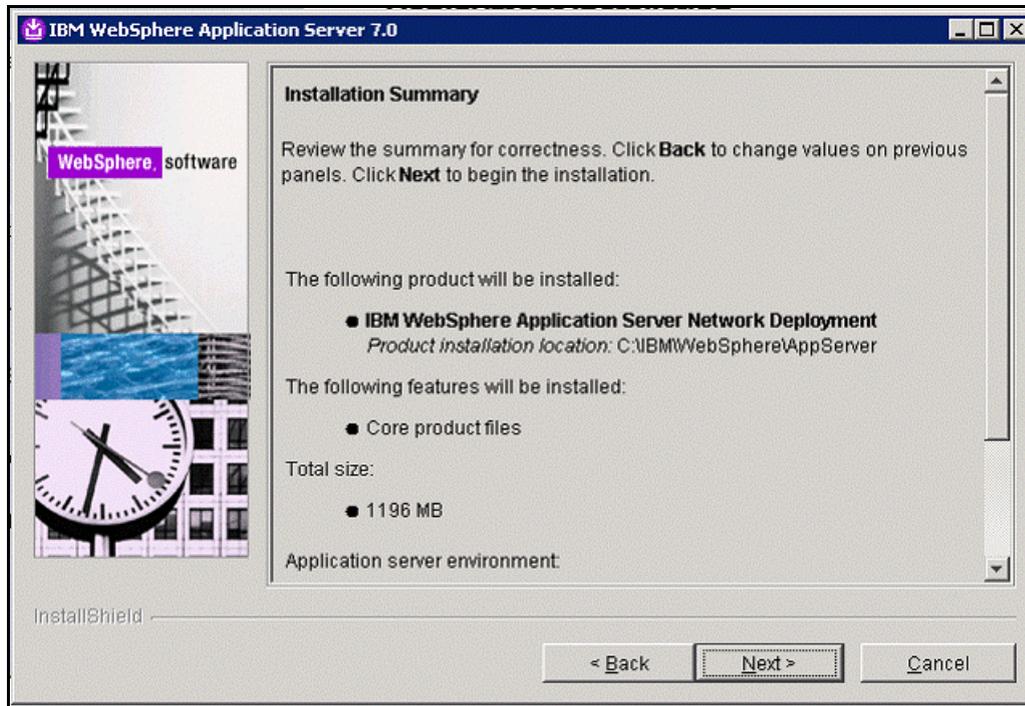


Figure 43. IBM WebSphere Application Server 7.0: Installation Summary screen

9. Check the installation results and click **Finish**.

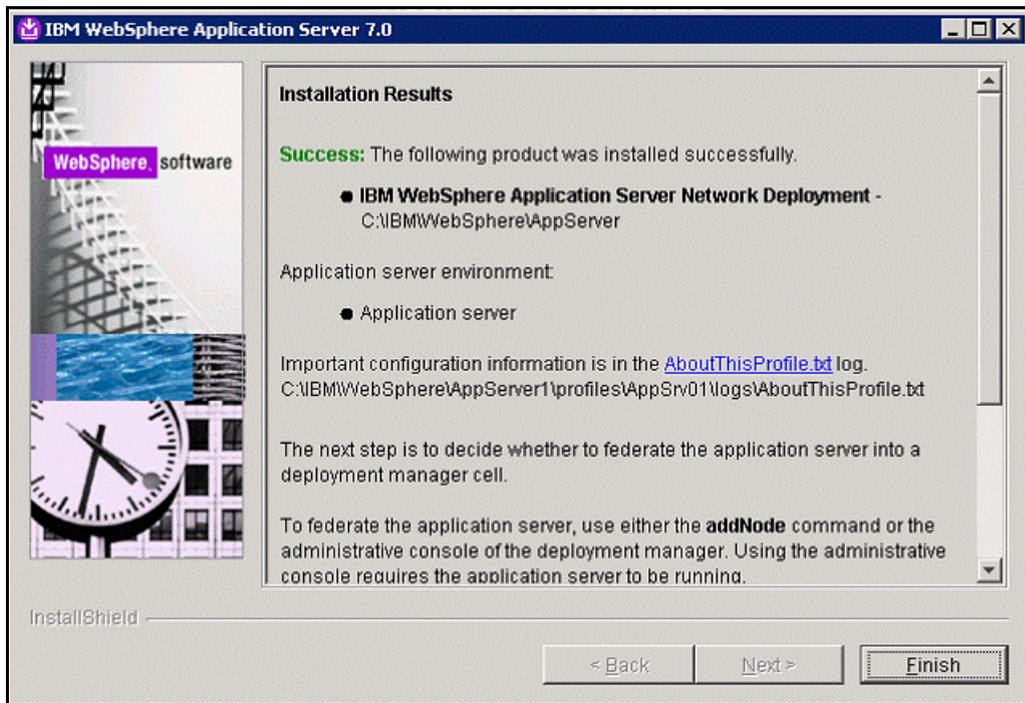


Figure 44. IBM WebSphere Application Server 7.0: Installation Results screen

Installing IBM HTTP Server

Follow the following steps to install IBM HTTP Server:

1. In the IBM HTTP Server Installation screen, select **Launch the installation wizard for IBM HTTP Server**.

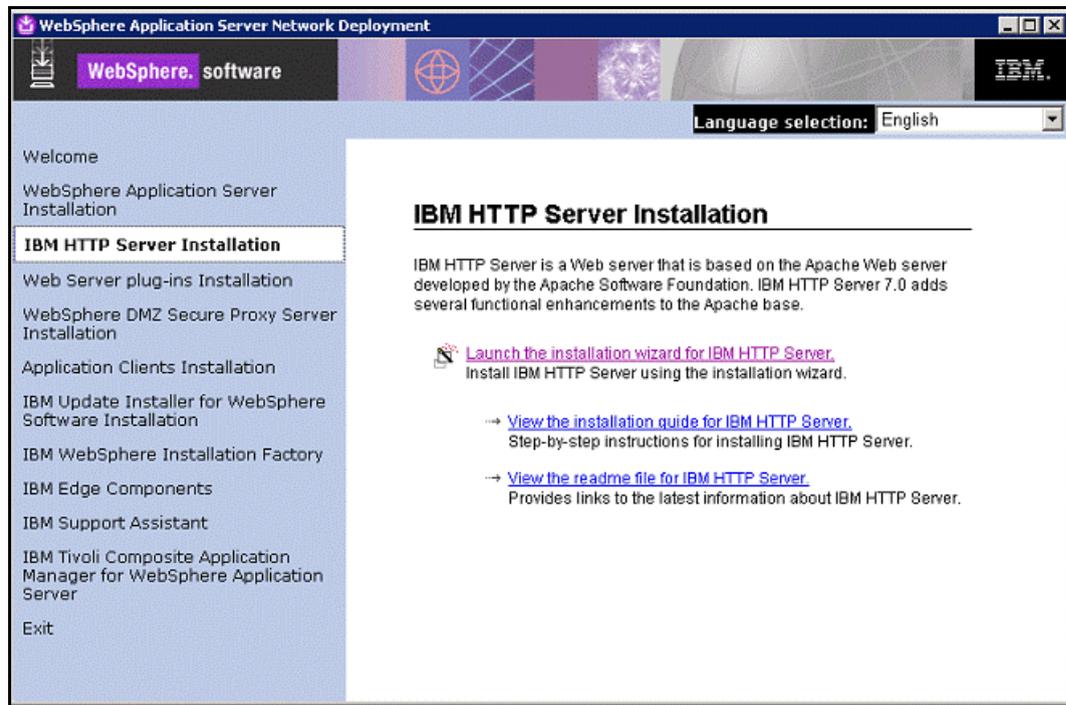


Figure 45. IBM HTTP Server Installation

2. In the welcome screen, click **Next**.

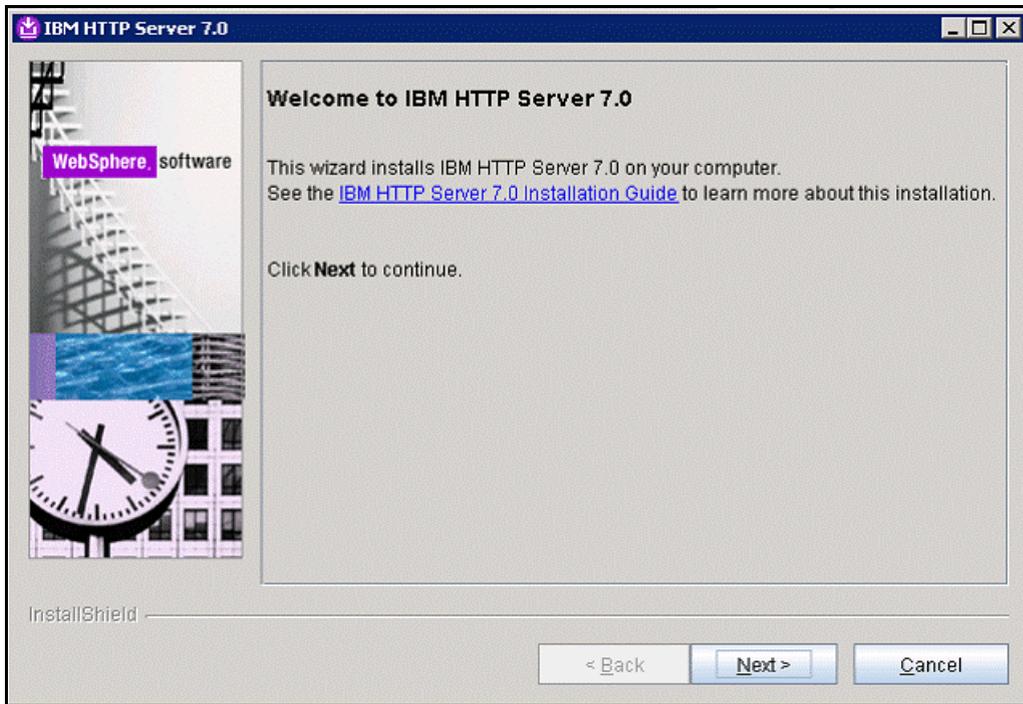


Figure 46. IBM HTTP Server 7.0 wizard: Welcome screen

3. In the Software License Agreement screen, click "I accept both the IBM and the non-IBM terms" and click **Next**.

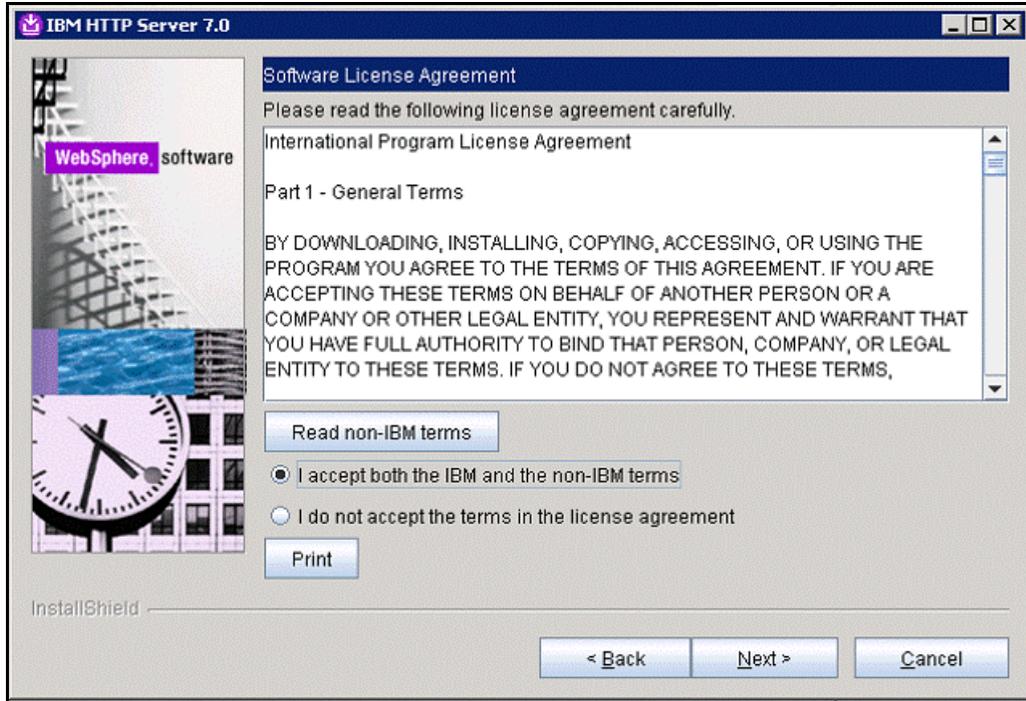


Figure 47. IBM HTTP Server 7.0: Software License screen

- ___ 4. In the System Prerequisites Check screen, click **Next**.

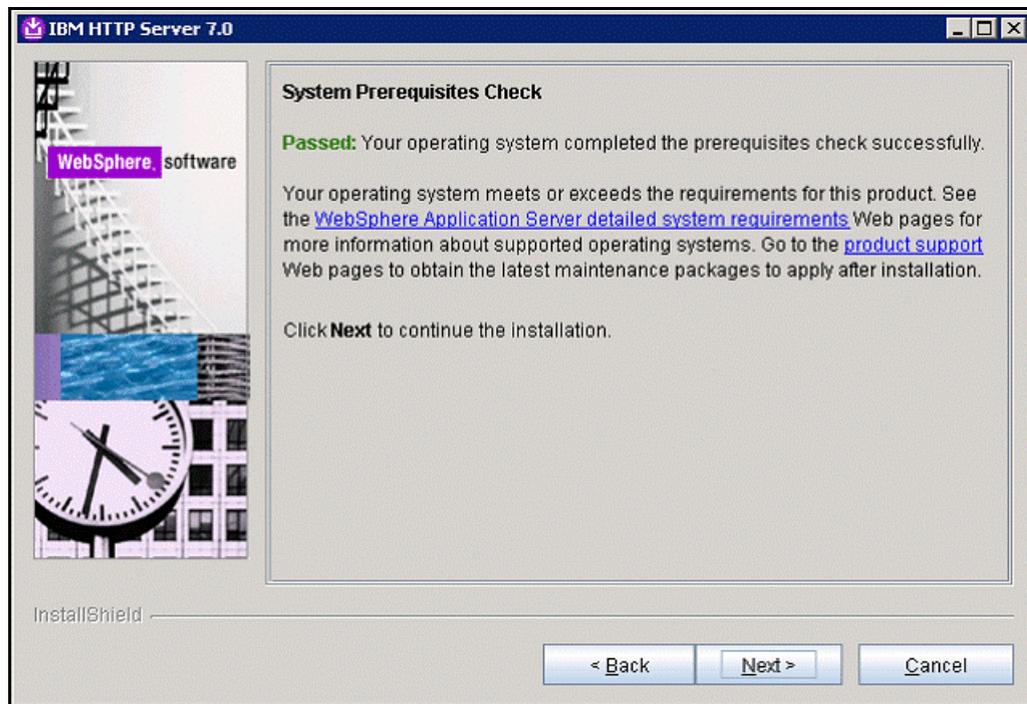


Figure 48. IBM HTTP Server 7.0: System Prerequisites Check screen

- ___ 5. Select the installation location and click **Next**.

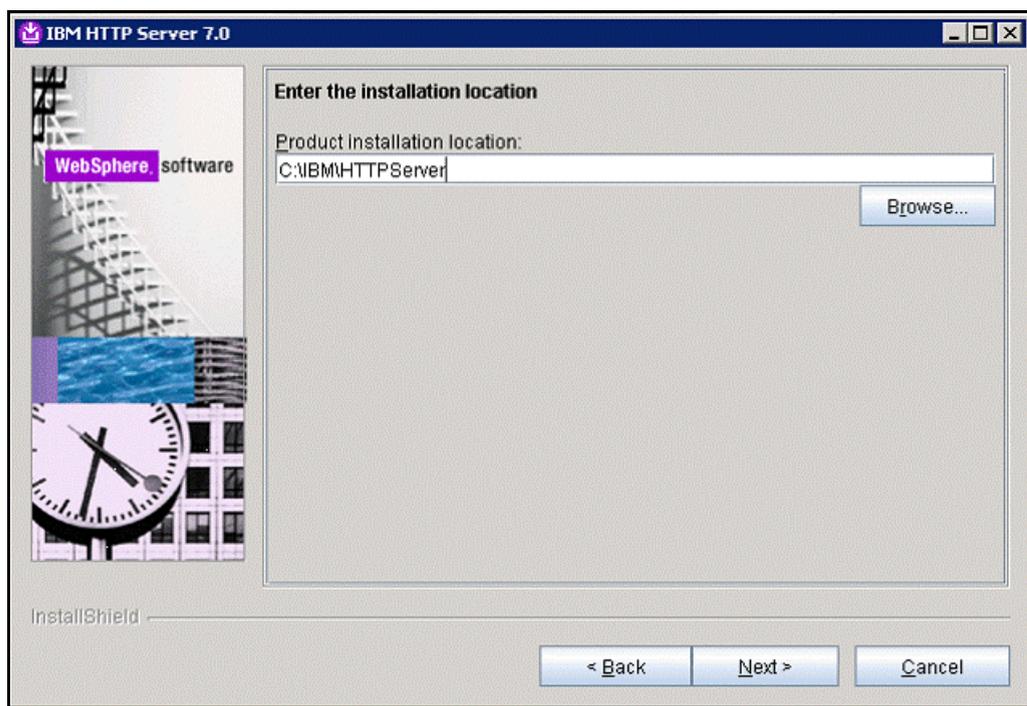


Figure 49. IBM HTTP Server 7.0: Installation location screen

___ 6. Assign the port values as shown in the screen and click **Next**.

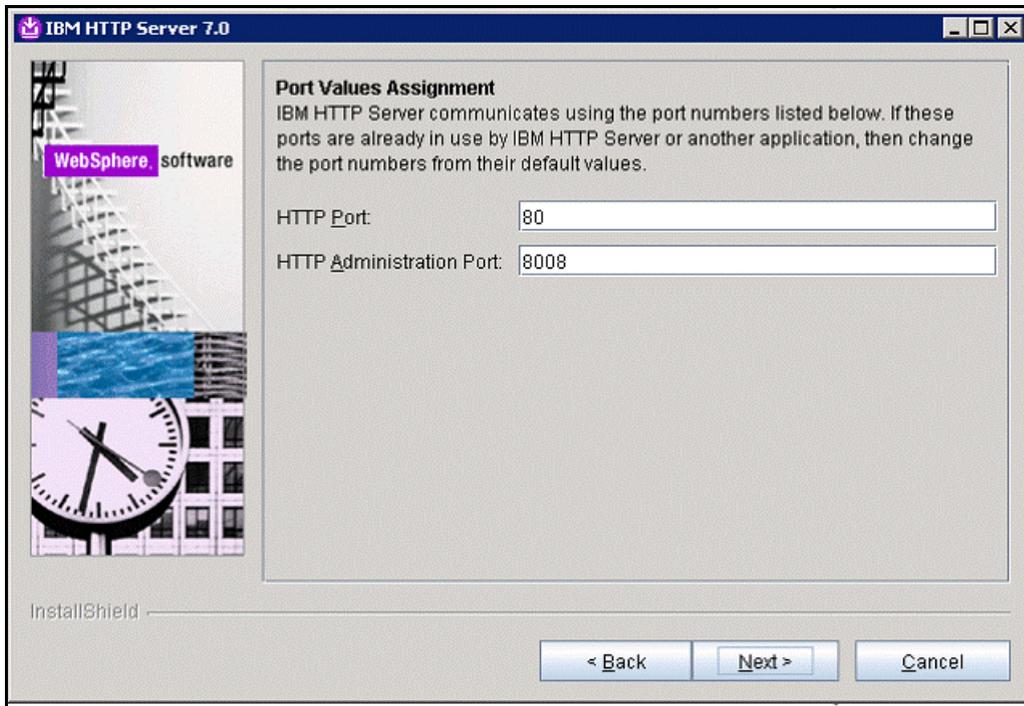


Figure 50. IBM HTTP Server 7.0: Port Values Assignment screen

___ 7. Select the option **Log on as a specified user account**.

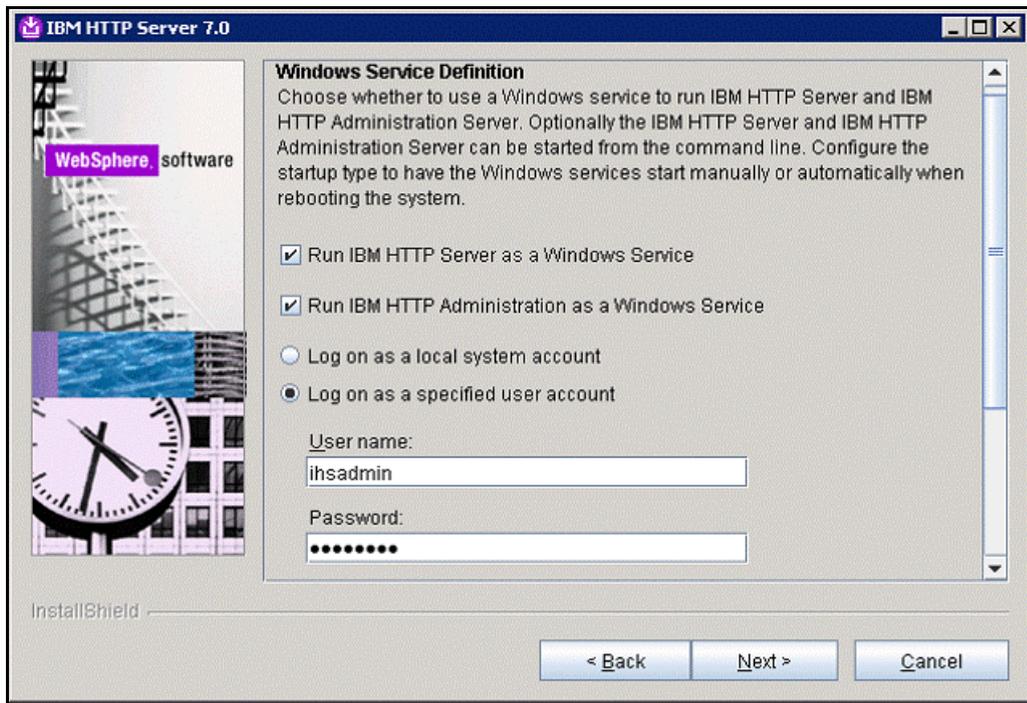


Figure 51. IBM HTTP Server 7.0: Windows Service Definition screen

- ___ 8. Enter the user name and password.

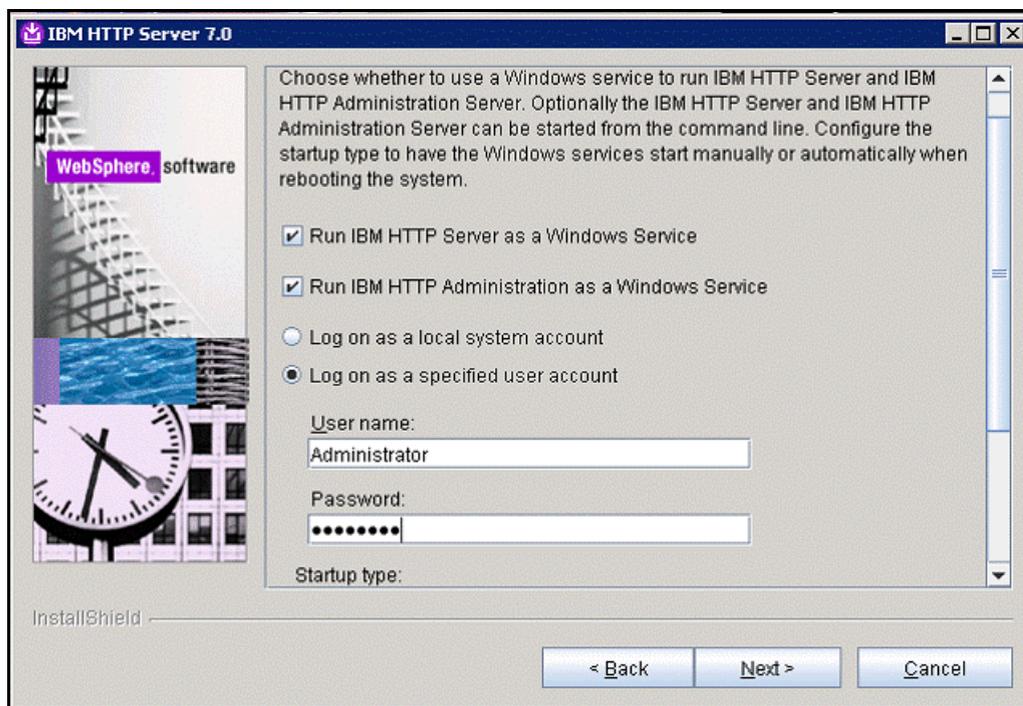


Figure 52. IBM HTTP Server 7.0: Entering user name and password in the Windows Service Definition screen

- ___ 9. Create a user ID for IBM HTTP Server administration server authentication. Enter the user ID and the password and click **Next**.

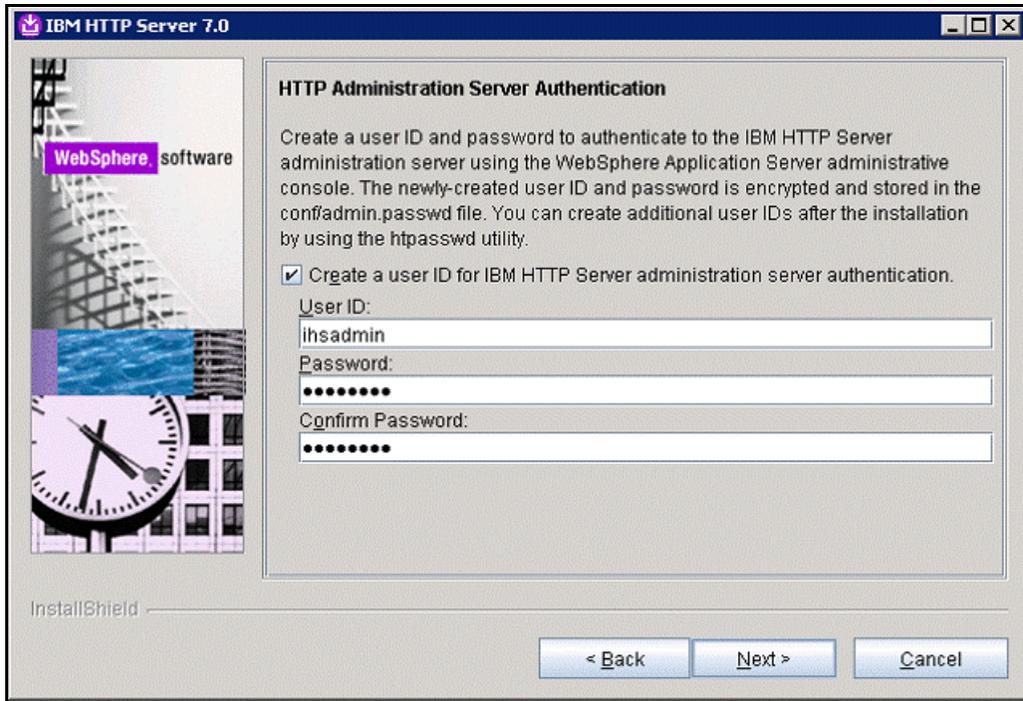


Figure 53. IBM HTTP Server 7.0: HTTP Administration Server Authentication screen

___ 10. Review the installation summary for correctness and click **Next**.

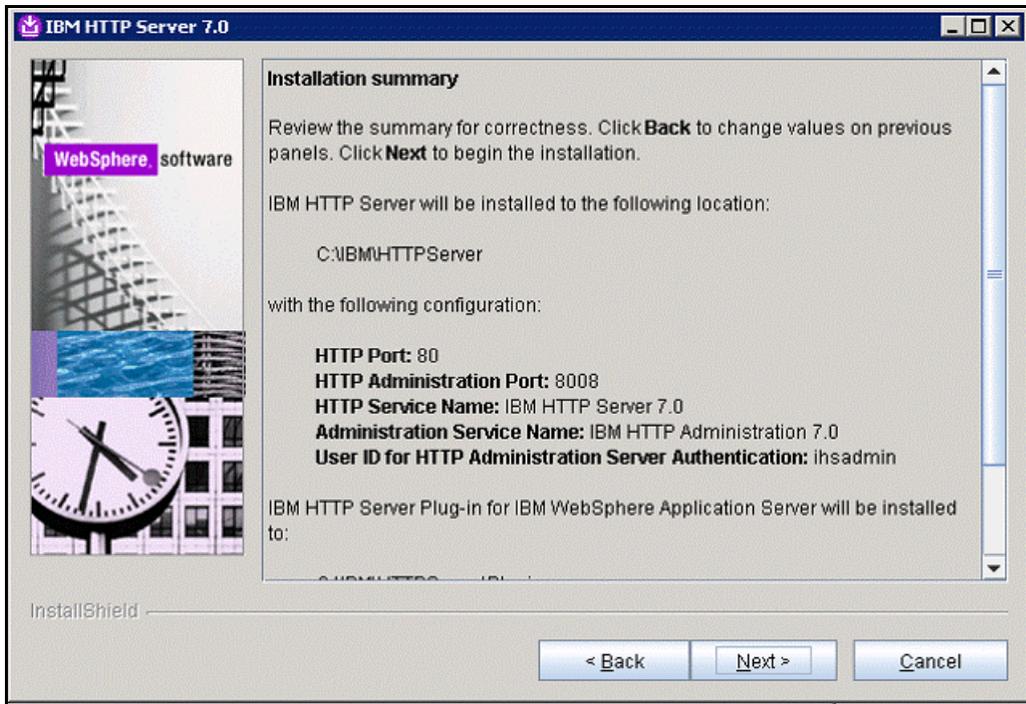


Figure 54. IBM HTTP Server 7.0: Installation summary screen

___ 11. When the product successfully installed, click **Finish**.

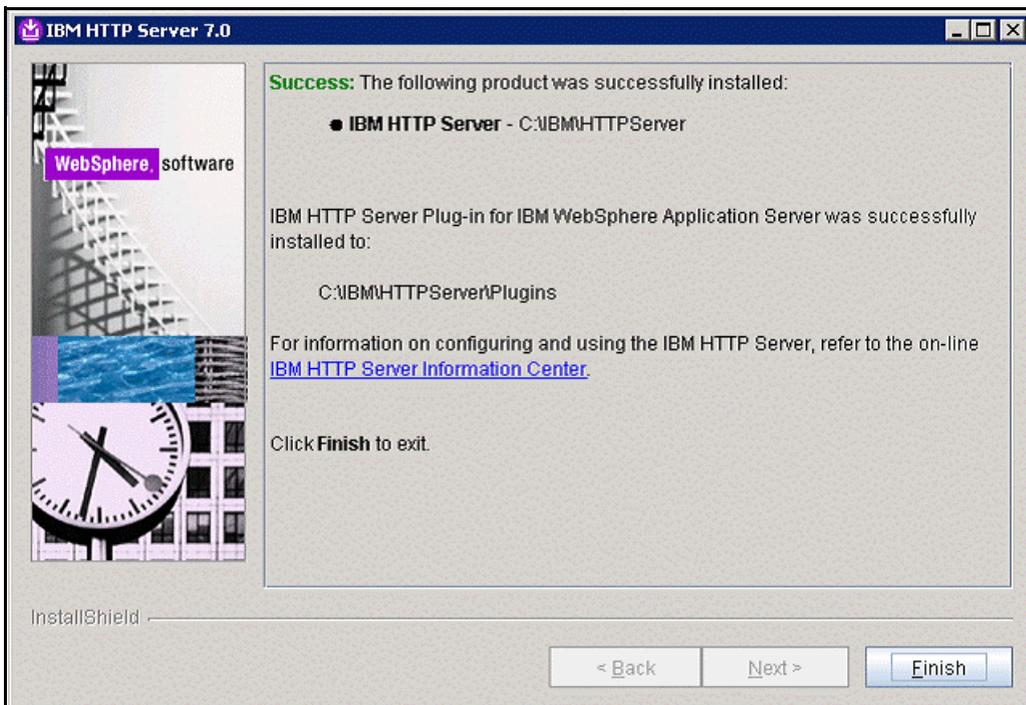


Figure 55. IBM HTTP Server 7.0: Installation completion screen

Installing Update Installer

Follow these steps to install the Update Installer 7.0.0.11:

1. Open the installation wizard for the Update Installer and click **Next**.

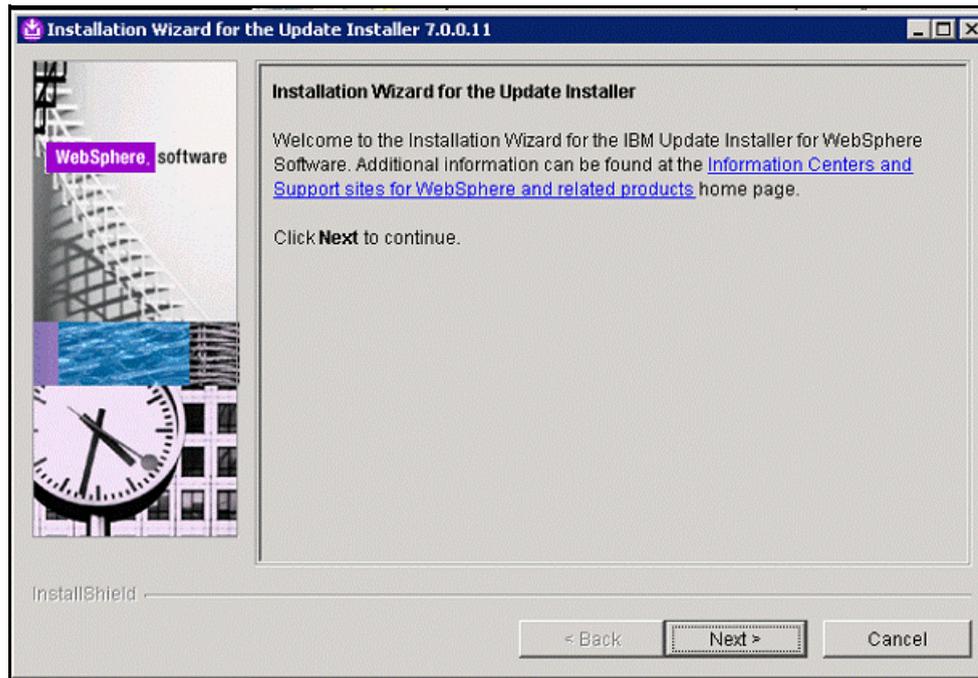


Figure 56. Installation Wizard for the Update Installer 7.0.0.11

- 2. In the Software License Agreement screen, select the option "I accept both the IBM and the non-IBM terms" and click **Next**.

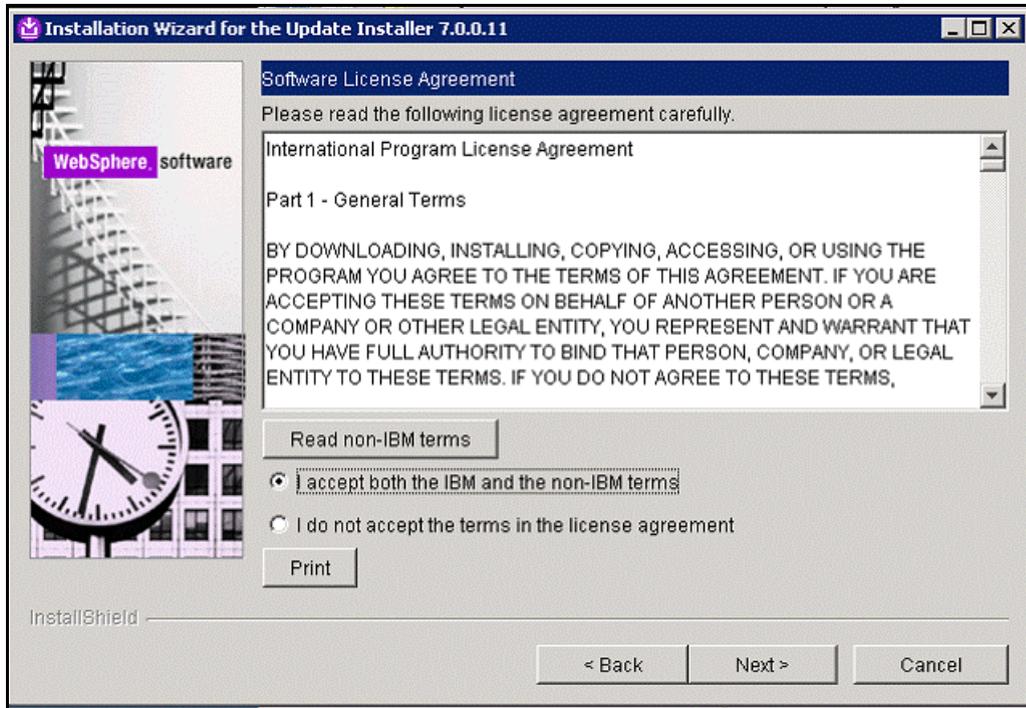


Figure 57. Installation Wizard for the Update Installer 7.0.0.11: Software License Agreement screen

- 3. Ensure that your operating system completes the prerequisites check and click **Next**.

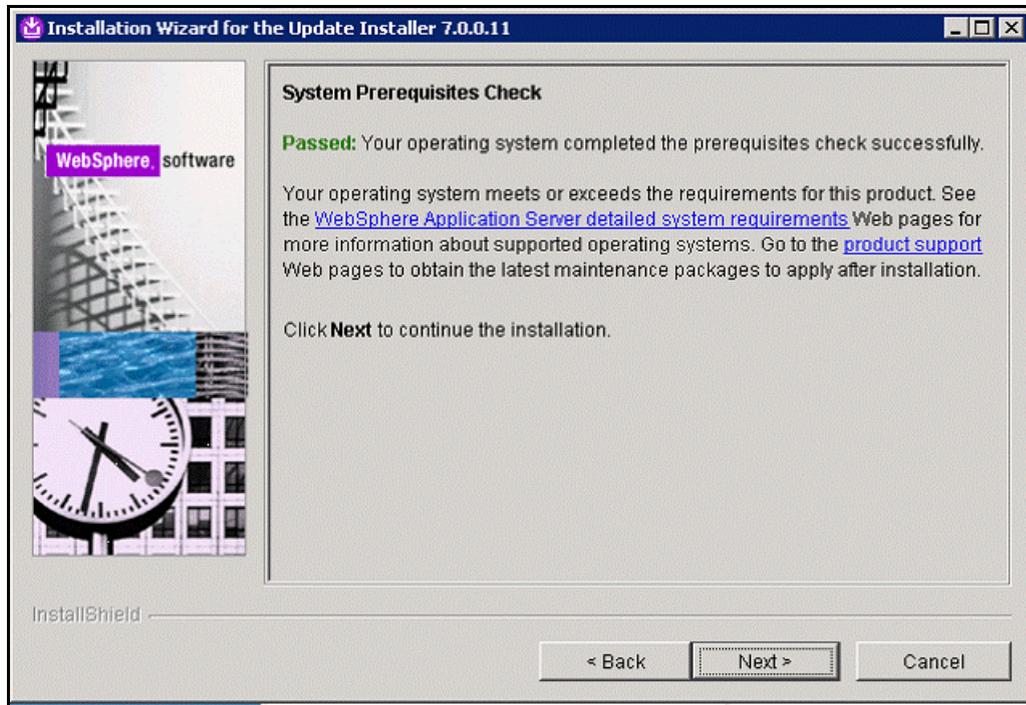


Figure 58. Installation Wizard for the Update Installer 7.0.0.11: System Prerequisites Check screen

4. Select the installation directory and click **Next**.

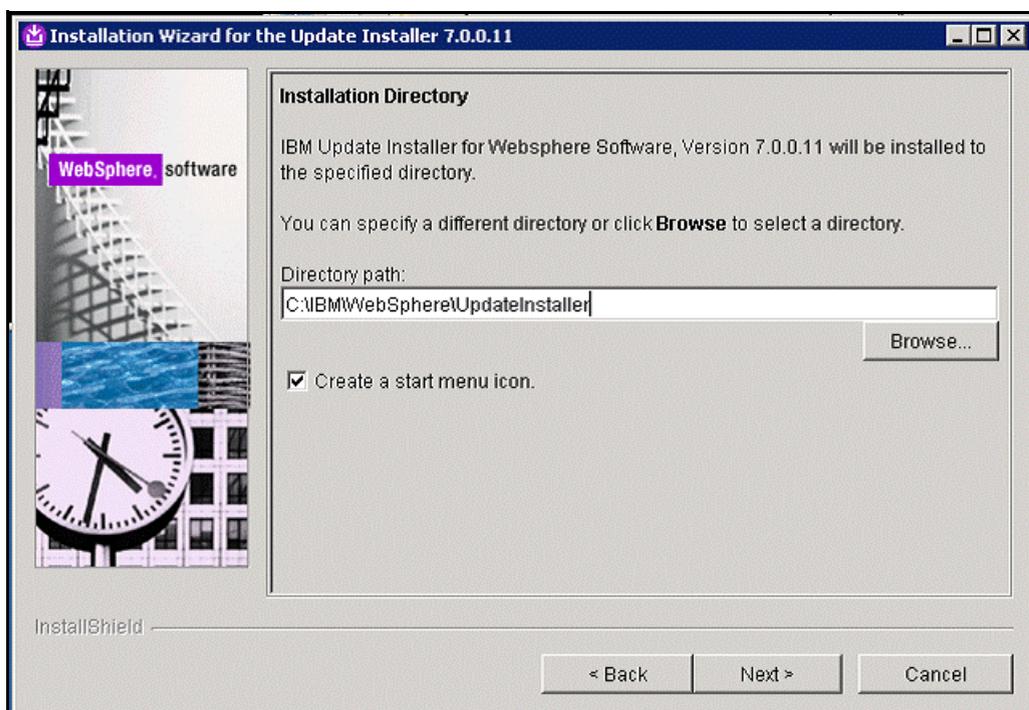


Figure 59. Installation Wizard for the Update Installer 7.0.0.11: Installation Directory screen

5. Review the installation summary and click **Next**.

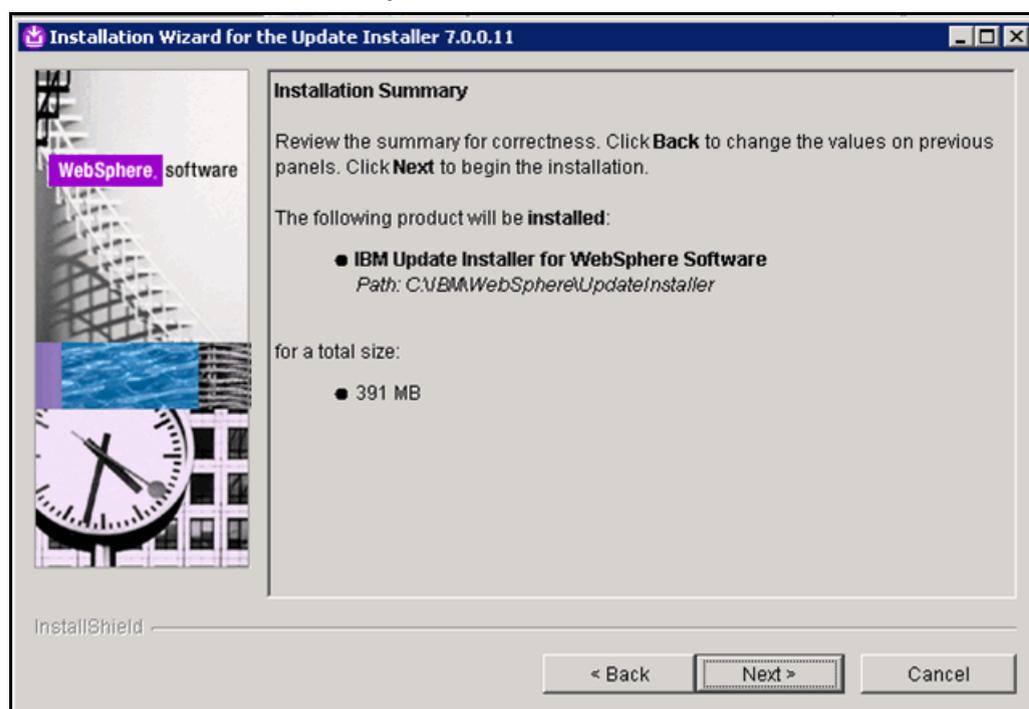


Figure 60. Installation Wizard for the Update Installer 7.0.0.11: Installation Summary screen

6. When the installation completes, click **Finish**.

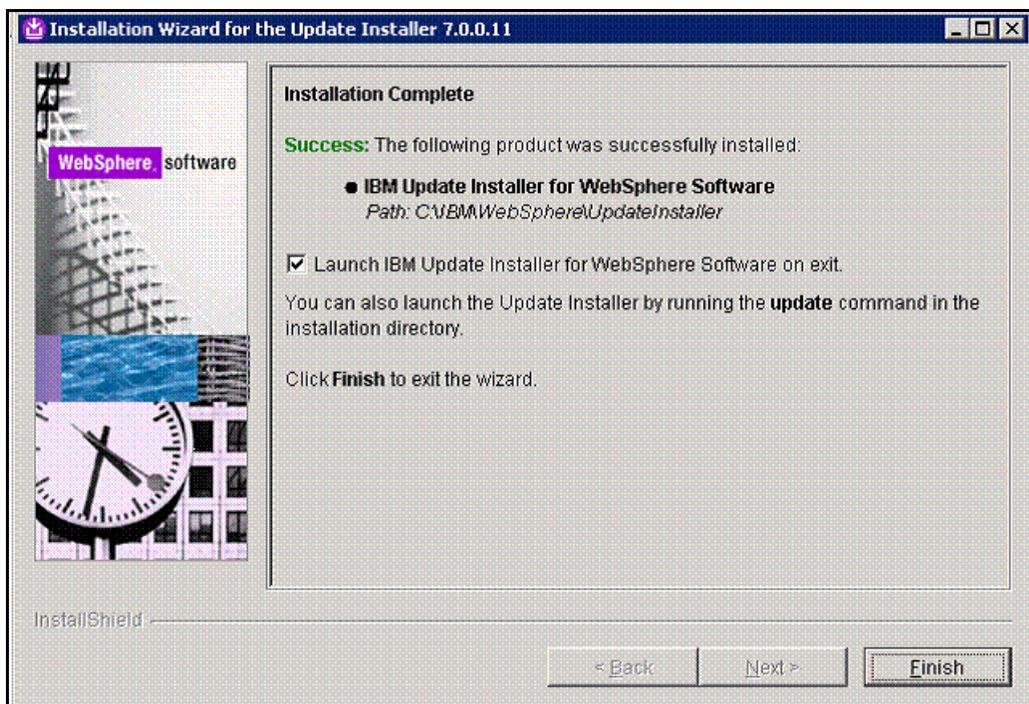


Figure 61. Installation Wizard for the Update Installer 7.0.0.11: Installation Complete screen

Apply 21 fix pack to both WebSphere Application Server and IBM HTTP Server and needed interim fixes to WebSphere Application Server

Follow these steps to apply 21 fix pack to both WebSphere Application Server and IBM HTTP Server and needed interim fixes to WebSphere Application Server:

1. Open the IBM Update Installer for WebSphere Software wizard and click **Next**.

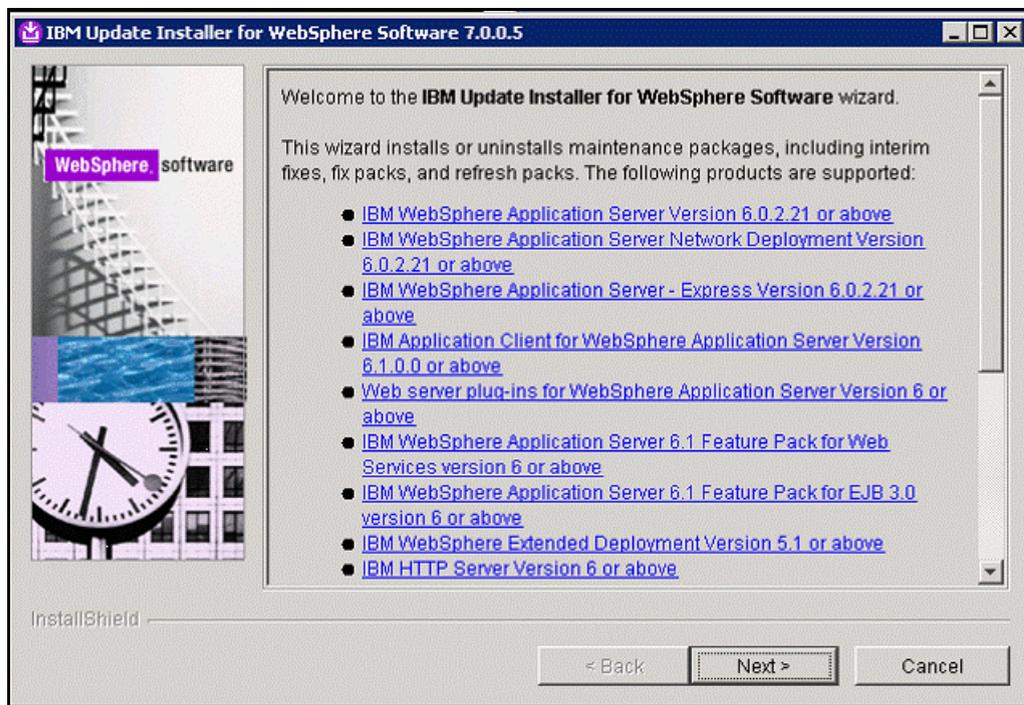


Figure 62. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: Welcome screen

2. Enter the installation location of the product you want to update and click **Next**.

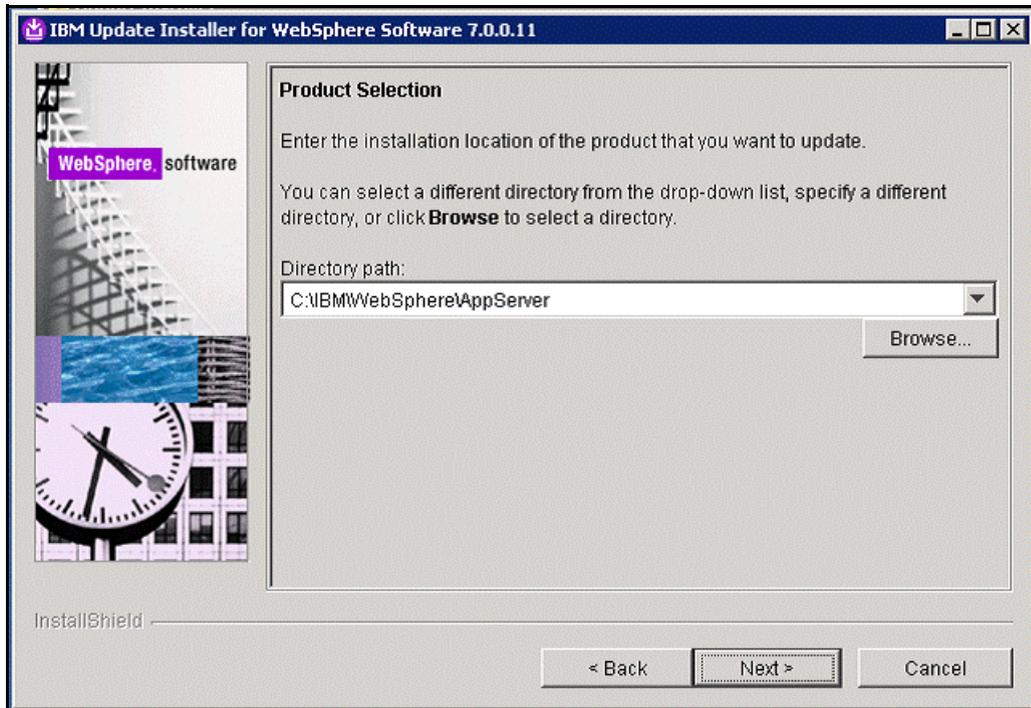


Figure 63. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: Product selection screen

3. Ensure that 7.0.0-WS-WAS-WinX64-FP0000021.pak and 7.0.0-WS-WASSDK-WinX64-FP0000021.pak are selected and click **Next**.

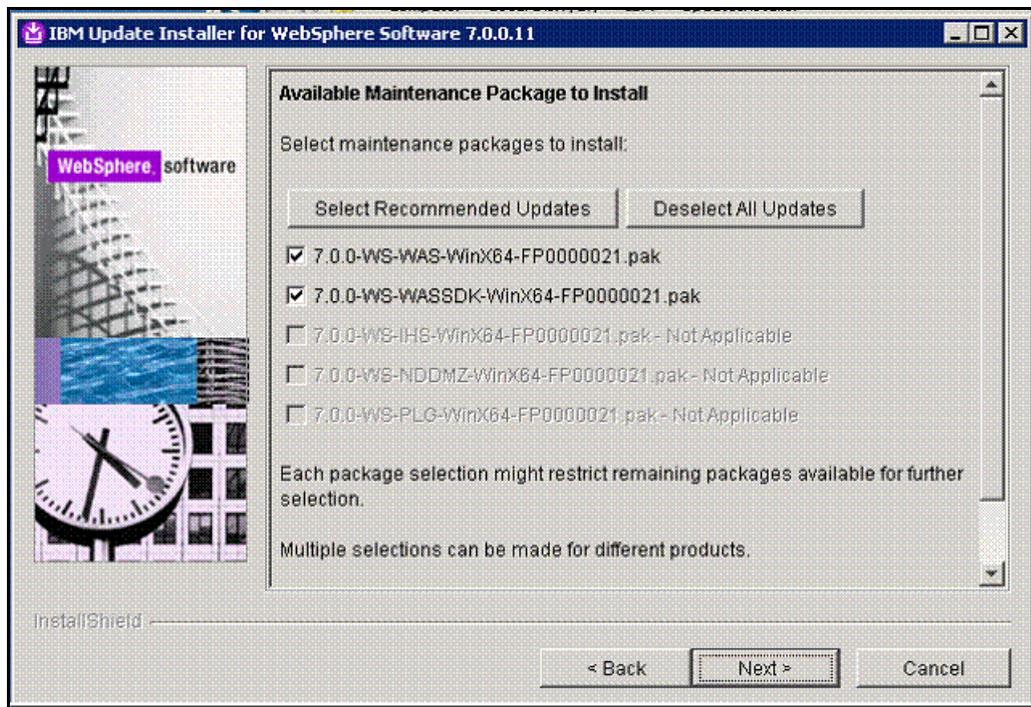


Figure 64. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: Available Maintenance Package to Install screen

4. Review the Installation Summary and click **Next**.

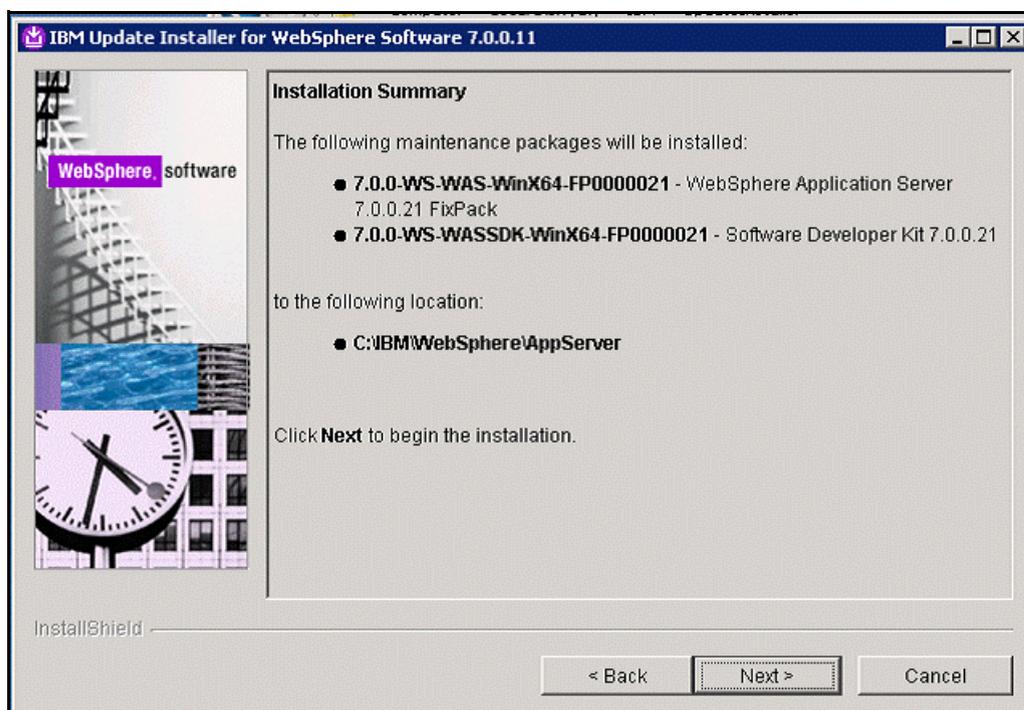


Figure 65. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: Installation Summary screen

5. In the screen IBM HTTP Server Plug-in for IBM WebSphere Application Server, click **Next** to install the plug-in that uses the remote installation scenario.

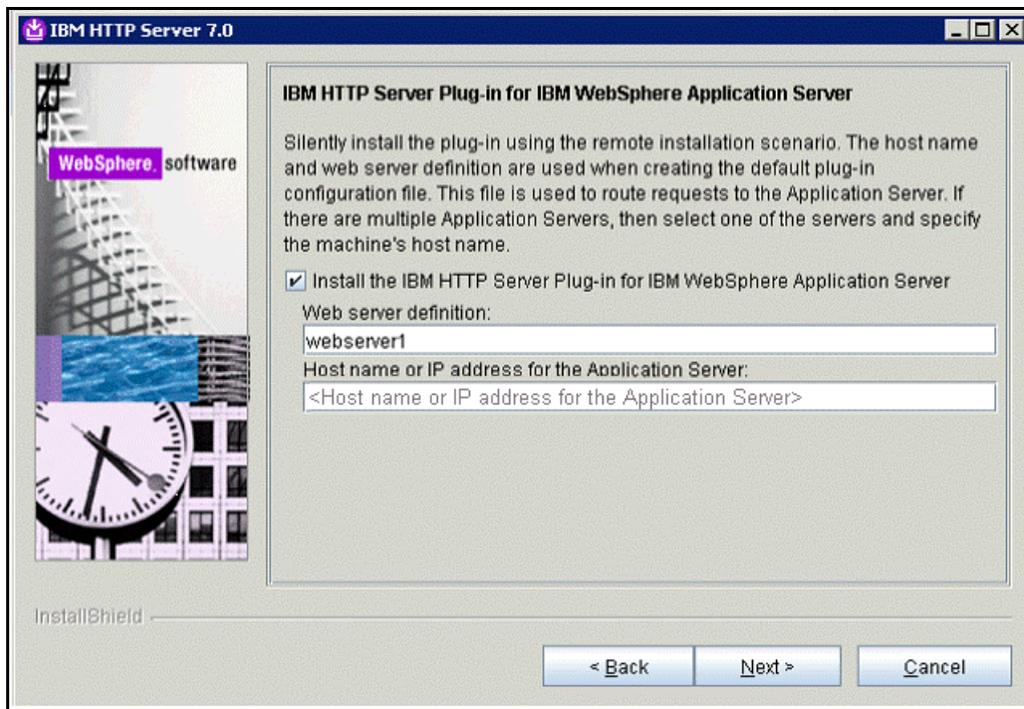


Figure 66. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: IBM HTTP Server Plug-in for IBM WebSphere Application Server screen

___ 6. In the Installation Complete screen, click **Finish**.

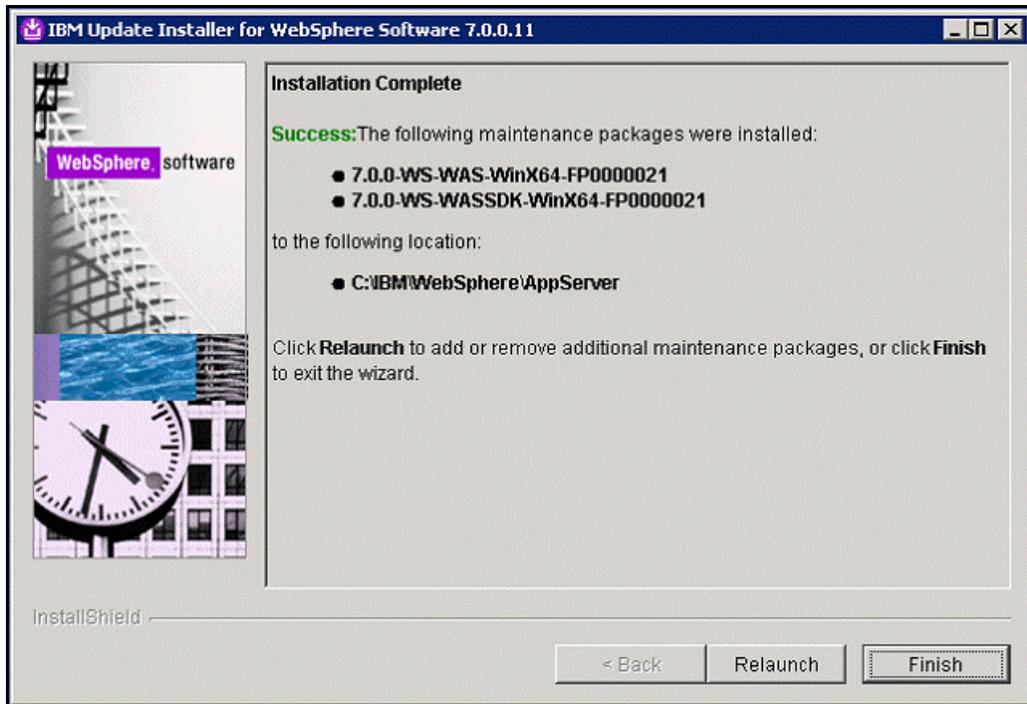


Figure 67. IBM Update Installer for WebSphere Software 7.0.0.5 wizard: Installation Complete screen

Apply WebSphere Application Server interim fixes

The WebSphere Application Server Required Fixes for 7.0.0.21 are as follows:

- PM53930:
<http://www-304.ibm.com/support/docview.wss?uid=swg21577532&myns=swgws&mynp=OCSSCKBL&mynp=OCSS7K4U&mynp=OCSSEQTP&mync=E>
- PM56596: <http://www-304.ibm.com/support/docview.wss?uid=swg24032675>
- PM60895:
<http://www-01.ibm.com/support/docview.wss?uid=swg24032589&myns=swgws&mynp=OCSSEQTP&mync=R>
- PM51981:
<http://www-933.ibm.com/support/fixcentral/swg/selectFix?product=ibm%2FWebSphere%2FWebSphere+Application+Server&fixids=7.0.0.21-WS-WAS-IFPM51981&source=dbluesearch&function=fixId&parent=Tivoli%20Service%20Management>
- PM65486: <http://www-01.ibm.com/support/docview.wss?uid=swg24033330>

**Note**

Visit this link for detailed information about the WebSphere Application Server Required Fixes for 7.0.0.21:

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

1. Open the IBM Update Installer for WebSphere Software wizard and click **Next**.

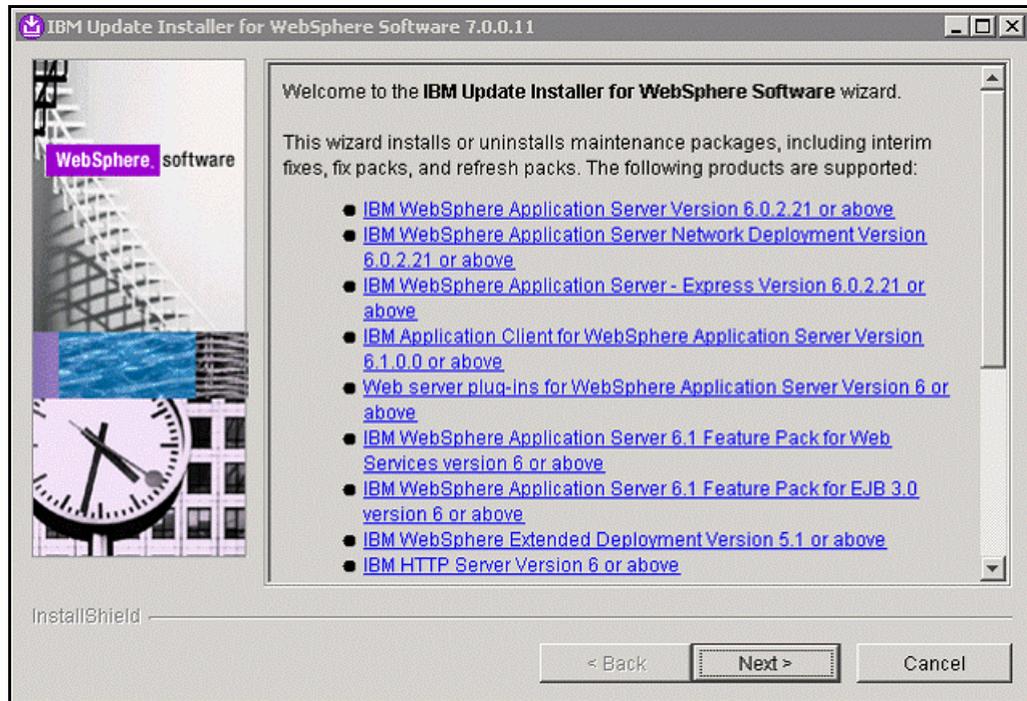


Figure 68. IBM Update Installer for WebSphere Software: Welcome screen

___ 2. Search for the installation location of the product that you want to update and click **Next**.

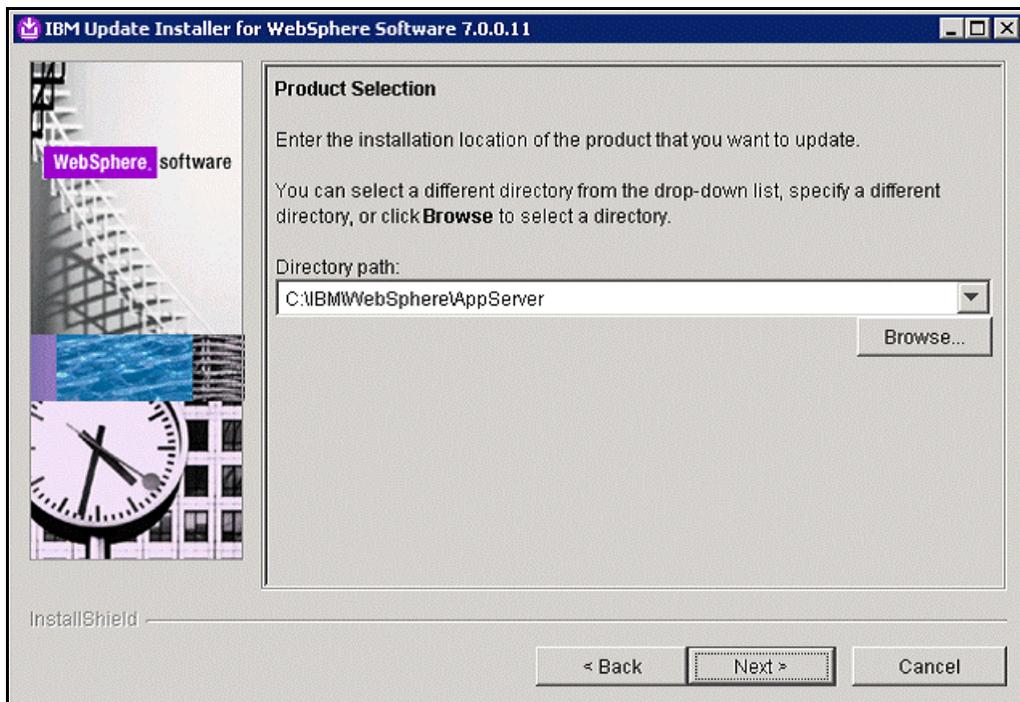


Figure 69. IBM Update Installer for WebSphere Software: Product Selection screen

___ 3. In the Maintenance Operation Selection screen, ensure that Install maintenance package is selected and click **Next**.

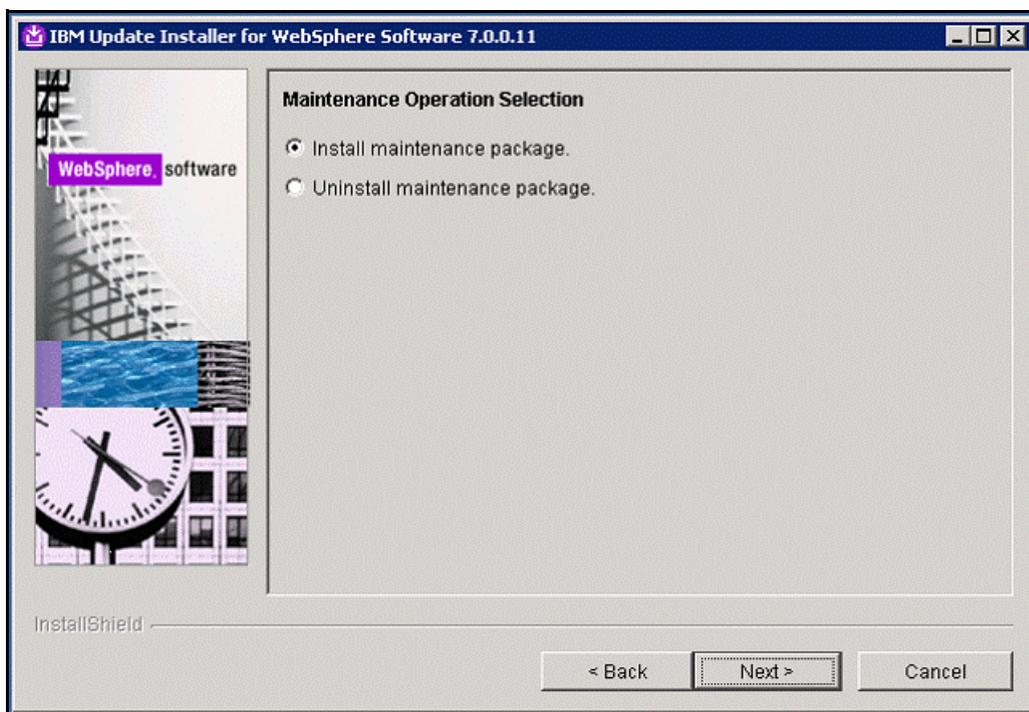


Figure 70. IBM Update Installer for WebSphere Software: Maintenance Operation Selection screen

4. Select the directory where you want to install the maintenance packages available for installation and click **Next**.

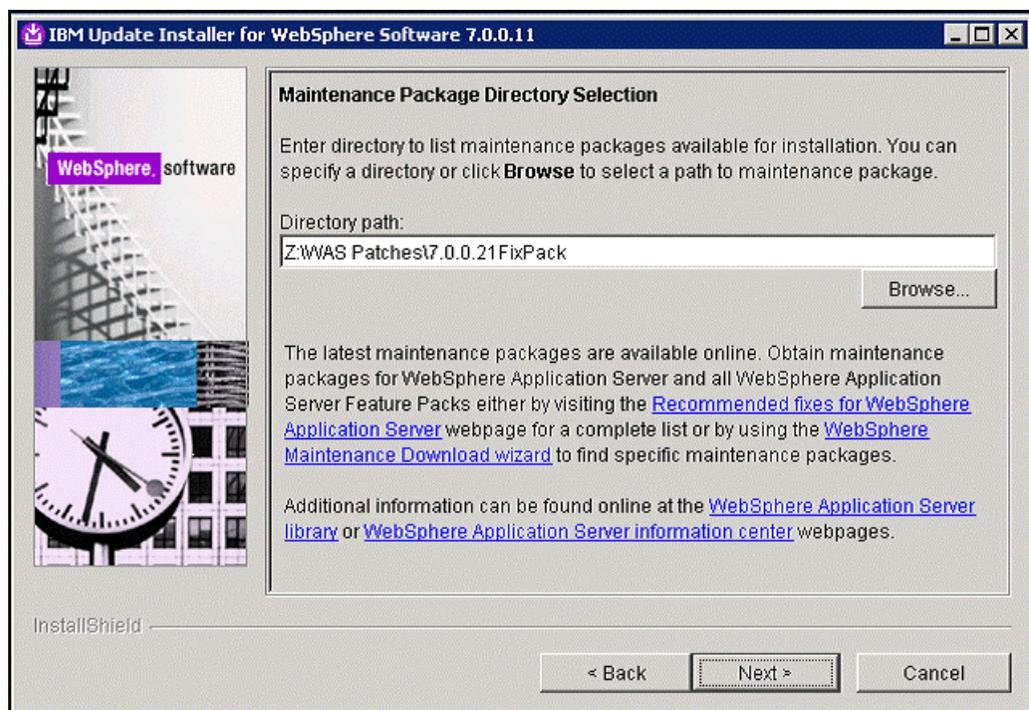


Figure 71. IBM Update Installer for WebSphere Software: Maintenance Package Directory Selection screen

5. Select the maintenance packages to install and click **Next**.

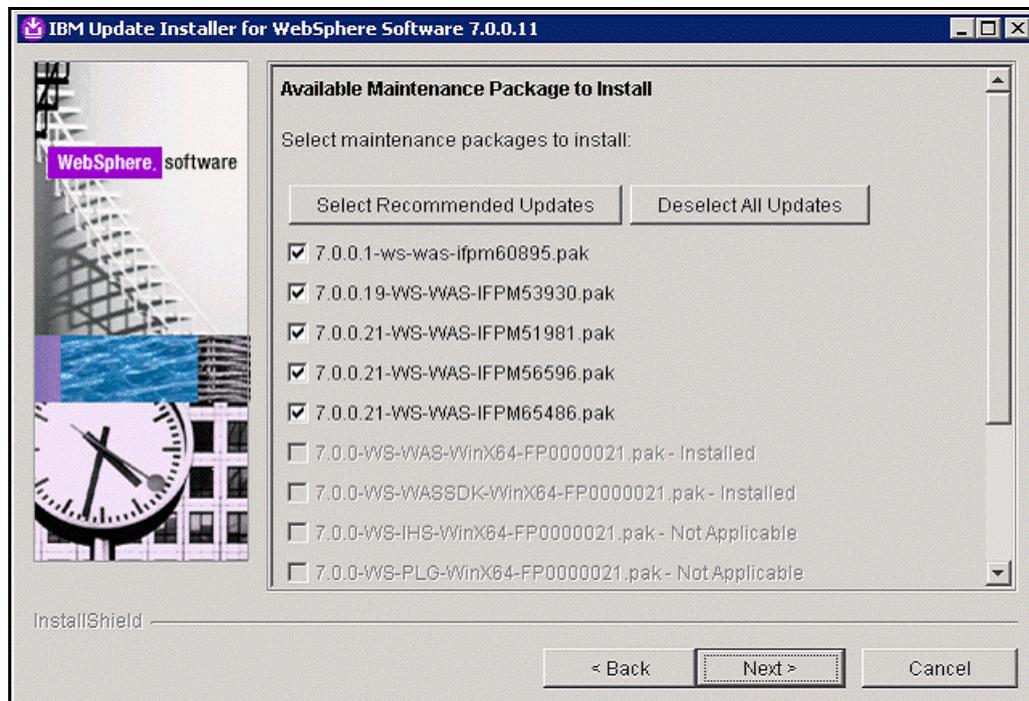


Figure 72. IBM Update Installer for WebSphere Software: Available Maintenance Package to Install screen

6. Review the Installation Summary screen and click **Next**.

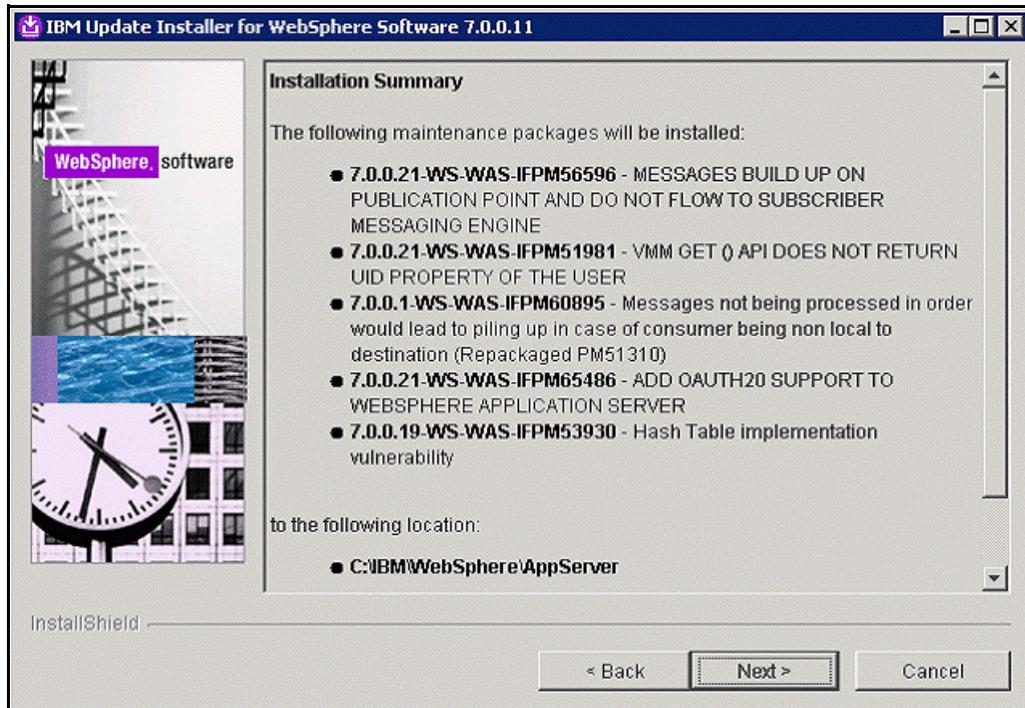


Figure 73. IBM Update Installer for WebSphere Software: Installation Summary screen

7. In the Installation Complete screen, click **Finish**.

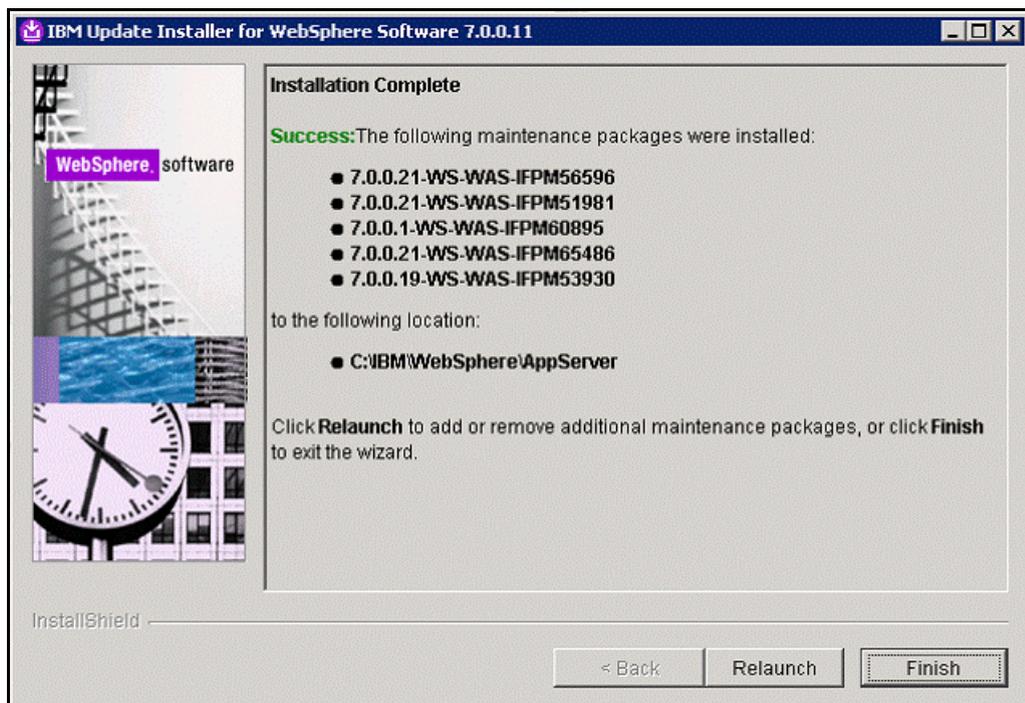


Figure 74. IBM Update Installer for WebSphere Software: Installation Complete screen

Federating nodes into Deployment Manager to make cluster environment

Adding a node to a cluster



Note

To add a node to an existing cluster, you must already have a cluster with at least one member.

Ensure that you installed IBM® WebSphere® Application Server Network Deployment (Application Server option) on the new node.

Although the same Deployment Manager manages both the IBM Cognos® Business Intelligence server and IBM Connections, you cannot add that node to the Connections cluster.

To add a node to a cluster, complete the following steps:

- ___ 1. Add a node to the Deployment Manager cell:
 - ___ a. Log on to the new node.
 - ___ b. Open a command prompt and change to the bin directory of the local WebSphere Application Server profile: `app_server_root/profiles/profile_name/bin`
 - ___ c. Run the `addNode` command to add this node to the Deployment Manager cell:


```
addnode [dmgr_host] [dmgr_port] [-username uid] [-password pwd]
[-localusername localuid] [-localpassword localpwd]
```

where

 - `dmgr_host` is the host name of the Deployment Manager
 - `dmgr_port` is the SOAP port of the deployment manager (the default is 8879)
 - `uid` and `pwd` are the Deployment Manager administrator user name and password
 - `localuid` and `localpwd` are the user name and password for the WebSphere Application Server administrator of the node
 - ___ d. Open the `addNode.log` file and confirm that the node was successfully added to the Deployment Manager cell. The file is stored in the following location:

```
app_server_root/profiles/profile_name/log/addNode.log
```

- ___ 2. Copy the relevant JDBC files from the Deployment Manager node to this node, placing them in the same location as the JDBC files on the Deployment Manager. If, for example, you copied the `db2jcc.jar` file from the `C:\IBM\SQLLIB` directory on the Deployment Manager, you must copy the same file to the `C:\IBM\SQLLIB` directory on this node. See the following table to determine which files to copy. See the following table to determine which files to copy:

Table 1: JDBC files

Database type	JDBC files
DB2®	<code>db2jcc.jar</code> <code>db2jcc_license_cu.jar sql</code>
Oracle	<code>ojdbc6.jar</code>
SQL Server	<code>sqljdbc4.jar</code>

- ___ 3. Ensure that the shared folders that are used for the application content stores in the cluster are accessible from the new node: from the new node, try to access the shared directories.
- ___ 4. Add extra members to an existing IBM Connections cluster:
 - ___ a. Log on to the Deployment Manager Integration Solutions Console.
 - ___ b. Click **Servers > Clusters > *cluster_name* > Cluster members > New**. Specify the following information about the new cluster member:
 - Member name: The name of the server instance that is created for the cluster. The Deployment Manager creates a server instance with this name.



Note

Each member name in the same cluster must be unique. The Integration Solutions Console prevents you from reusing the same member name in a cluster.

- Select node: The node where the server instance is located.
- Click **Add Member** to add this member to the cluster member list.
- ___ c. Click **Next** to go to the summary page where you can examine detailed information about this cluster member. Click **Finish** to complete this step or click **Previous** to modify the settings.
 - ___ d. Click **Save** to save the configuration.
 - ___ e. Click **Server > Servers > Clusters > *cluster_name* > Cluster members**. In the member list, click the new member that you added in the previous step.
 - ___ f. On the detailed configuration page, click **Ports** to expand the port information of the member. Make a note of the `WC_defaulthost` and `WC_defaulthost_secure` port numbers. For example, the `WC_defaulthost` port number is typically 9084, while the `WC_defaulthost_secure` port number is typically 9447.
 - ___ g. Click **Environment > Virtual Hosts > *default_host* > Host Aliases > New**. Enter the following information for the host alias for the `WC_defaulthost` port:

- Host name: The IP address or DNS host name of the node where the new member is located.
- Port: The port number for `WC_defaulthost`. For example, 9084.

Click **OK** to complete the virtual host configuration.

- __ h. Click **Save** to save the configuration.
- __ i. Repeat the previous two substeps to add the host alias for the `WC_defaulthost_secure` port.
- __ j. Click **System administration > Nodes**.
- __ k. In the node list page, select all the nodes where the target cluster members are located and then click **Synchronize**.



Note

What to do next:

Configure IBM HTTP Server to connect to this node.

Repeat this task for each new node that you want to add to a cluster.

Setting up federated repositories

Follow these steps to set up federated repositories:

- ___ 1. Log on to Deployment Manager WebSphere Application Server console by <https://connections.example.com:9043/ibm/console> as **wasadmin/wasadmin**.
- ___ 2. Go to **Security > Global security** page, click **Configure...** beside federated repositories.

Global security

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

Security Configuration Wizard Security Configuration Report

Administrative security

Enable administrative security

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

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources

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

User account repository

Current realm definition
Federated repositories

Available realm definitions
Federated repositories [Configure...](#) [Set as current](#)

Authentication

Authentication mechanisms and expiration

- [LTPA](#)
- Kerberos and LTPA

(This function is currently disabled. See the [IBM Support site](#) for possible future updates.)

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

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

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

Figure 75. Global security page

- ___ 3. Click **Add Base entry to Realm...**

Repositories in the realm:

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

Select	Base Entry	Repository Identifier	Repository Type
You can administer the following resources:			
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

Figure 76. Repositories in the realm section

___ 4. Click **Add Repository...**

Figure 77. Global security > Federated repositories > Repository reference

___ 5. Input LDAP information that was gathered in the previous section.

Figure 78. LDAP information

___ 6. Click **OK** and then **Save**.

___ 7. Input base entry under this repository.

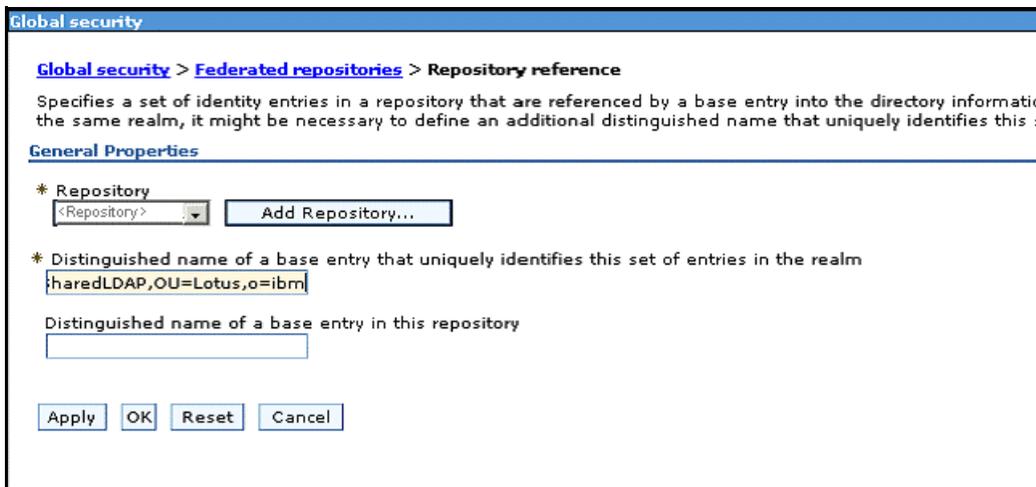


Figure 79. Input base entry under the repository

___ 8. Click **OK** and then **Save**.

___ 9. Change the primary administrator user to be a real user in LDAP, for example, **User1**.

___ 10. Click **OK** and then **Save**.

___ 11. On the global security page, check **Enable application security**.

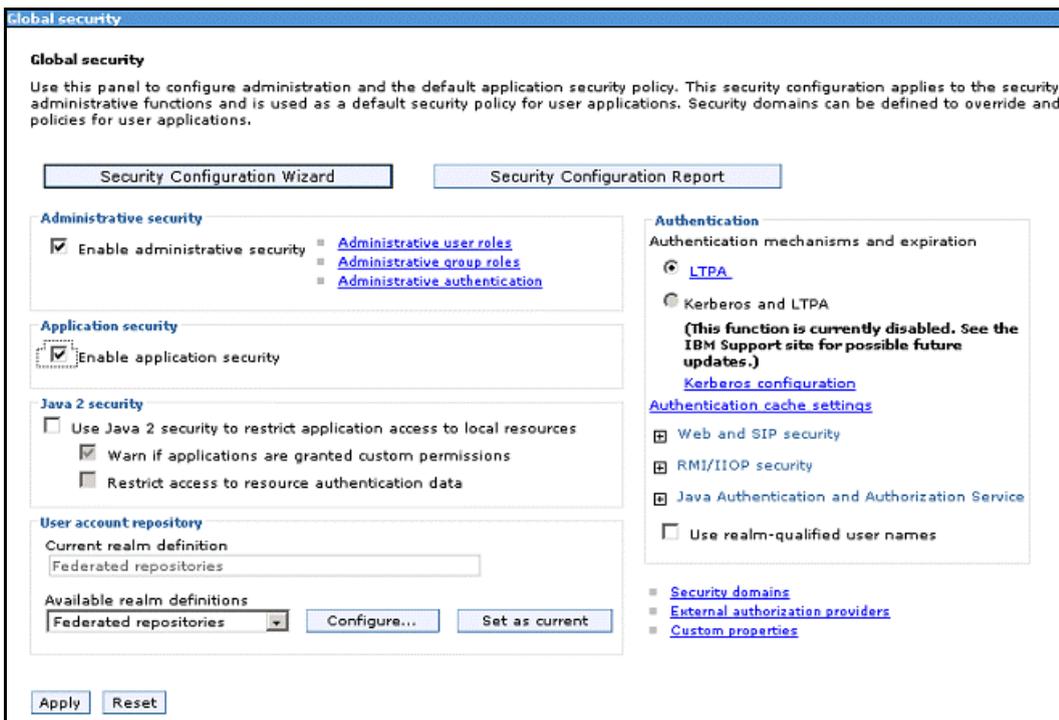
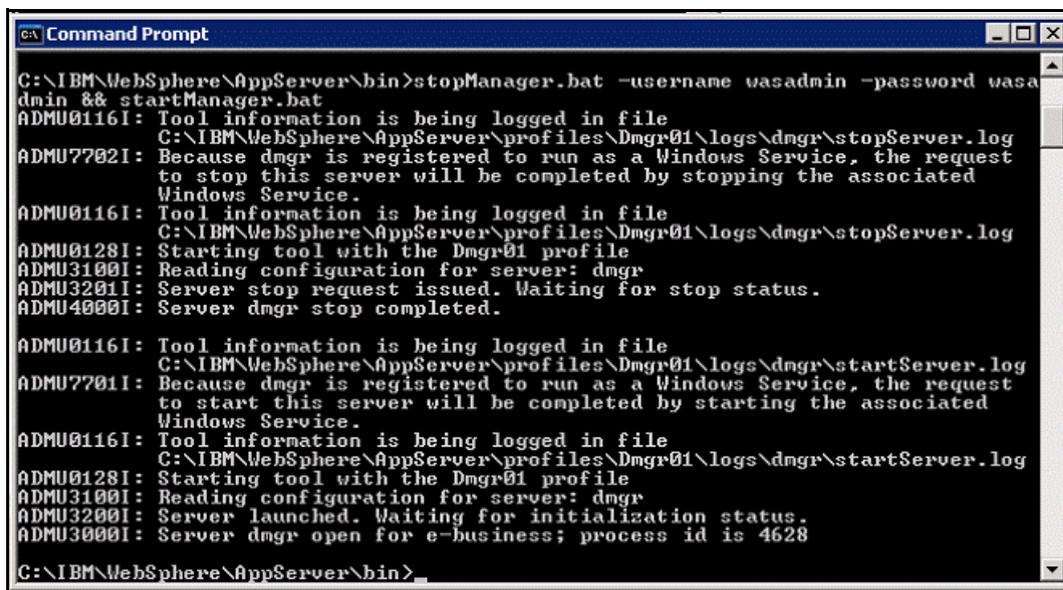


Figure 80. Global security page > Enable application security

___ 12. Click **Apply** and then **Save**.

___ 13. Restart Deployment Manager and Node agent.



```

C:\IBM\WebSphere\AppServer\bin>stopManager.bat -username wasadmin -password wasadmin && startManager.bat
ADMU0116I: Tool information is being logged in file
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\logs\dmgr\stopServer.log
ADMU7702I: Because dmgr is registered to run as a Windows Service, the request
to stop this server will be completed by stopping the associated
Windows Service.
ADMU0116I: Tool information is being logged in file
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\logs\dmgr\stopServer.log
ADMU0128I: Starting tool with the Dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server dmgr stop completed.

ADMU0116I: Tool information is being logged in file
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\logs\dmgr\startServer.log
ADMU7701I: Because dmgr is registered to run as a Windows Service, the request
to start this server will be completed by starting the associated
Windows Service.
ADMU0116I: Tool information is being logged in file
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\logs\dmgr\startServer.log
ADMU0128I: Starting tool with the Dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 4628

C:\IBM\WebSphere\AppServer\bin>

```

Figure 81. Restarting Deployment Manager and Node agent

___ 14. Verify you can login Deployment Manager was console as the administrator user you set.



Information

If you want to enable Domino SSO with other IBM products in the future, you should follow the following step to modify Domino LDAP repository:

- ___ 1. Stop Deployment Manager and Node agent.
- ___ 2. Go to `C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\ConnectionsCell01\wim\config` and backup the `wimconfig.xml` with a new name like `wimconfig.xml.bak`.
- ___ 3. Use a text edit tool to open `wimconfig.xml`.
- ___ 4. Find below two lines:


```

<config:baseEntries name="OU=SharedLDAP,OU=Lotus,o=ibm"
nameInRepository="" />
<config:participatingBaseEntries name="OU=SharedLDAP,OU=Lotus,o=ibm" />

```
- ___ 5. Change them to:


```

<config:baseEntries name="" nameInRepository="" />
<config:participatingBaseEntries name="" />

```
- ___ 6. Save your changes to `wimconfig.xml`.
- ___ 7. Start Deployment Manager and Node agent.

8. Go to the WebSphere Application Server console. The base entry name for Domino LDAP changed:

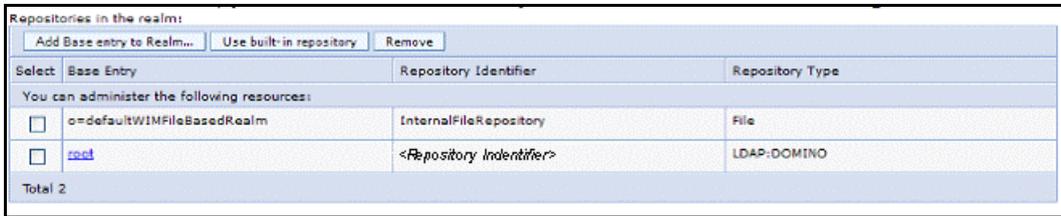


Figure 82. Repositories in the realm

You can verify that the LDAP is configured successfully by searching user and group in WebSphere Application Server console:

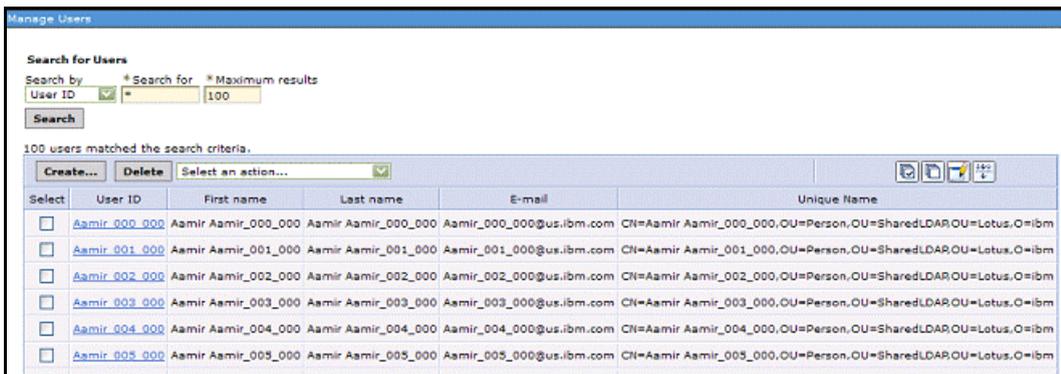


Figure 83. Manage users

Creating databases by using the Database wizard

To create databases by using the Database wizard, follow these steps:

1. Open the Database wizard for IBM Connections 4.0 and click **Next**.

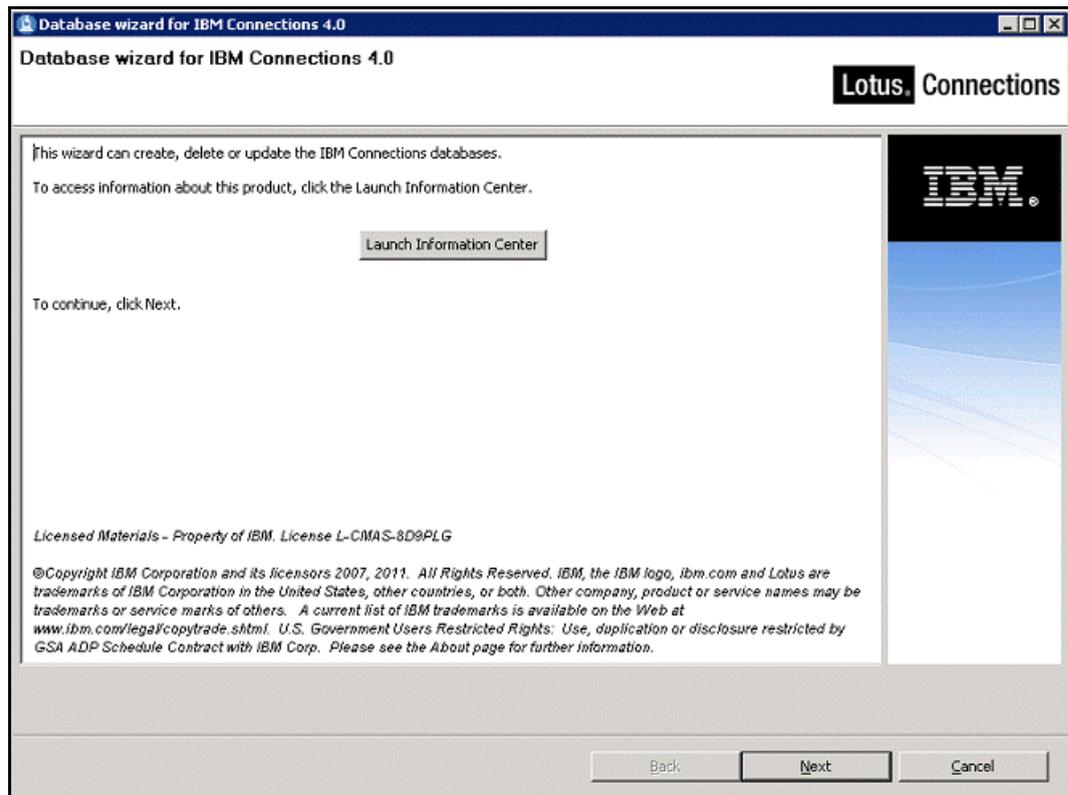


Figure 84. Database wizard for IBM Connections 4.0

- ___ 2. In the Database task selection screen, ensure that the option “Create” is selected and click **Next**.

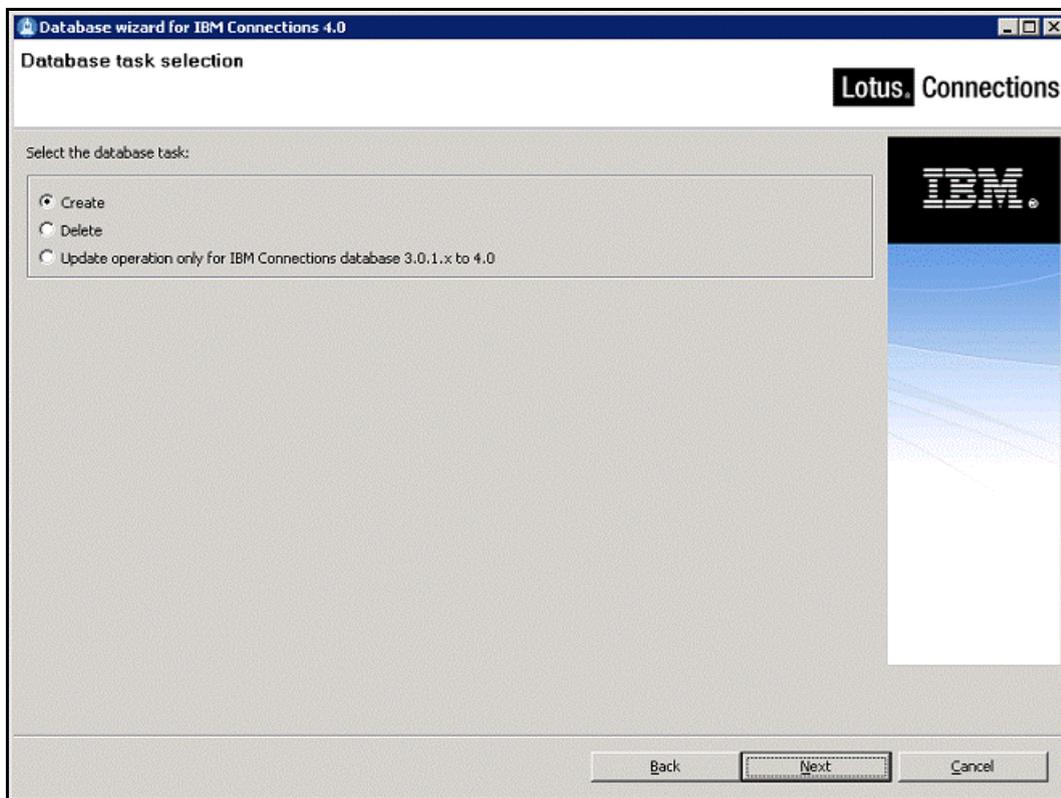


Figure 85. Database wizard for IBM Connections 4.0: Database task selection screen

- ___ 3. In the Database selection screen, select Oracle Enterprise Edition as database type, select the installation location, type the database instance and click **Next**.

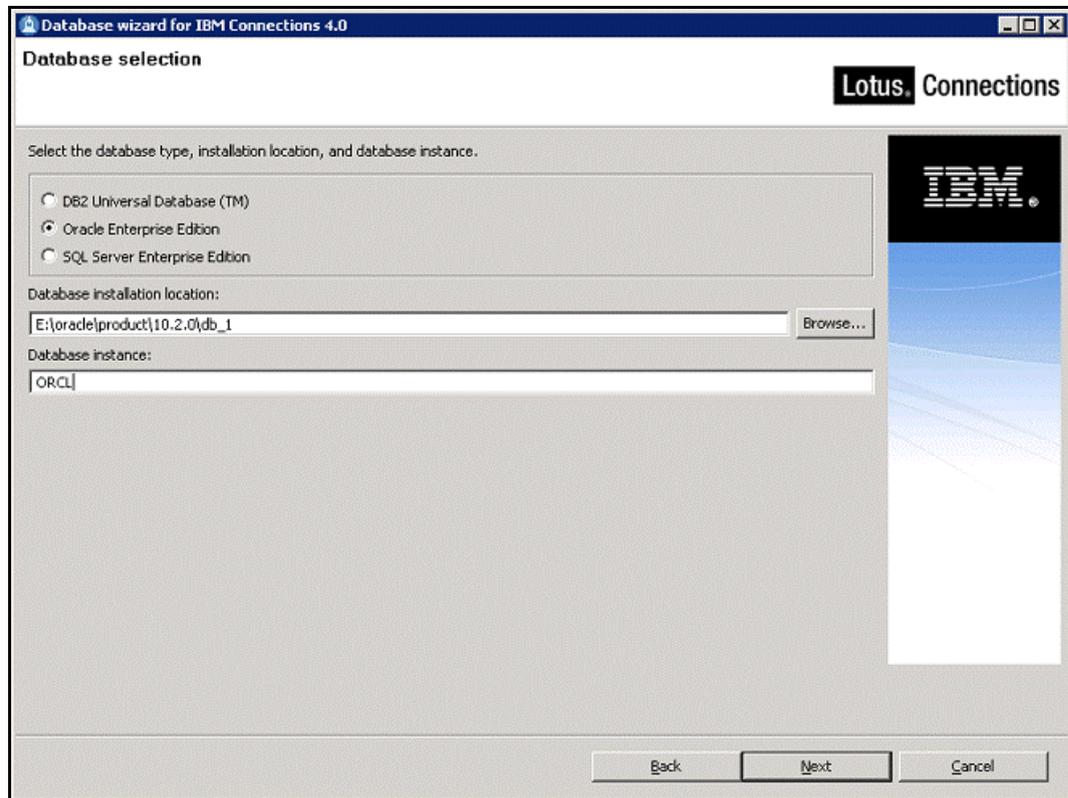


Figure 86. Database wizard for IBM Connections 4.0: Database selection screen

4. In the Applications selection screen, select the applications for which you want to create databases. In this example, all available options are selected. Click **Next**.

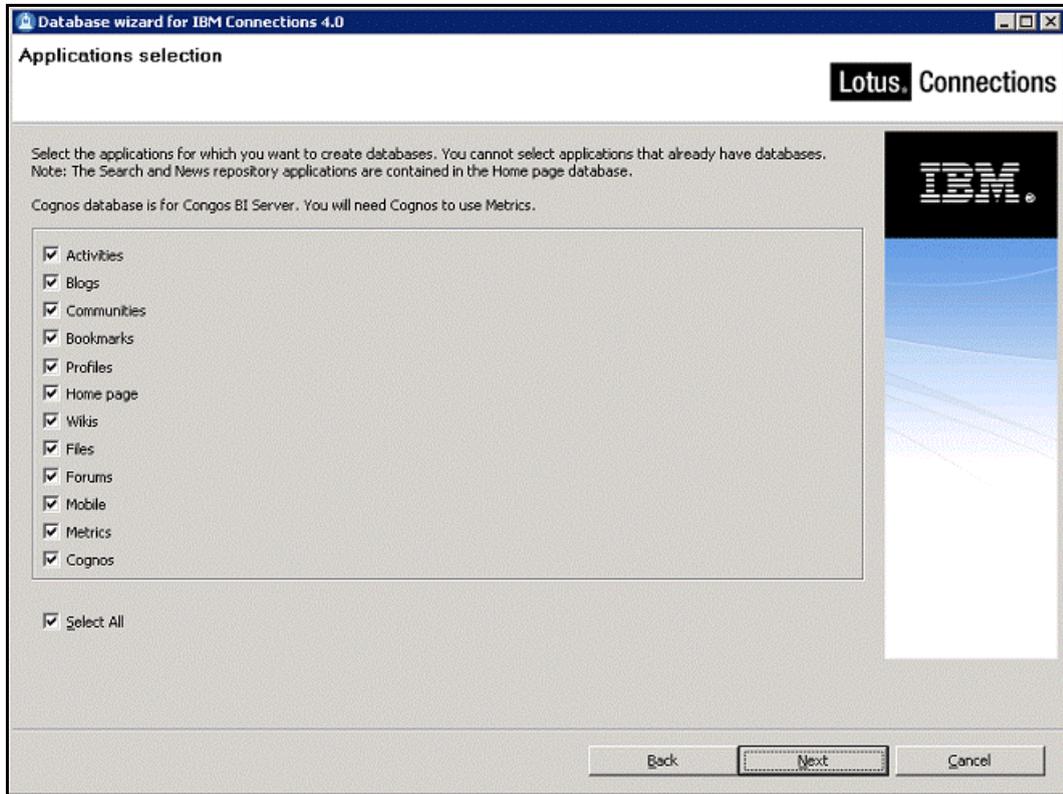


Figure 87. Database wizard for IBM Connections 4.0: Applications selection screen

- ___ 5. Introduce the password for all applications and click **Next**.

Database wizard for IBM Connections 4.0

Database authentication for applications

Lotus Connections

Specify the passwords for the database users.

Use the same password for all applications

Password: [masked] Confirm password: [masked]

Create different passwords for each application

	Database username	Password	Confirm password
Activities	OAUUSER		
Blogs	BLOGSUSER		
Communities	SINCOMMUSER		
Bookmarks	DOGEARUSER		
Home page	HOMEPAGEUSER		
Wikis	WIKISUSER		
Files	FILESUSER		
Forums	DFUSER		
Mobile	MOBILEUSER		
Metrics	METRICSUSER		
Cognos	COGNOS		

Back Next Cancel

Figure 88. Database wizard for IBM Connections 4.0: Database authentication for applications screen

___ 6. Review the pre-configuration task summary and click **Create**.

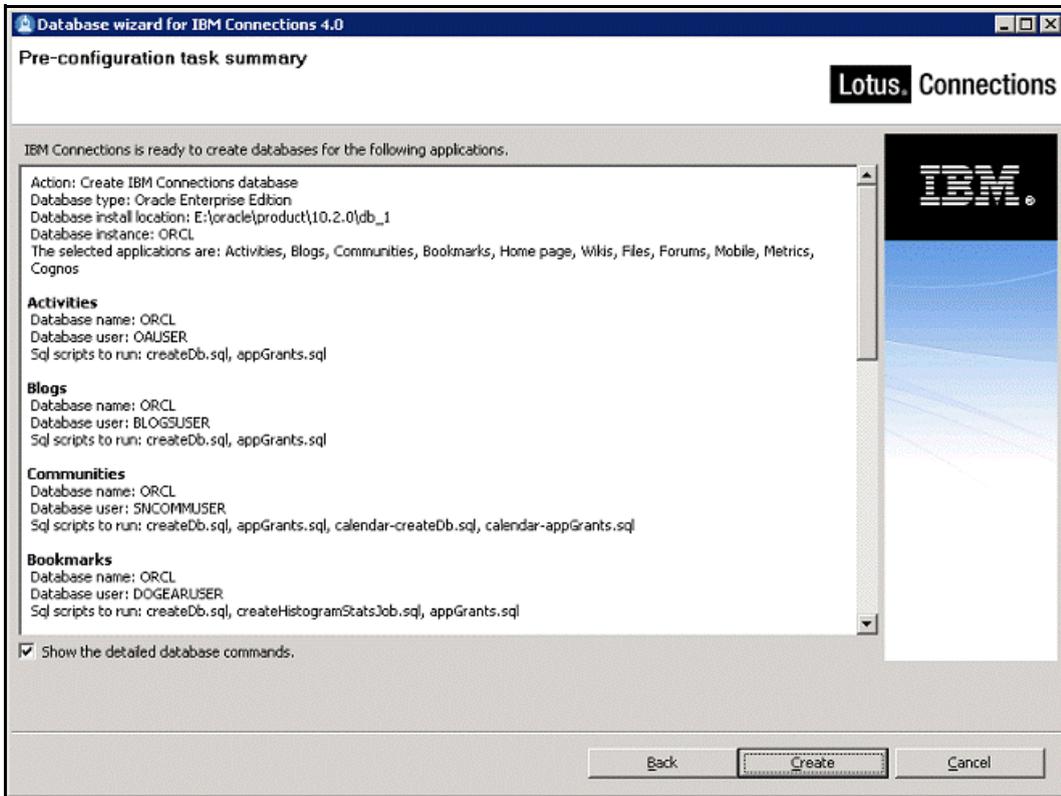


Figure 89. Database wizard for IBM Connections 4.0: Pre-configuration task summary screen

7. The commands screen is displayed. Click **Execute** to run them.

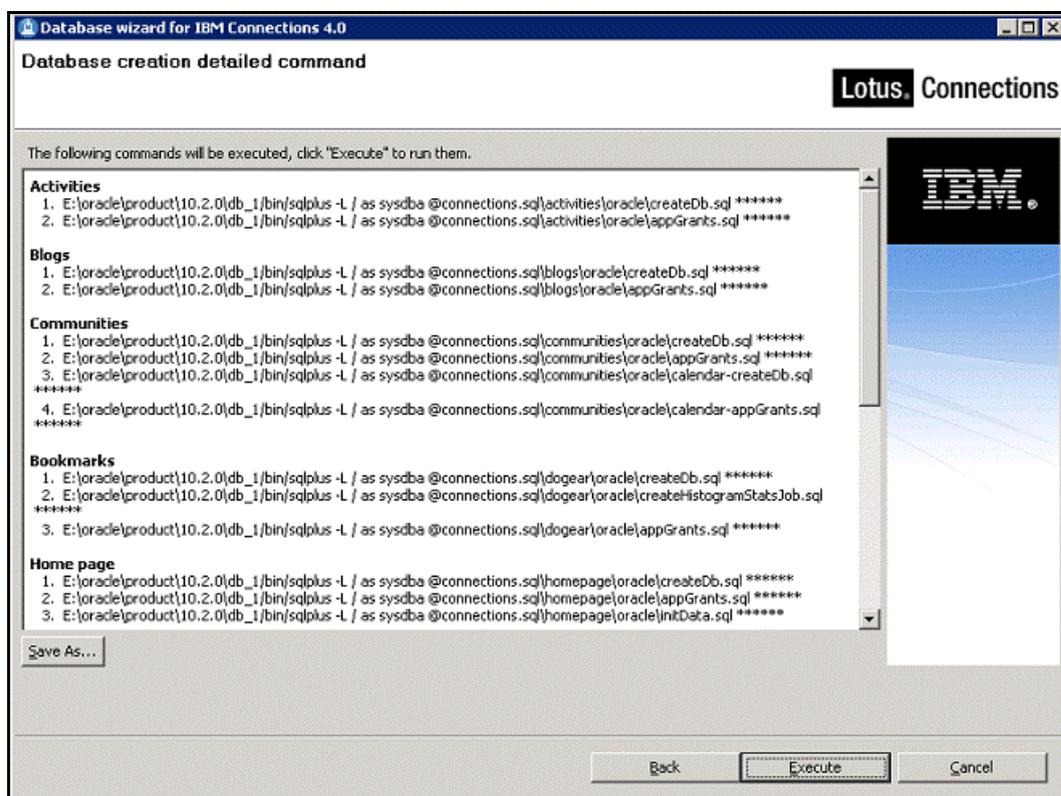


Figure 90. Database wizard for IBM Connections 4.0: Database creation detailed command screen

The database creation screen is displayed.

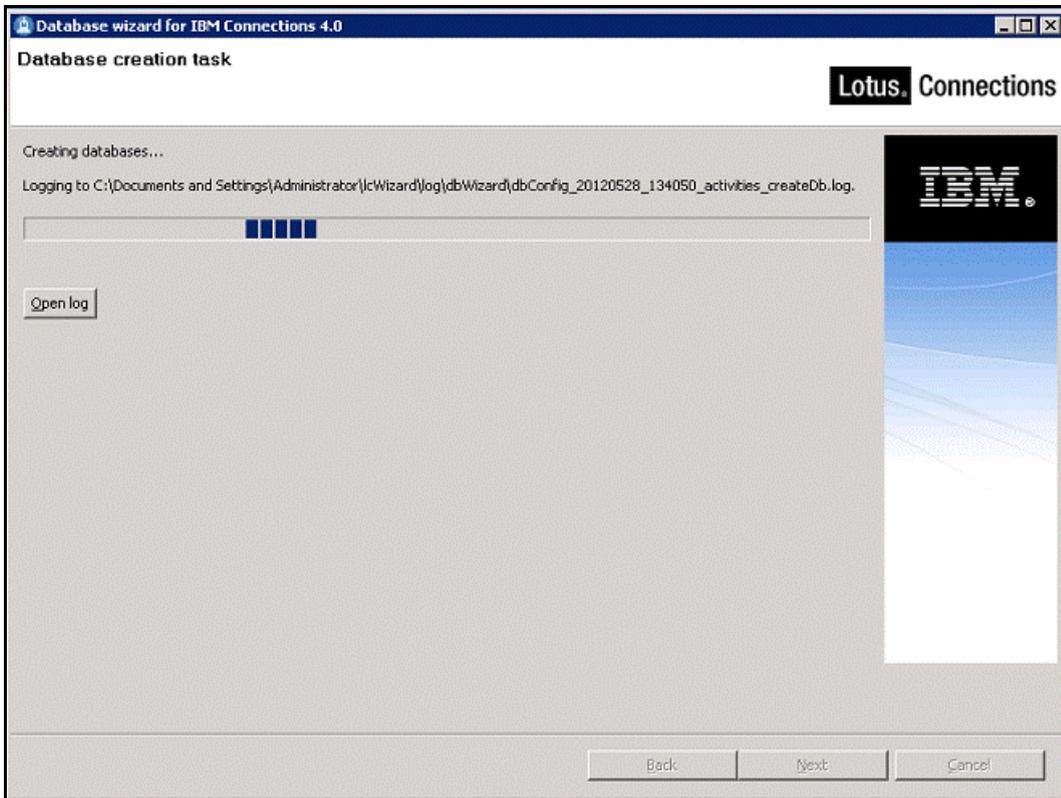


Figure 91. Database wizard for IBM Connections 4.0: Database creation task screen

8. When the database creation task completes, click **Finish**.

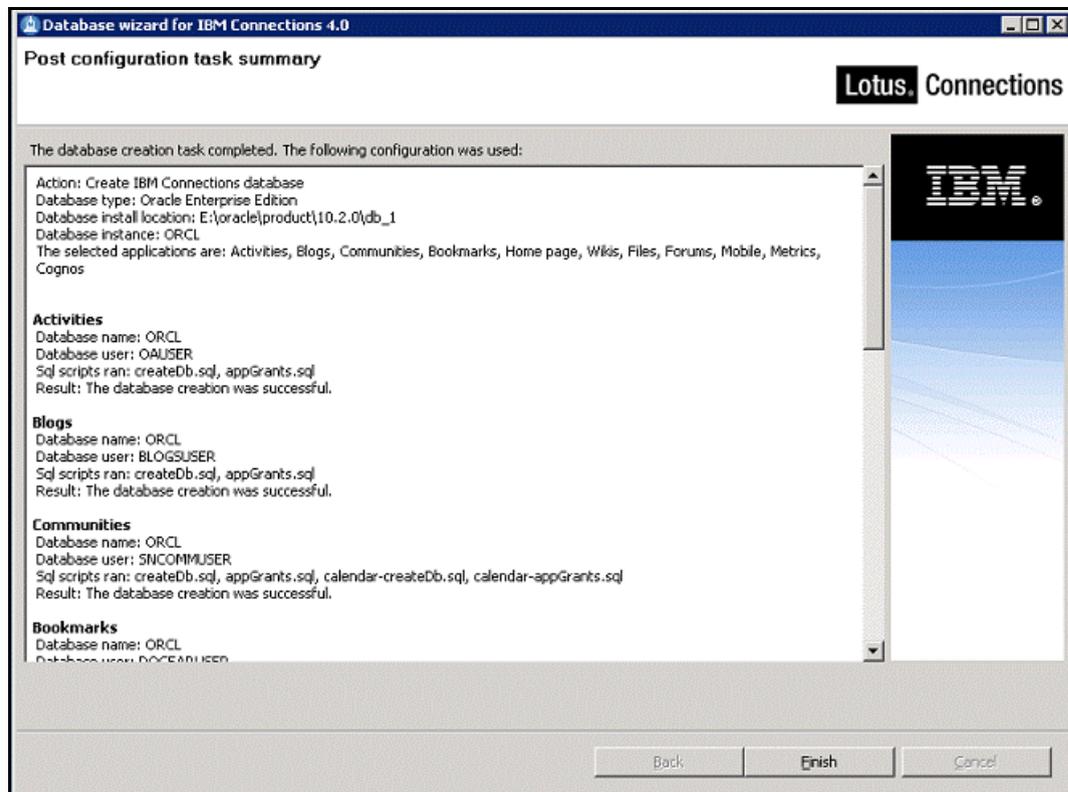


Figure 92. Database wizard for IBM Connections 4.0: Post configuration task summary screen



Information

Visit the following web page for further information:

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Creating_databases_with_the_database_wizard_ic40&content=pdcontent

Populating the Profiles database by using population wizard

Follow these steps to populate the Profiles database by using the population wizard:

1. Open the Profiles population wizard for IBM Connections 4.0 and click **Next**.

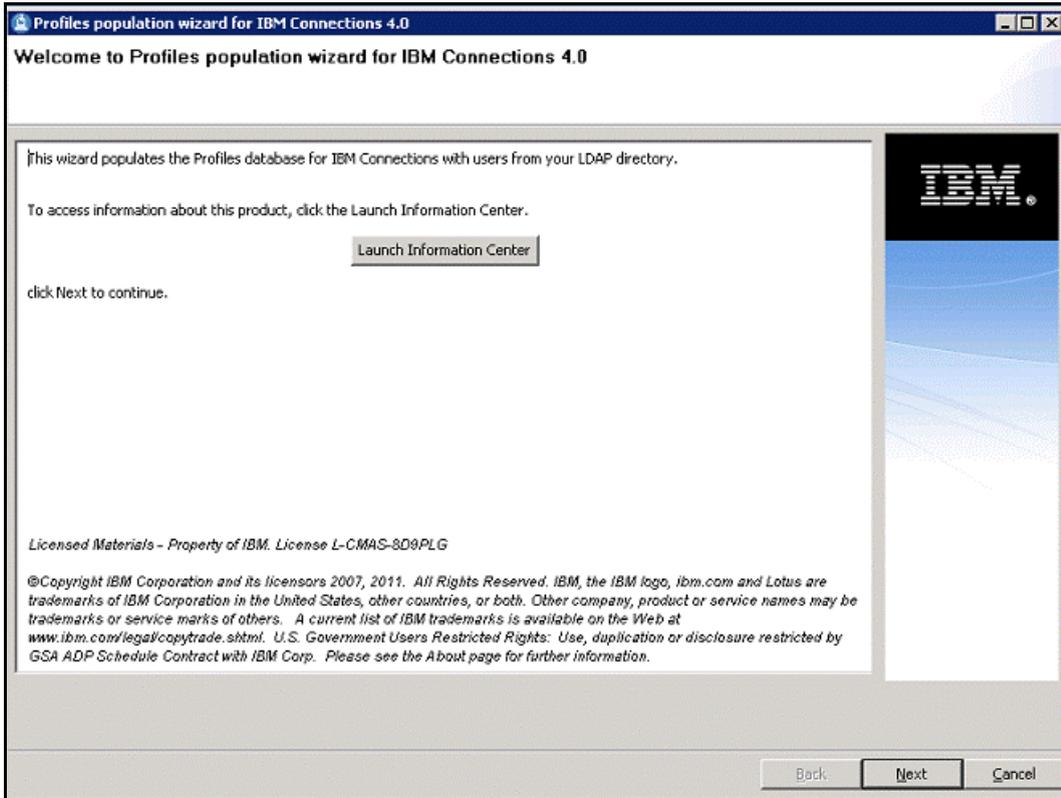


Figure 93. Profiles population wizard for IBM Connections 4.0

- ___ 2. Select the location of the Tivoli Integrator installation directory and click **Next**.

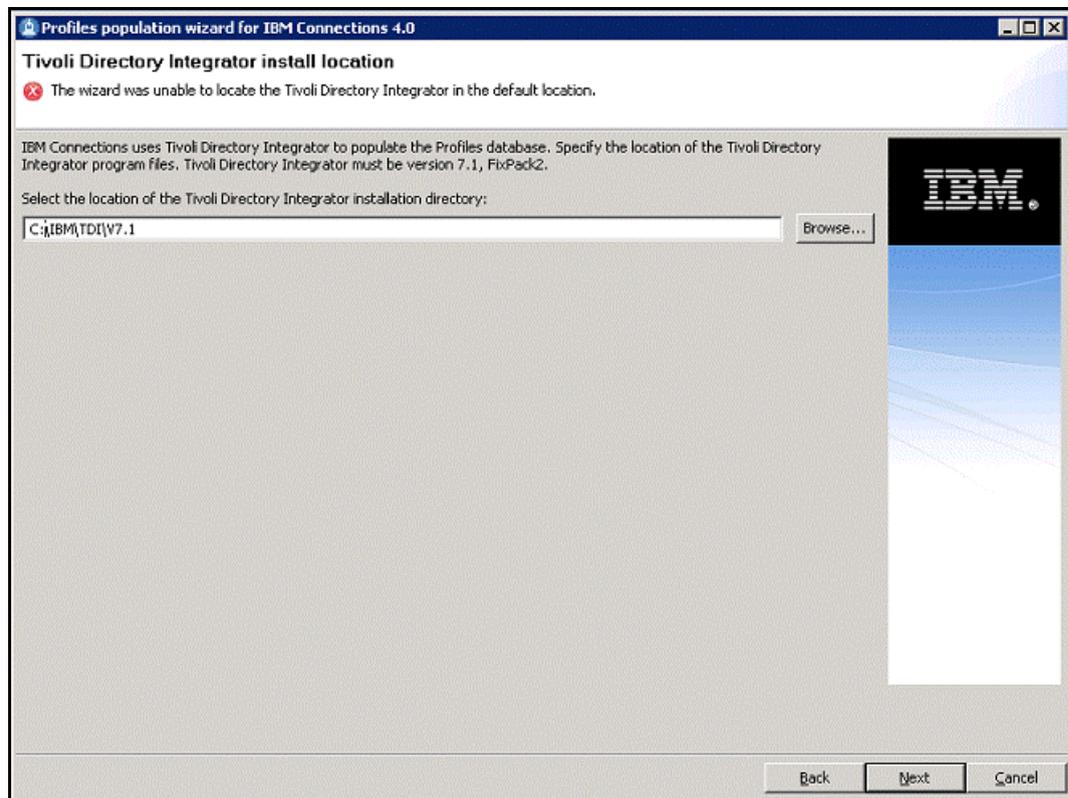


Figure 94. Profiles population wizard for IBM Connections 4.0: Tivoli Directory Integrator installation location screen

- ___ 3. Select Oracle Enterprise Edition as the profiles database type and click **Next**.

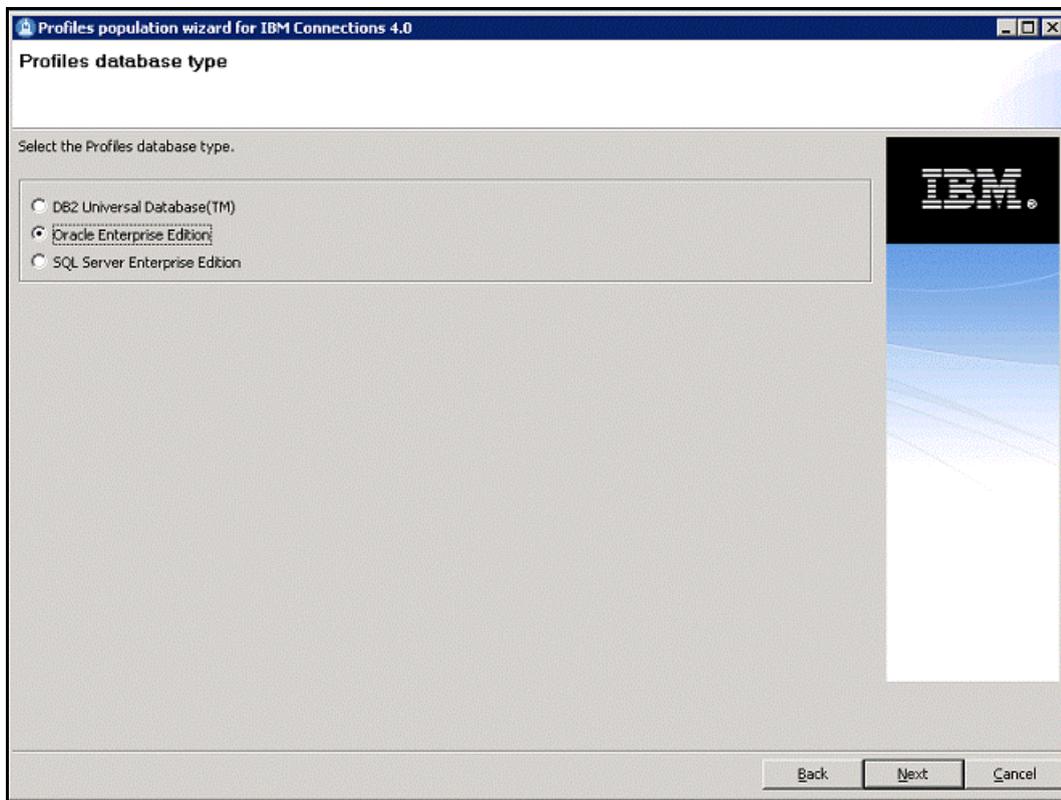
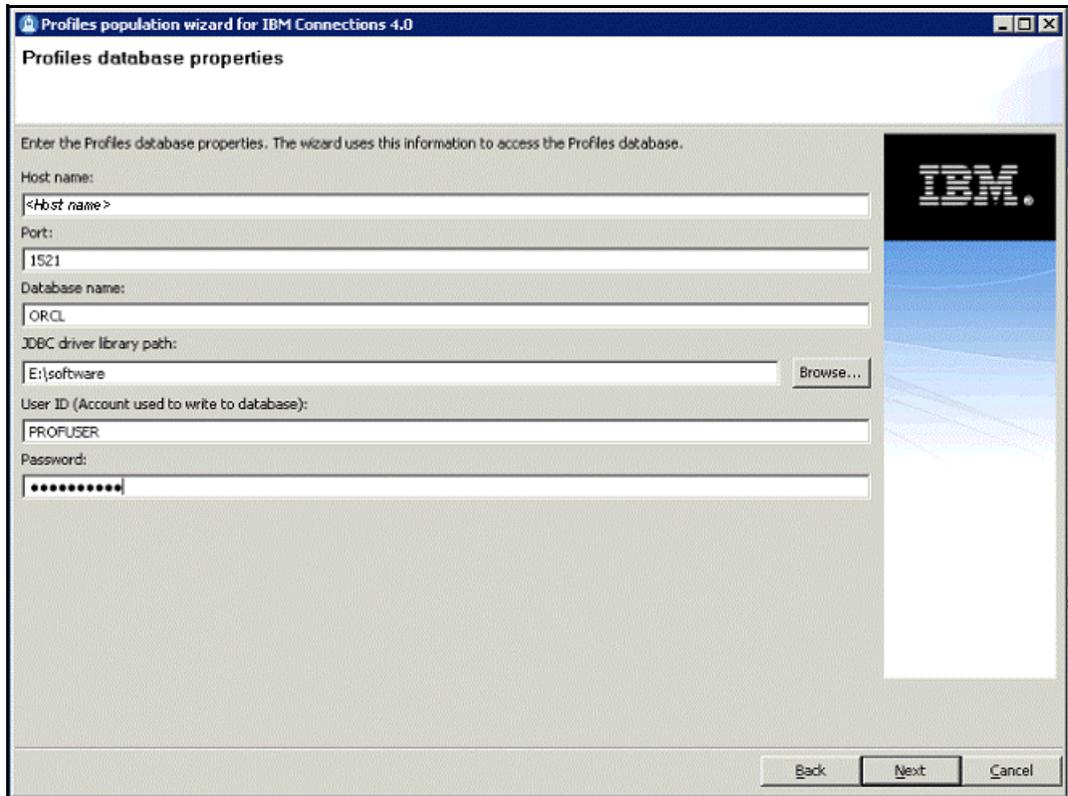


Figure 95. Profiles population wizard for IBM Connections 4.0: Profiles database type screen

- ___ 4. Enter the profiles database properties and click **Next**.



The screenshot shows a window titled "Profiles population wizard for IBM Connections 4.0". The main heading is "Profiles database properties". Below this, a message states: "Enter the Profiles database properties. The wizard uses this information to access the Profiles database." The form contains the following fields and controls:

- Host name: A text box containing the placeholder text "<Host name>".
- Port: A text box containing the value "1521".
- Database name: A text box containing the value "ORCL".
- JDBC driver library path: A text box containing "E:\software" and a "Browse..." button to its right.
- User ID (Account used to write to database): A text box containing the value "PROFUSER".
- Password: A text box filled with ten dots, indicating a masked password.

At the bottom right of the window, there are three buttons: "Back", "Next", and "Cancel". An IBM logo is visible on the right side of the window's content area.

Figure 96. Profiles population wizard for IBM Connections 4.0: Profiles database properties screen

- ___ 5. Specify the LDAP host name and port to enable the Profiles population wizard to connect to the LDAP server and click **Next**.

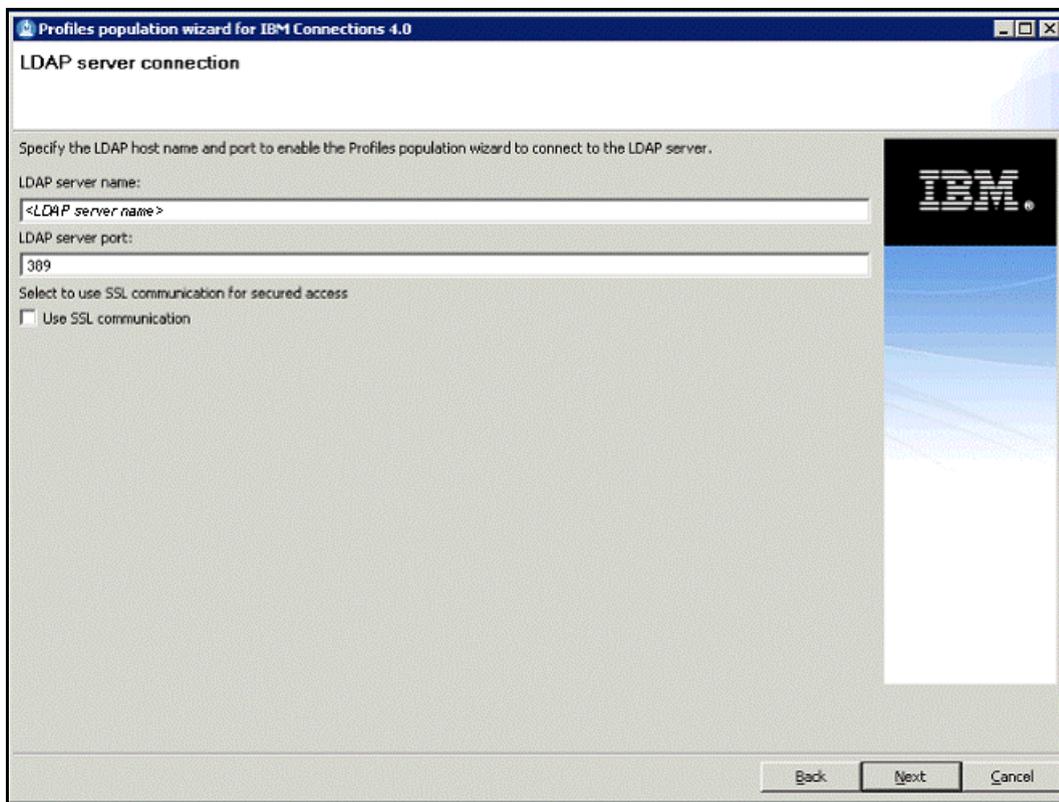
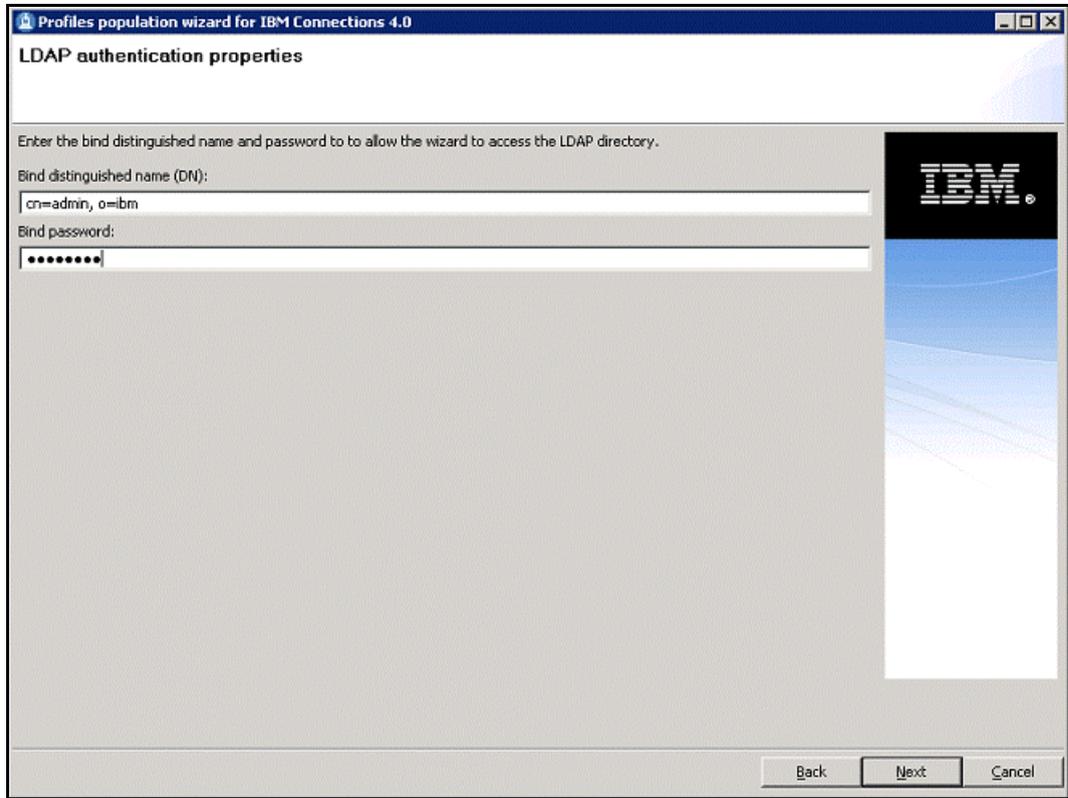


Figure 97. Profiles population wizard for IBM Connections 4.0: LDAP server connection screen

- ___ 6. Enter the bind distinguished name and password to allow the wizard to access the LDAP directory and click **Next**.



The screenshot shows a window titled "Profiles population wizard for IBM Connections 4.0" with the subtitle "LDAP authentication properties". The main text reads: "Enter the bind distinguished name and password to allow the wizard to access the LDAP directory." Below this, there are two input fields. The first is labeled "Bind distinguished name (DN):" and contains the text "cn=admin, o=ibm". The second is labeled "Bind password:" and contains a series of dots. To the right of the input fields is a vertical panel with the IBM logo at the top and a blue gradient background below. At the bottom of the window, there are three buttons: "Back", "Next", and "Cancel".

Figure 98. Profiles population wizard for IBM Connections 4.0: LDAP authentication properties screen

7. Enter the base distinguished name and filter for this wizard to begin searching for users in the LDAP directory tree and click **Next**.

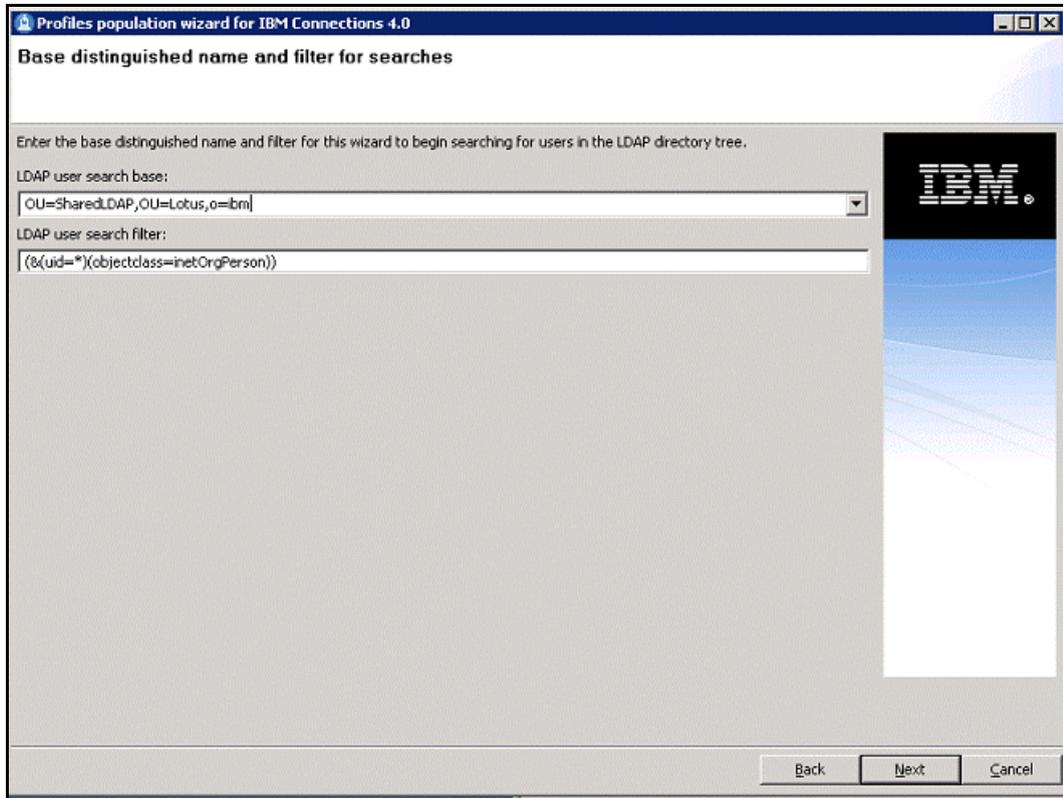


Figure 99. Profiles population wizard for IBM Connections 4.0: Base distinguished name and filter for searches screen

- ___ 8. Select an LDAP attribute or a JavaScript function for each field in the Profiles database and click **Next**.

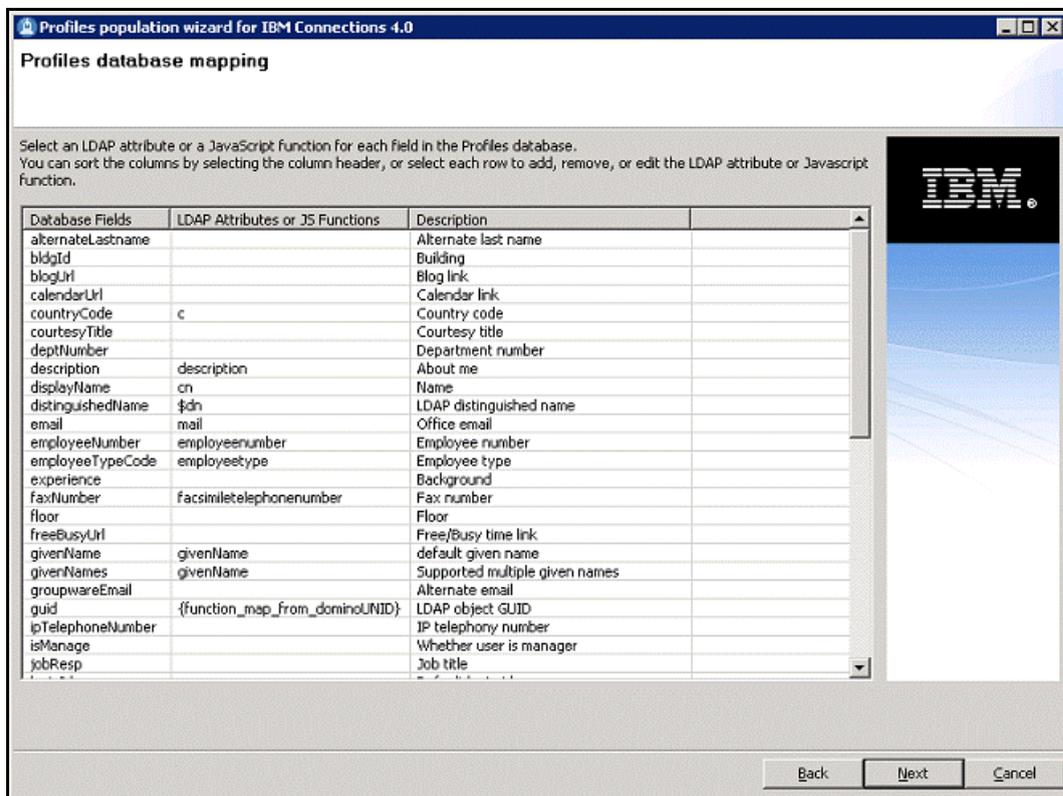


Figure 100. Profiles population wizard for IBM Connections 4.0: Profiles database mapping

9. Select each type of optional information that you want to add and click **Next**.

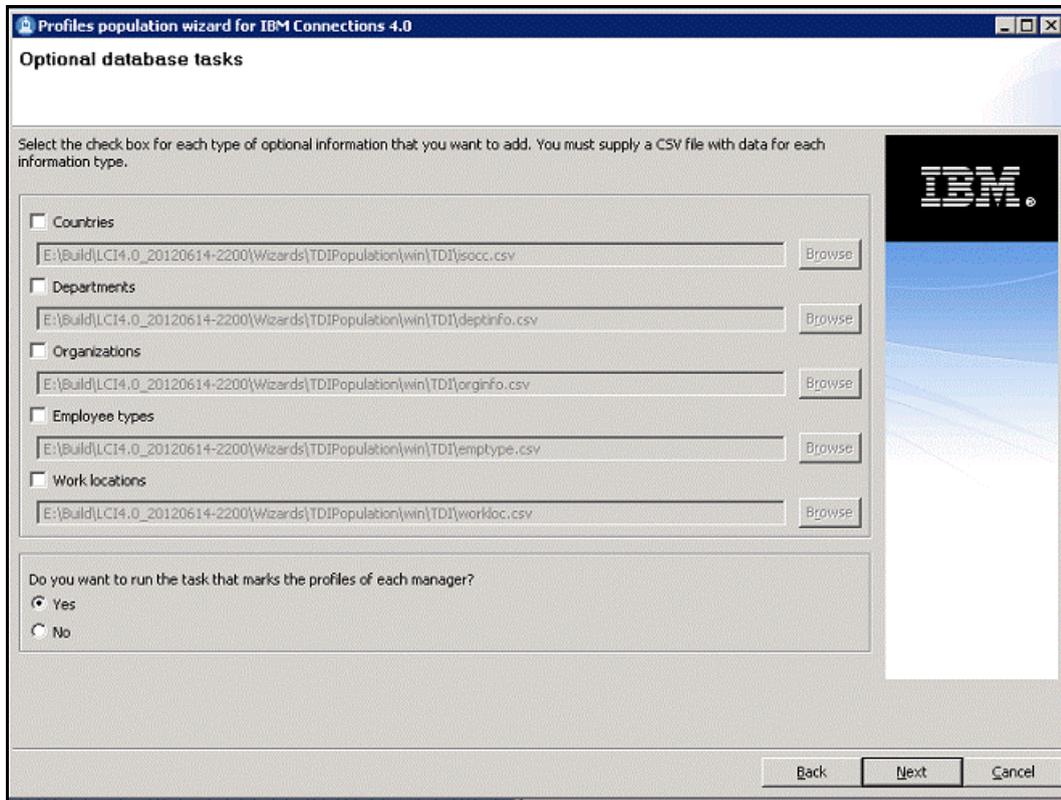


Figure 101. Profiles population wizard for IBM Connections 4.0: Optional database tasks

The population task starts populating.

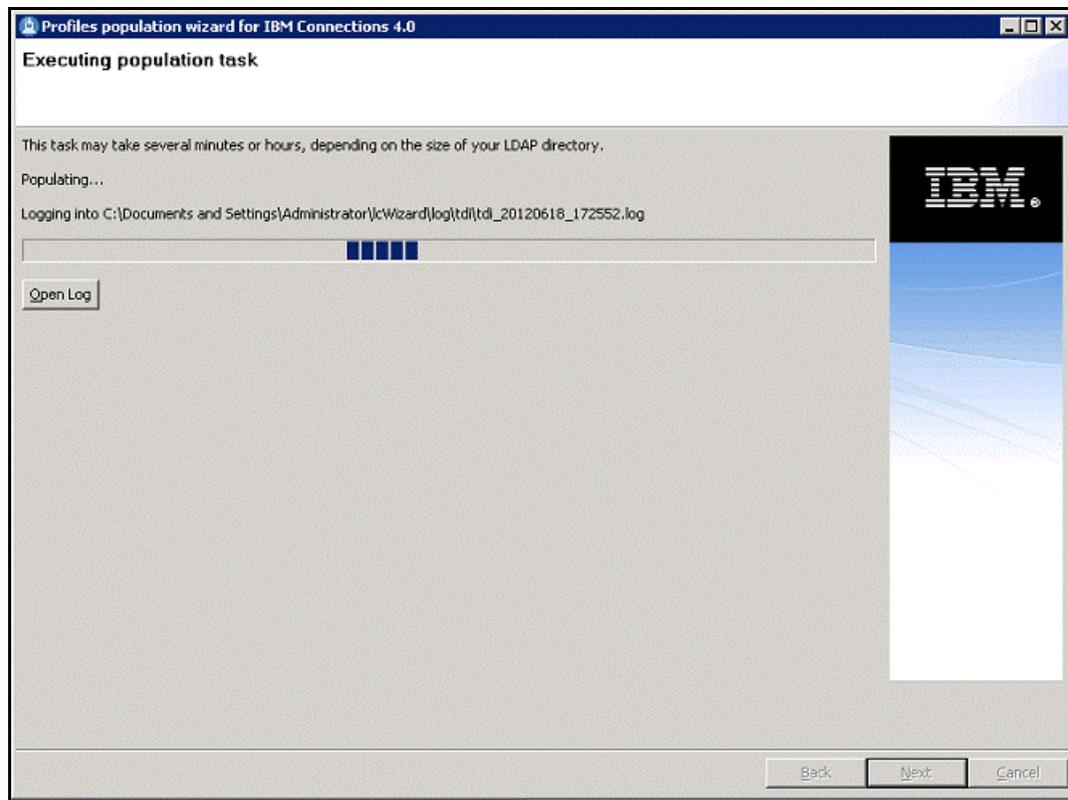


Figure 102. Profiles population wizard for IBM Connections 4.0: Population task execution screen

___ 10. Review the population completion summary. Click **Finish**.

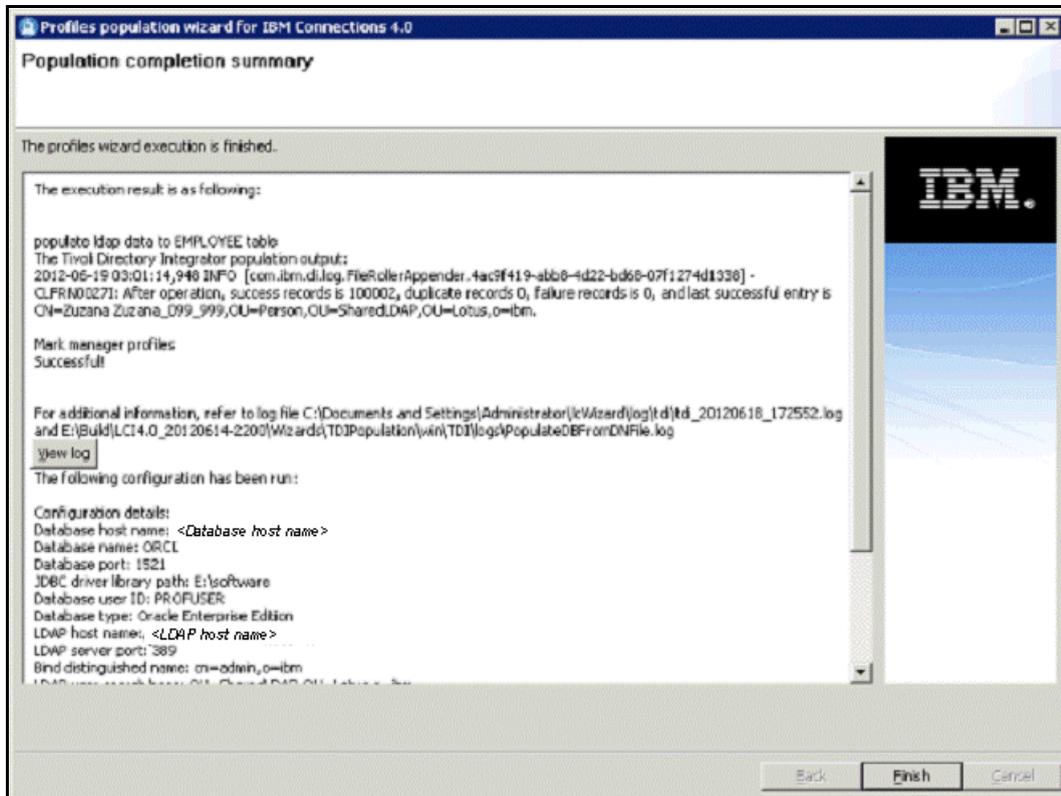


Figure 103. Profiles population wizard for IBM Connections 4.0: Population completion summary screen



Information

Visit the following web page for further information:

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Populating_the_Profiles_database_ic40&content=pdcontent

Preparing a shared folder and local folder on Deployment Manager/Node computers

To prepare a shared folder and local folders on Deployment Manager/Node computers, follow these steps:

1. Select one folder location as Connections shared folder and make it accessible to all Deployment Manager/Node computers by using the same format.



Example

`\\connections.example.com\LCShare.`

2. On each node computer, create a local folder in the same location to work as Connections local folder.



Example

`C:\IBM\LCLocal.`

2. Installing IBM Connections 4.0 using LC wizard

Follow these steps to install IBM Connections 4.0 using LC wizard:

1. Open the IBM Connections 4.0.0 wizard.

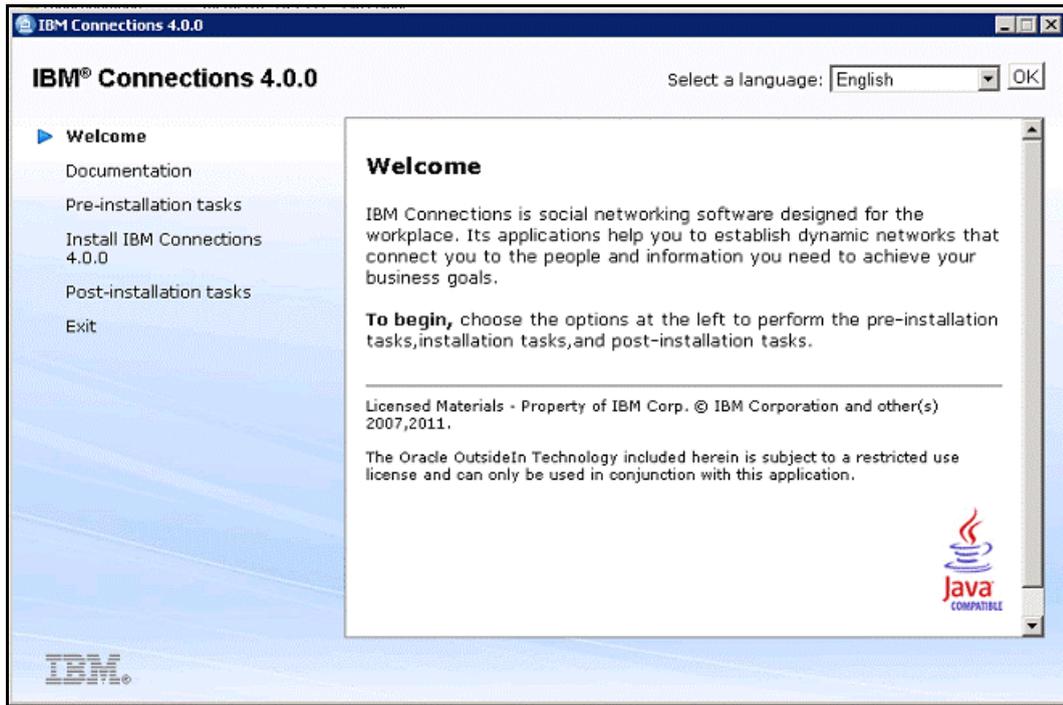


Figure 104. IBM Connections 4.0.0 wizard: Welcome Screen

2. Click **Install IBM Connections 4.0.0**.

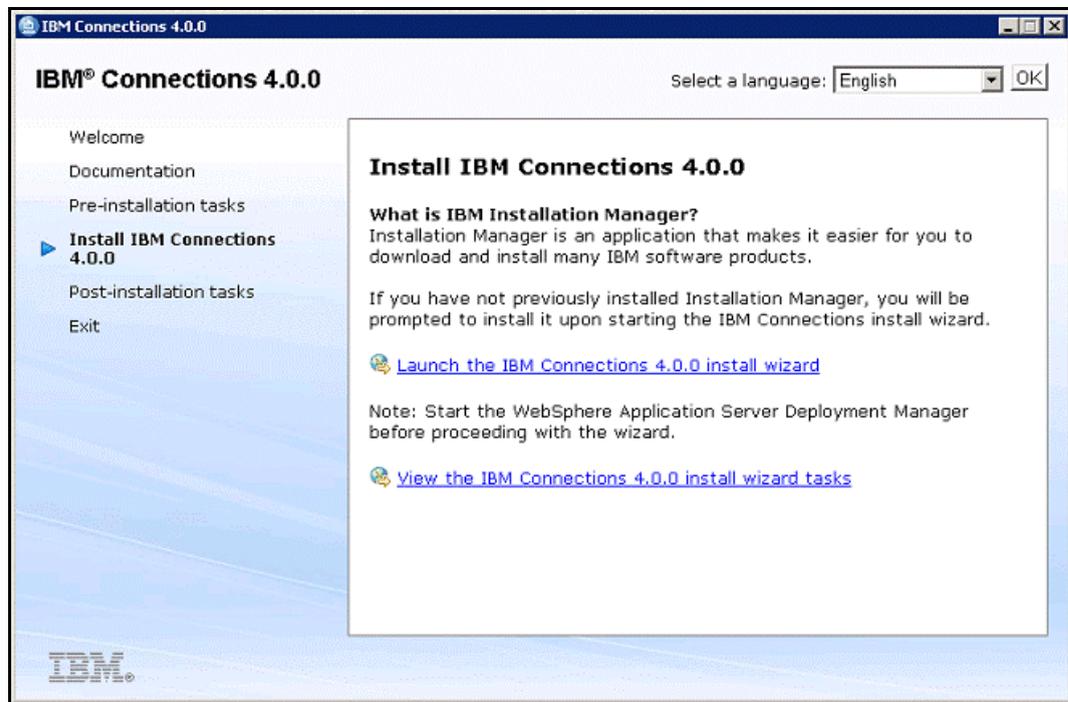


Figure 105. IBM Connections 4.0.0: Install IBM Connections 4.0.0

3. Select the packages to install and click **Next**.

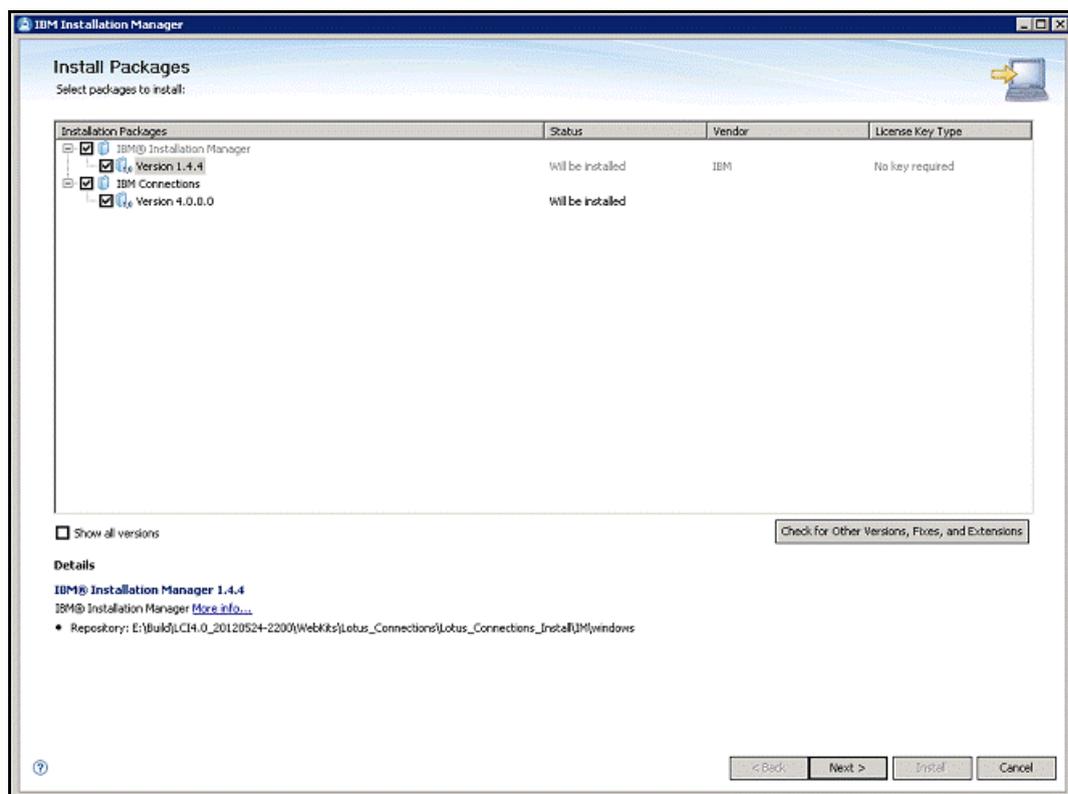


Figure 106. IBM Connections 4.0.0: Install Packages screen

4. Accept the license agreements carefully and click **Next**.

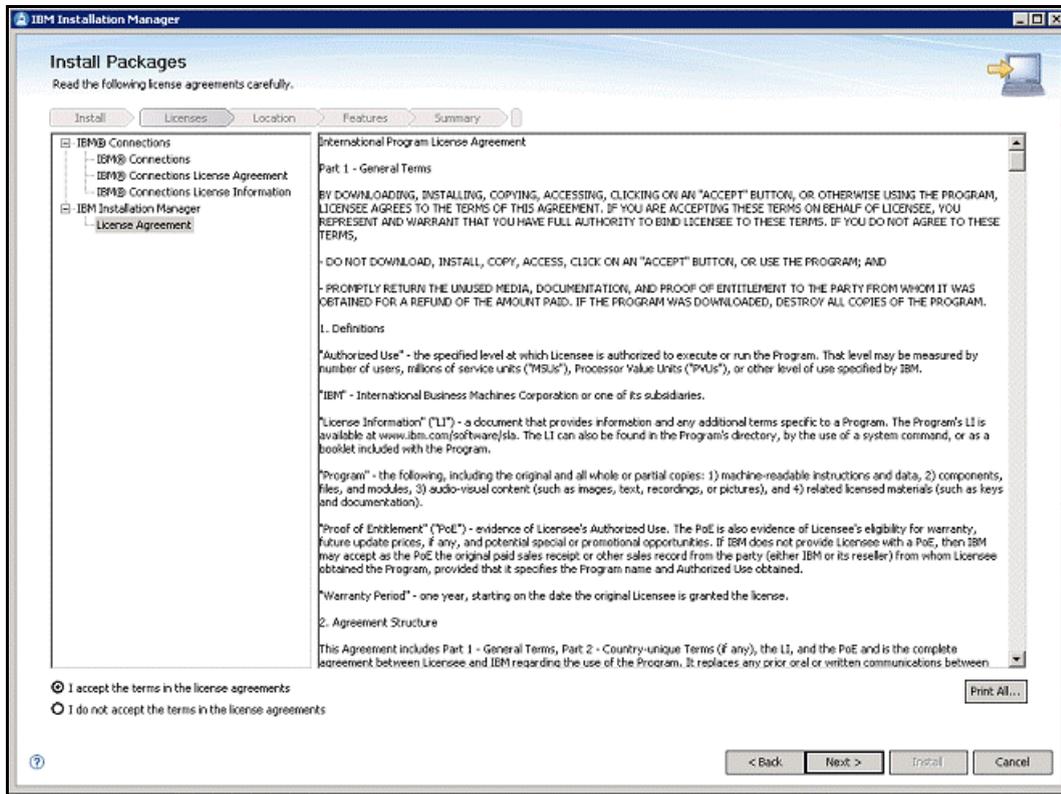


Figure 107. IBM Connections 4.0.0: Install Packages screen: License agreements

- ___ 5. Select a location for the shared resources directory and a location for Installation Manager and click **Next**.

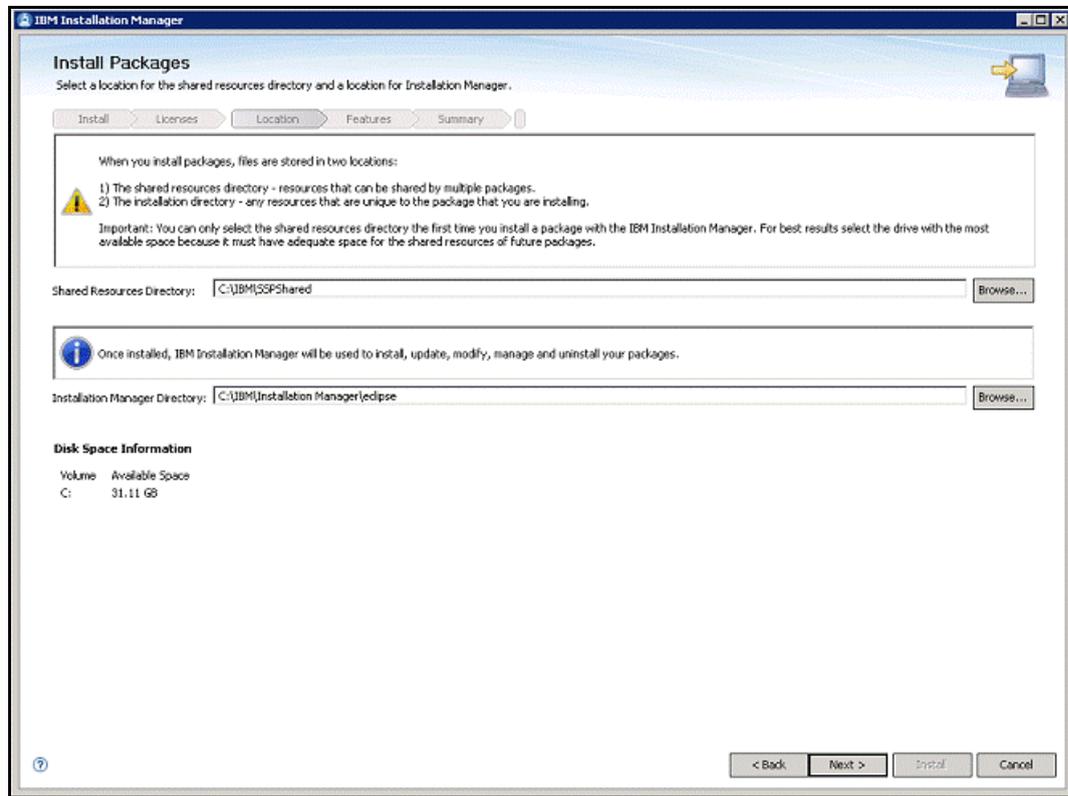


Figure 108. IBM Connections 4.0.0: Install Packages screen: Location selection

- ___ 6. If wanted, create a package group by selecting **Create a new package group** and click **Next**.

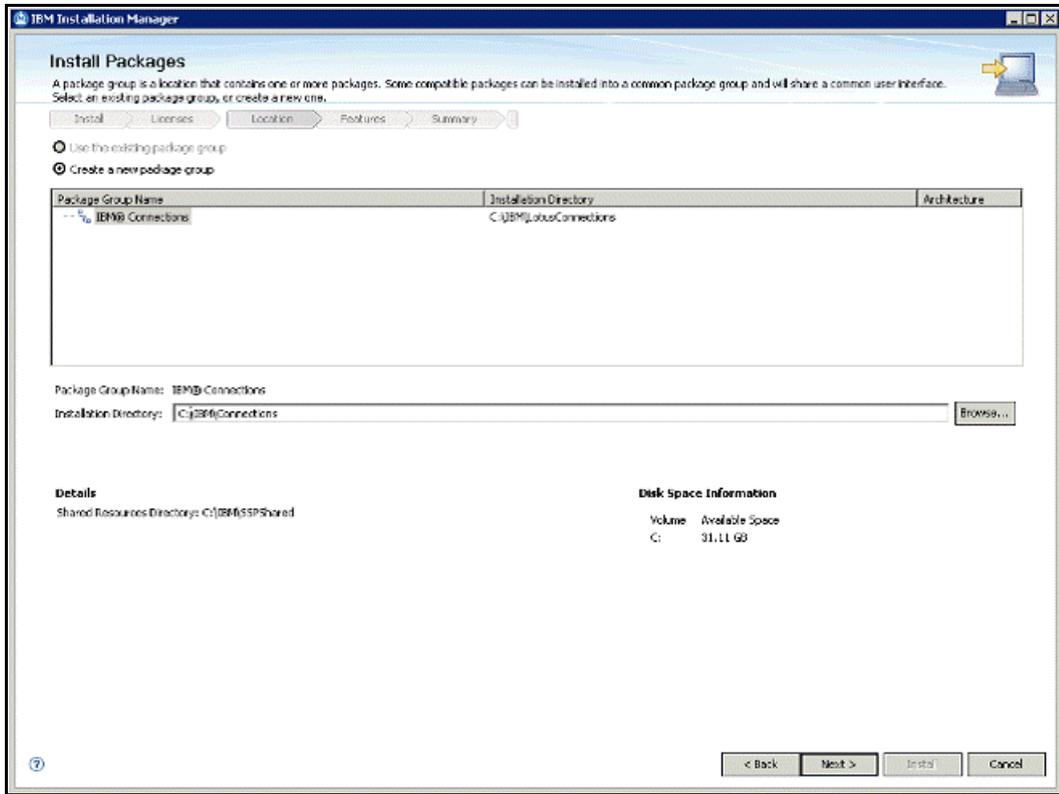


Figure 109. IBM Connections 4.0.0: Install Packages screen: Create package group

7. Select the features that you want to install and click **Next**.

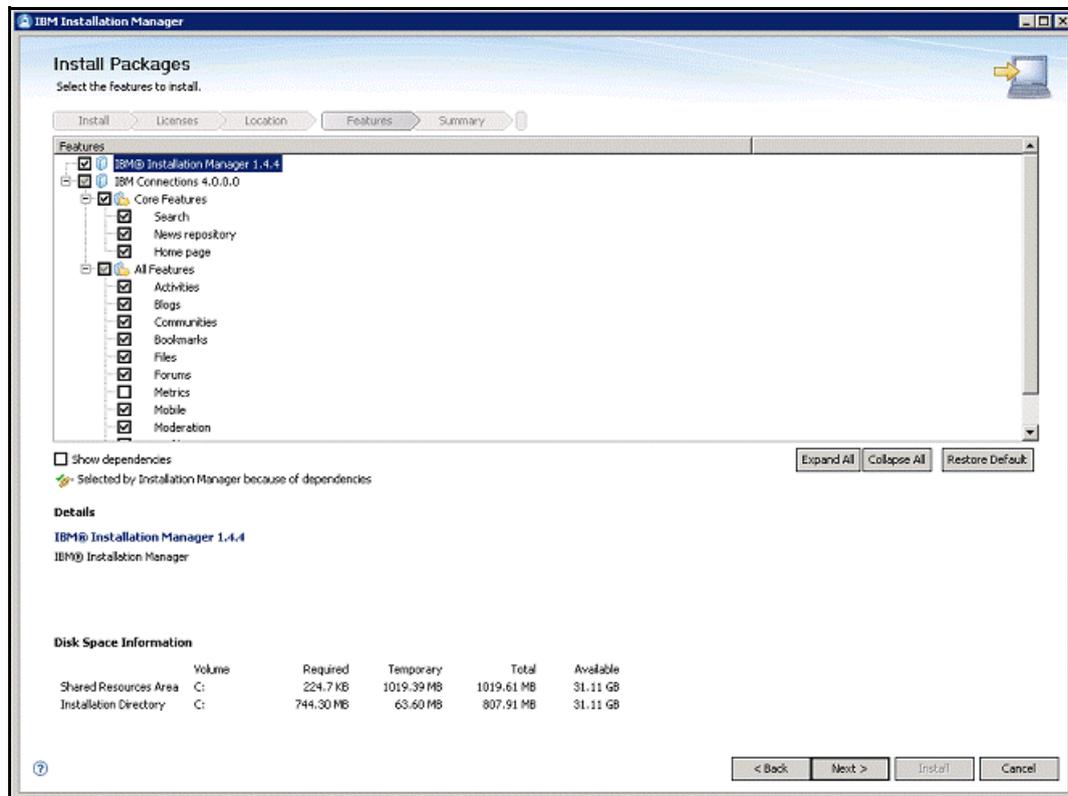


Figure 110. IBM Connections 4.0.0: Install Packages screen: Features to install

8. Complete the configurations for the packages.

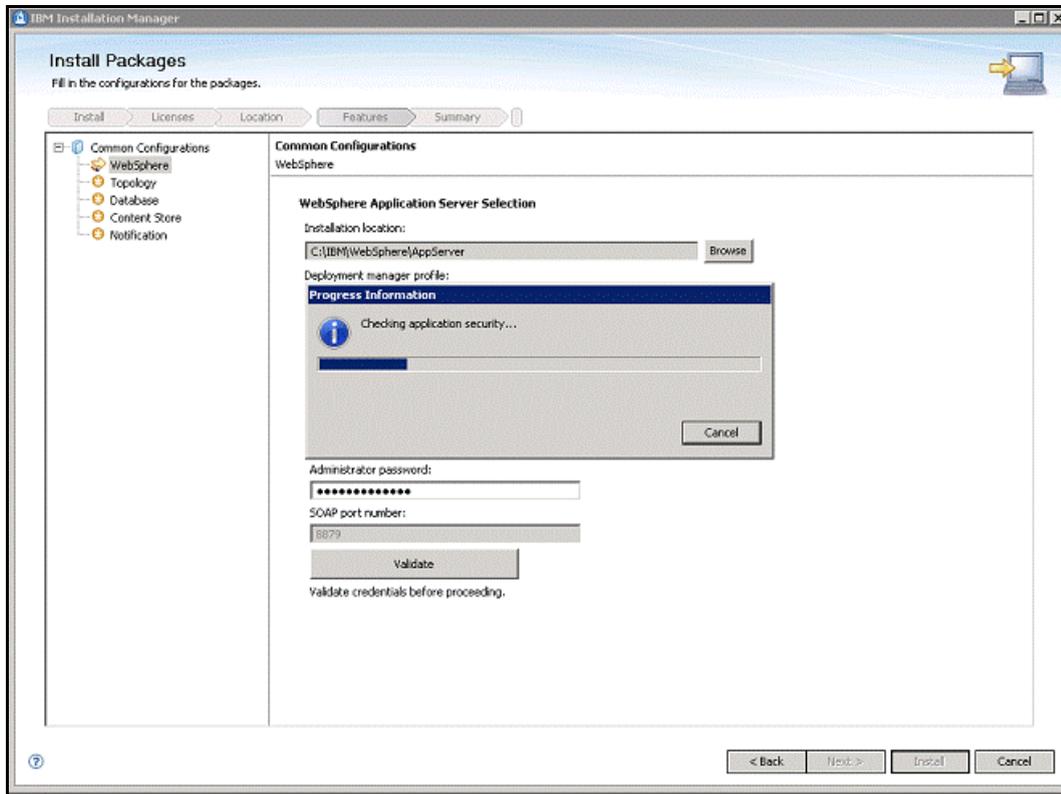


Figure 111. IBM Connections 4.0.0: Install Packages screen: WebSphere configurations

- ___ 9. Enter the host name and the deployment manager credentials.

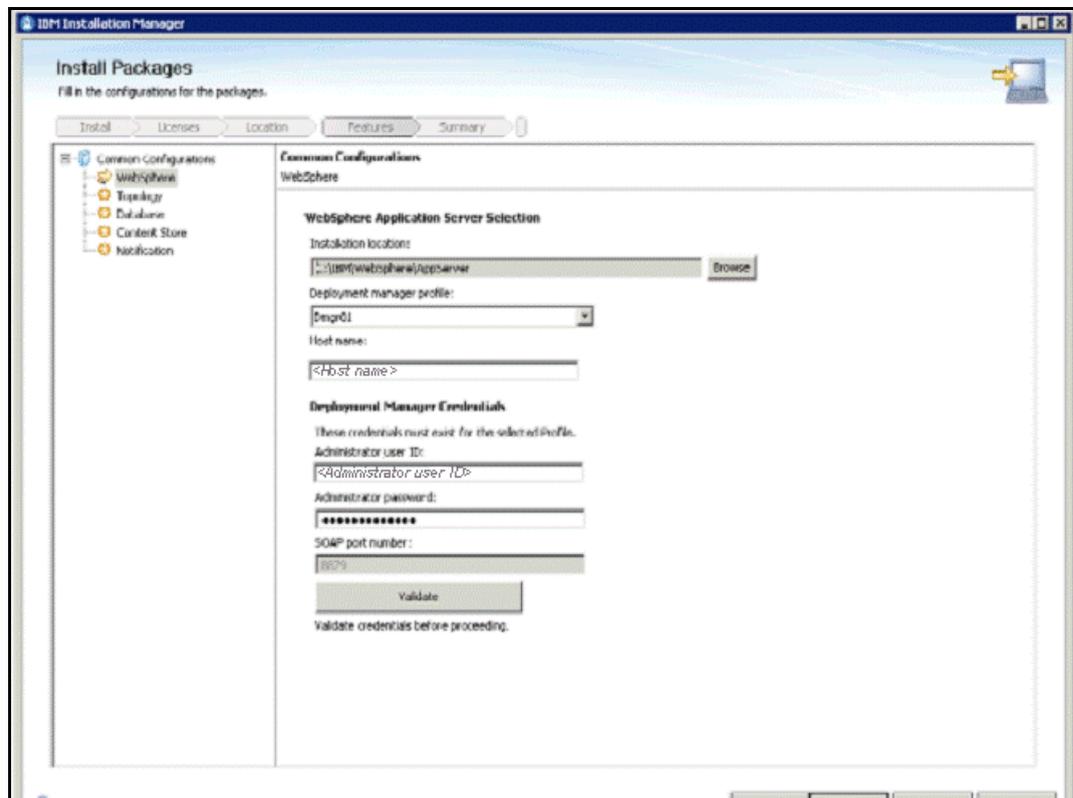


Figure 112. IBM Connections 4.0.0: Install Packages screen: Host name and credentials

- ___ 10. In the Topology screen, select **Small: All applications are grouped in the same cluster as deployment type**.

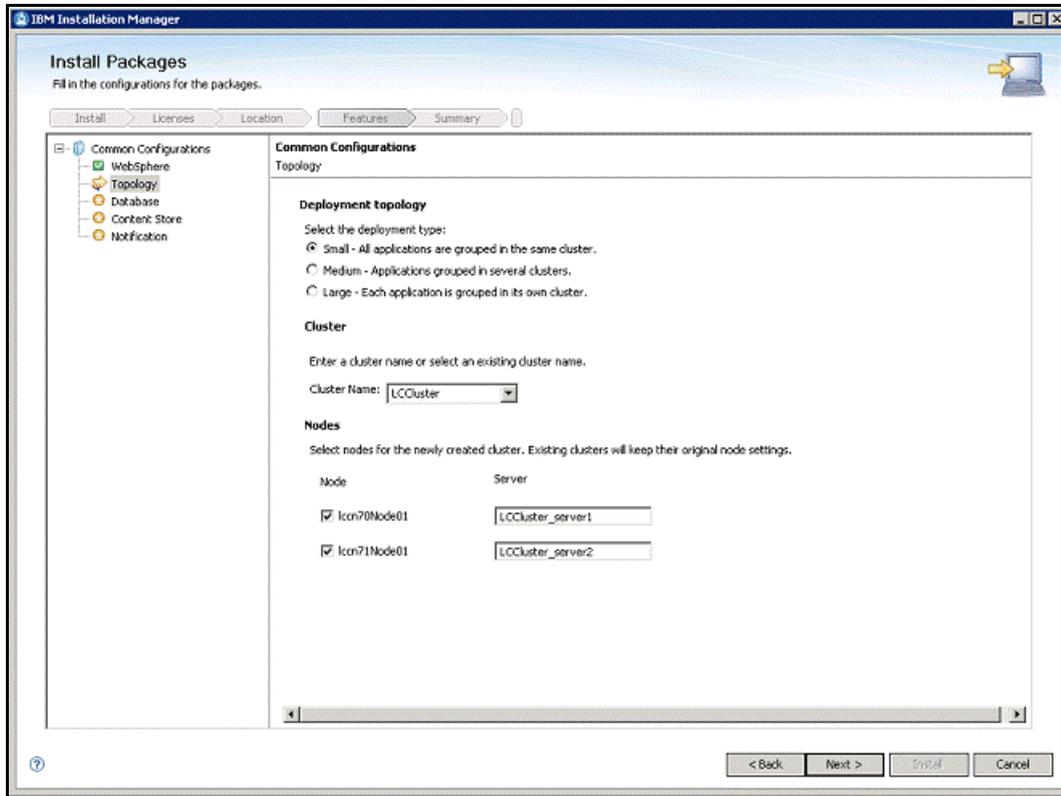


Figure 113. IBM Connections 4.0.0: Install Packages screen: Topology configurations

- ___ 11. In the Database screen, select **Yes, the applications are on the same database instance for the database location.**

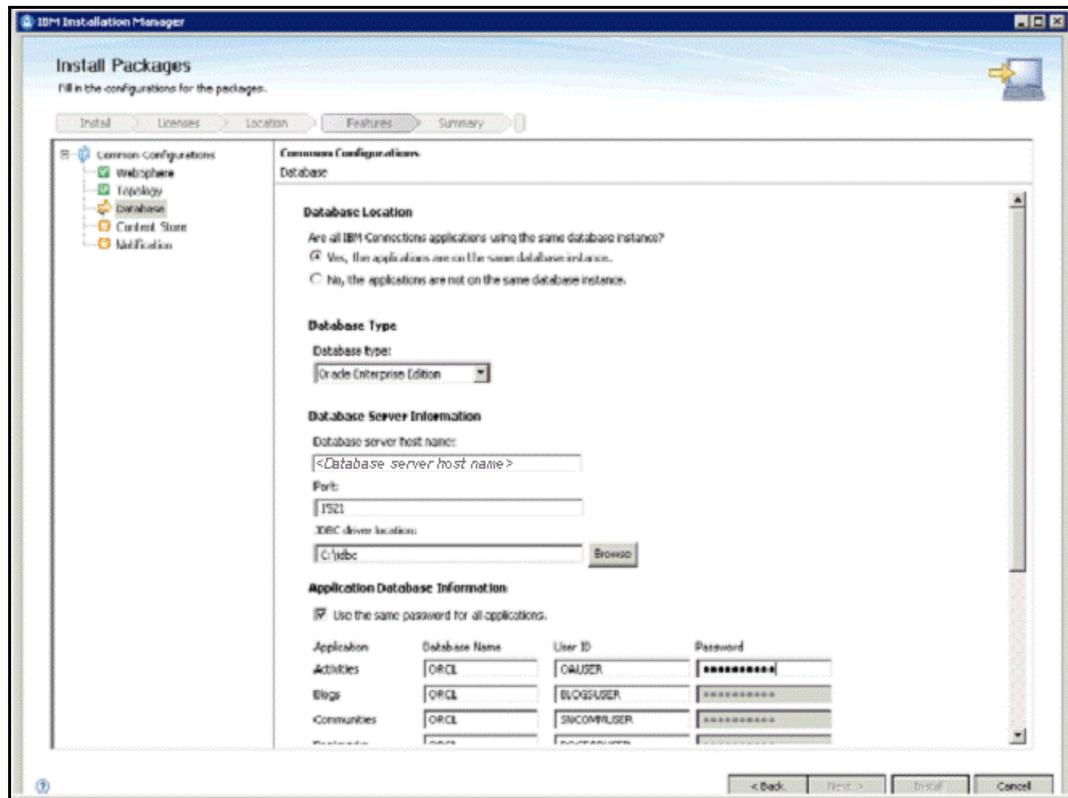


Figure 114. IBM Connections 4.0.0: Install Packages screen: Database configurations

The ORCL database starts validating.

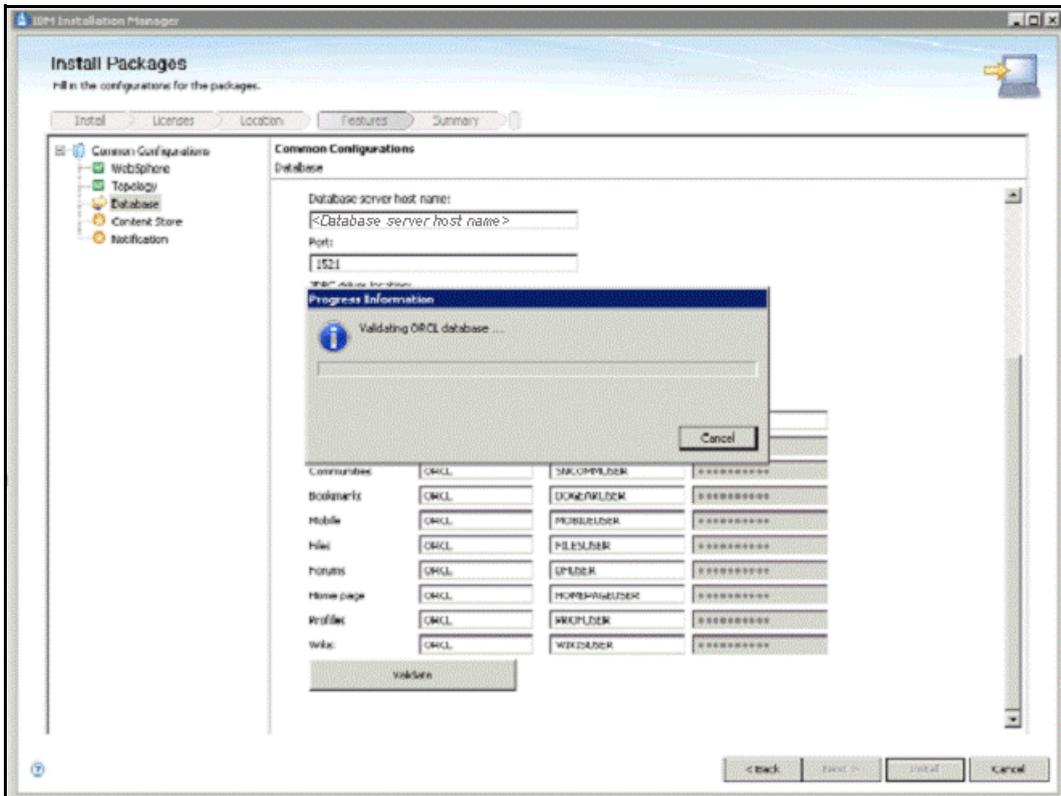


Figure 115. IBM Connections 4.0.0: Install Packages screen: Database validation

- ___ 12. In the Content Store screen, select a network shared location and a local content store.

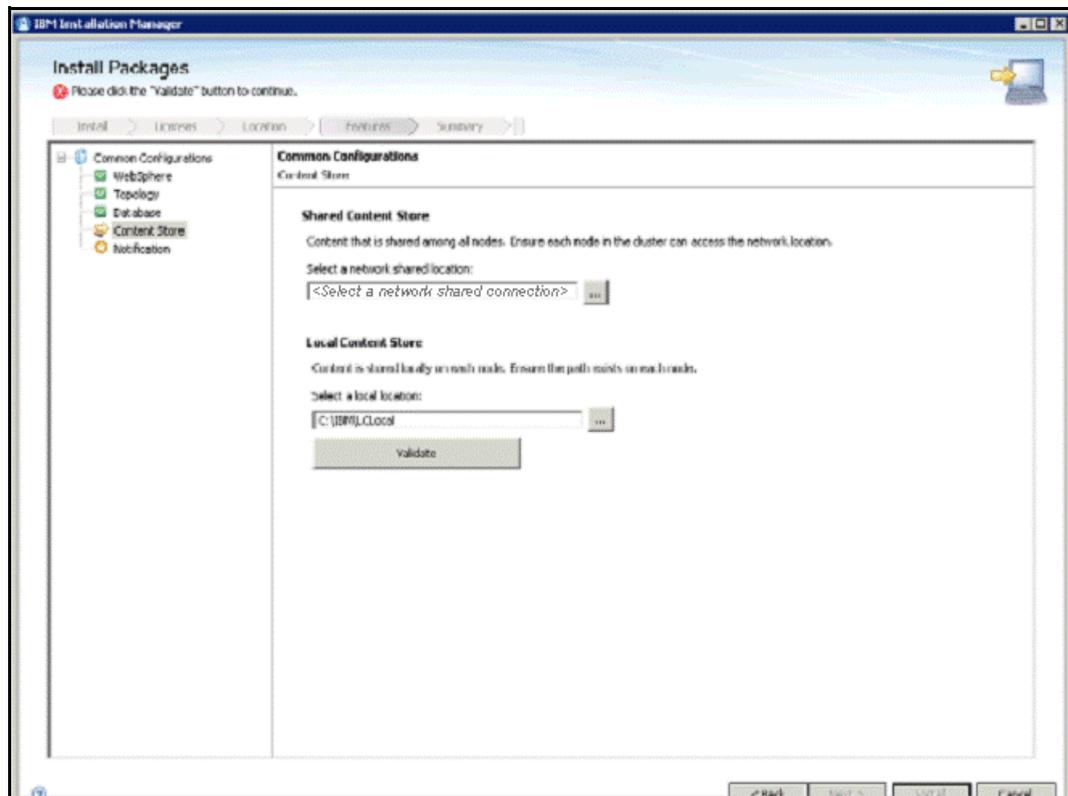


Figure 116. IBM Connections 4.0.0: Install Packages screen: Content Store configurations

___ 13. Configure the notification settings as shown in the following two figures and click **Next**.

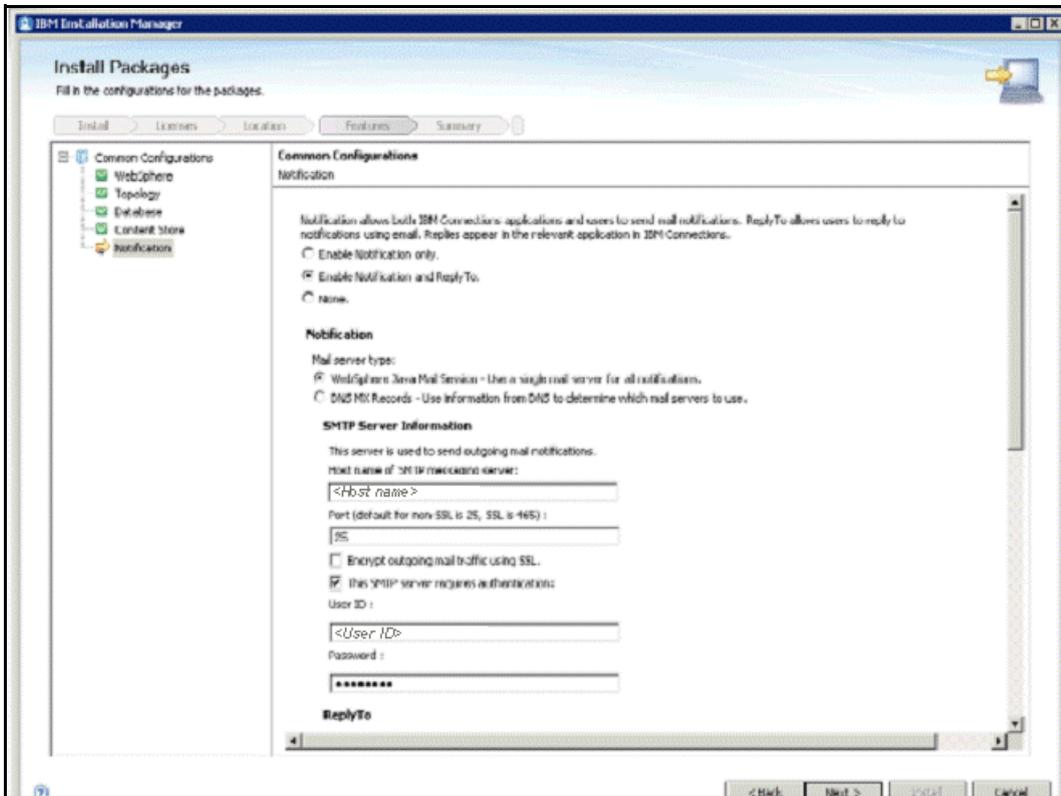


Figure 117. IBM Connections 4.0.0: Install Packages screen: Notification settings (1 of 2)

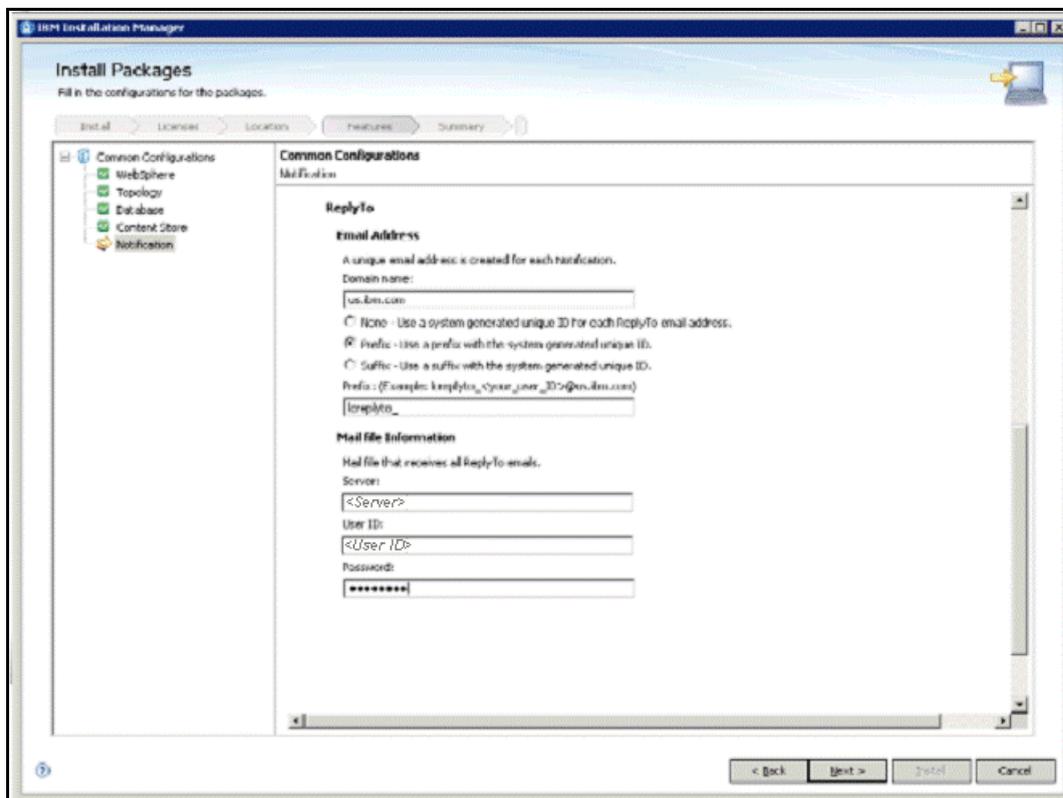


Figure 118. IBM Connections 4.0.0: Install Packages screen: Notification settings (2 of 2)

14. Review the summary information and click **Install**.

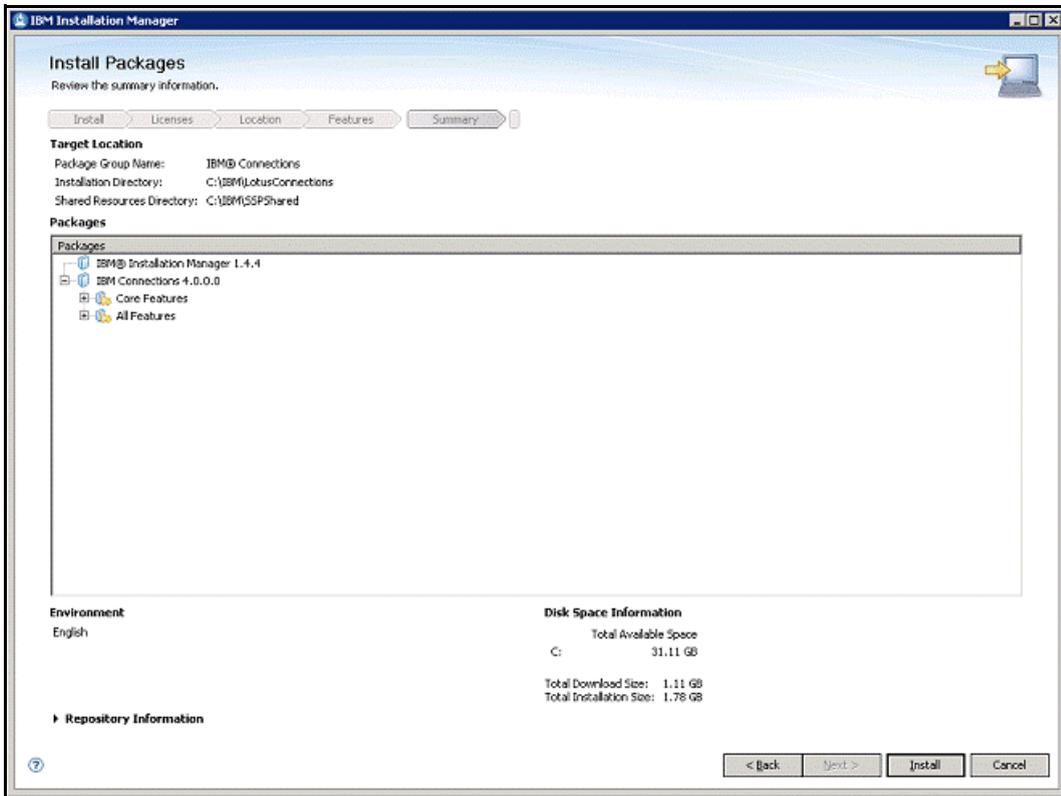


Figure 119. IBM Connections 4.0.0: Install Packages screen: Summary information

The installation starts.

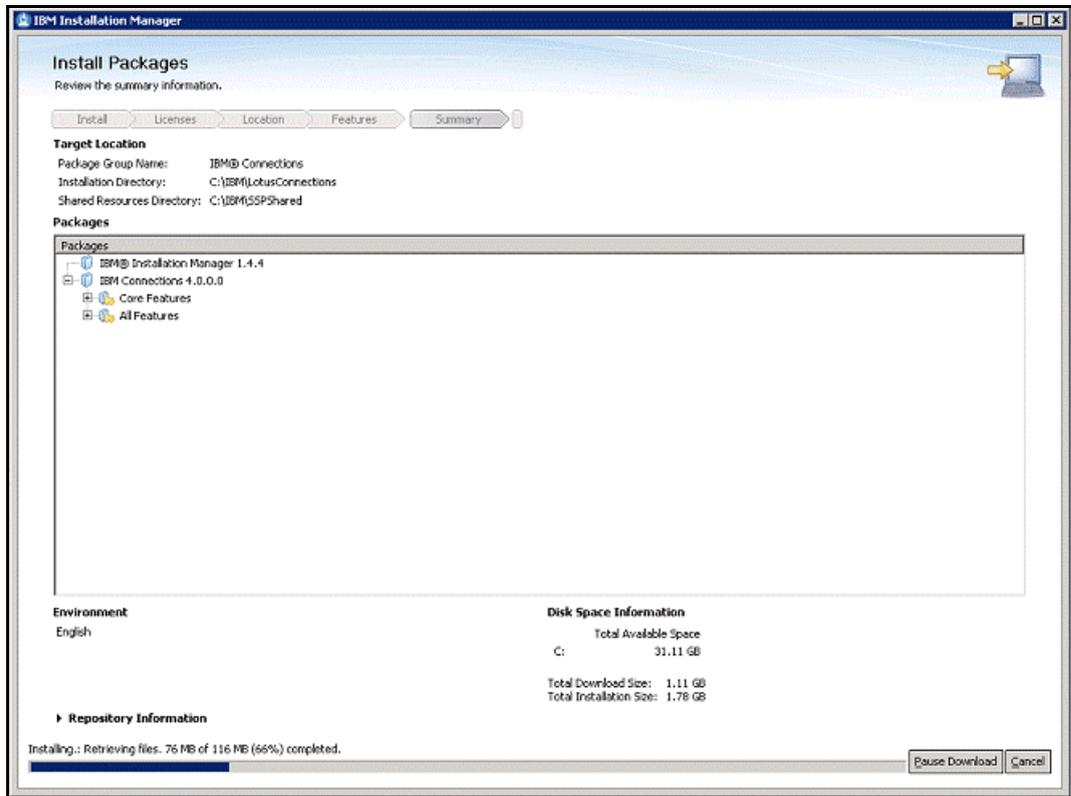


Figure 120. IBM Connections 4.0.0: Installation starts

The packages installation finishes.

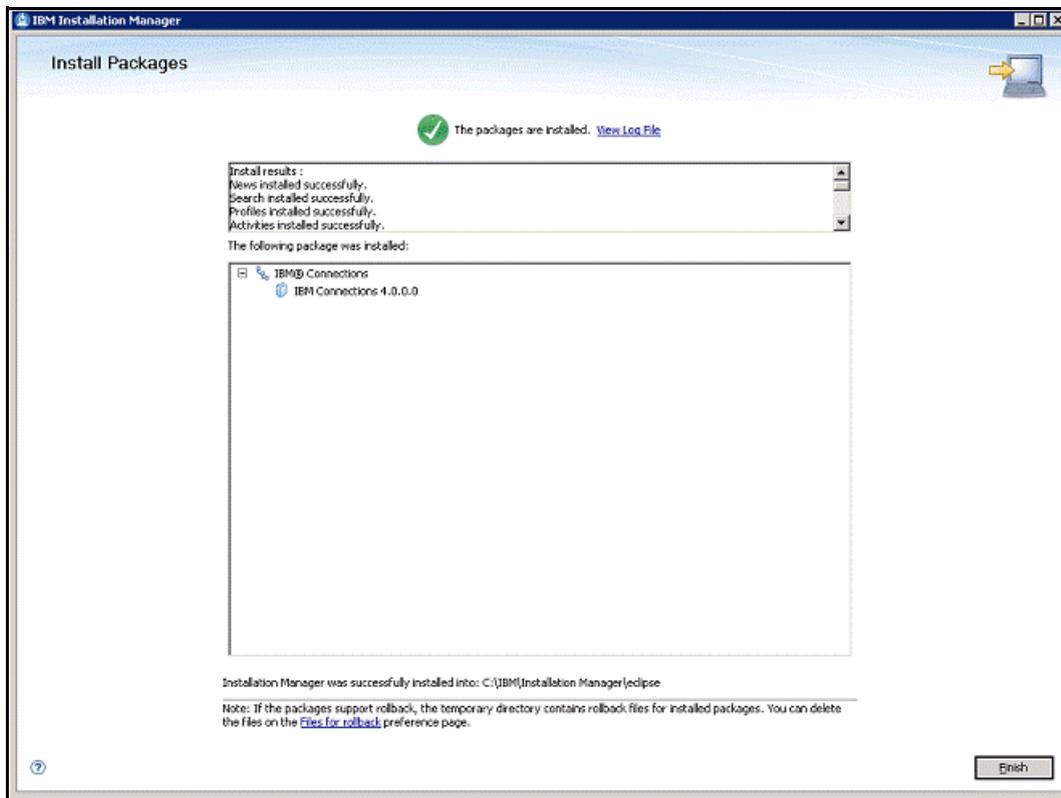


Figure 121. IBM Connections 4.0.0: Installation completion



Hint

Synchronize all Connections nodes in WebSphere Application Server console and wait some time before moving on.

3. Post-installation tasks

Configuring IBM HTTP Server with SSL

Defining IBM HTTP Server

Follow these steps to define an IBM HTTP Server:

- ___ 1. Log in to the WebSphere Application Server Integrated Solutions Console on the Deployment Manager and select **System administration > Nodes > Add Node**.

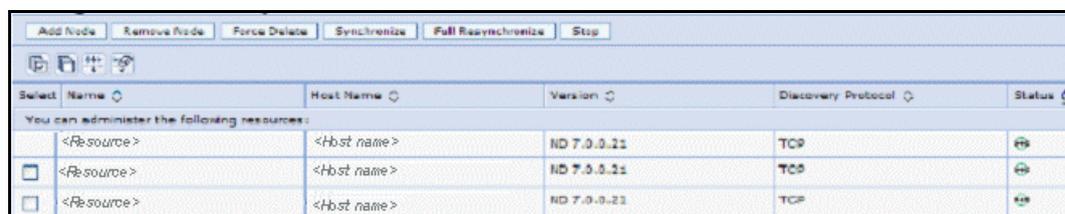


Figure 122. Deployment Manager: System administration > Nodes > Add Node

- ___ 2. Choose **Unmanaged node**.

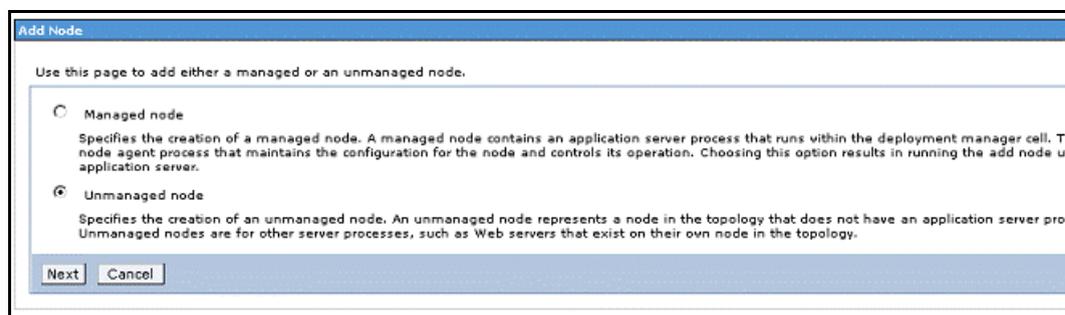


Figure 123. Add Node: Unmanaged node

___ 3. Input node name and host name.

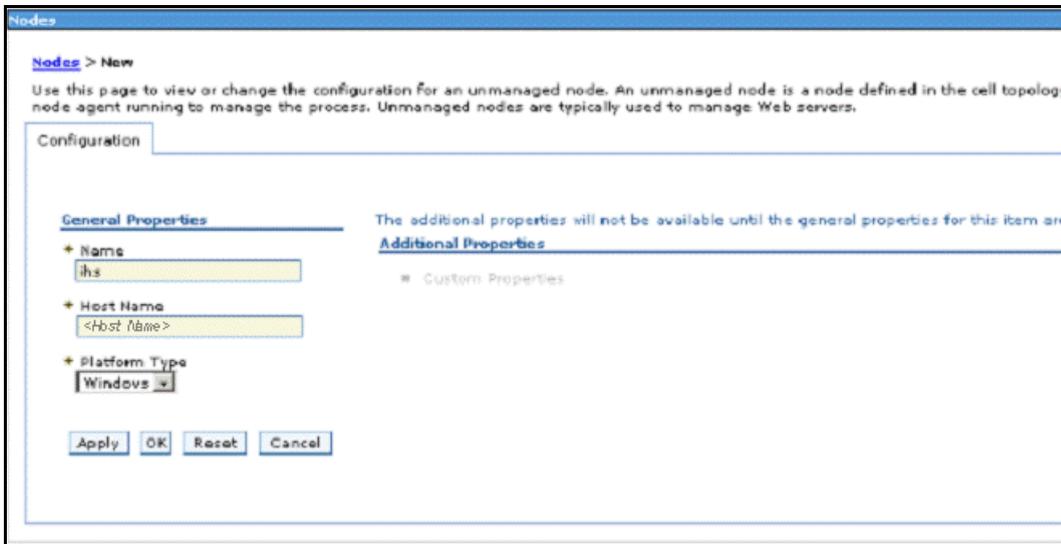


Figure 124. Nodes: Providing a node name and a host name

___ 4. Click **OK** and then **Save**.

___ 5. Select **Servers > Server Types > Web servers** and click **New**.

___ 6. Select the node that you created and input server name as **webserver1**.

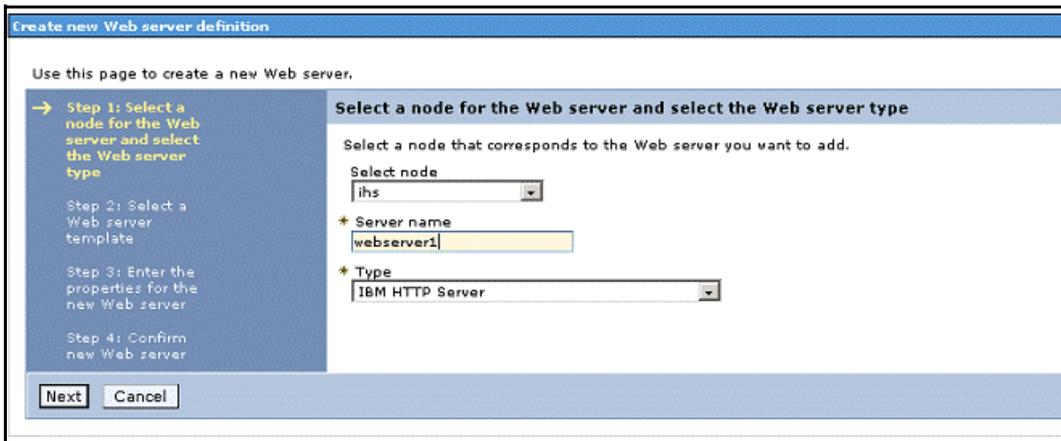


Figure 125. Create a web server definition: Server name

7. Click **Next** and then **Next** again.

Use this page to create a new Web server.

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

→ Step 2: Select a Web server template

Step 3: Enter the properties for the new Web server

Step 4: Confirm new Web server

Select a Web server template

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

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

Previous Next Cancel

Figure 126. Create a web server definition: Select a web server template

8. Modify the HTTP server installation path and input username/password for IBM HTTP Server administration.

Use this page to create a new Web server.

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

Step 2: Select a Web server template

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

Step 4: Confirm new Web server

Enter the properties for the new Web server

Enter the Web server properties.

* Port: 80

* Web server installation location: C:\IBM\HTTPServer

* Service name: IBMHTTPServer7.0

* Plug-in installation location: c:\IBM\HTTPServer\Plugins

Application mapping to the Web server: All

Enter the IBM Administration Server properties.

* Administration Server Port: 8008

* Username: ihsadmin

* Password: *****

* Confirm password: *****

Use SSL

Previous Next Cancel

Figure 127. Enter the properties for the new web server

9. Click **Next** and then **Finish**.

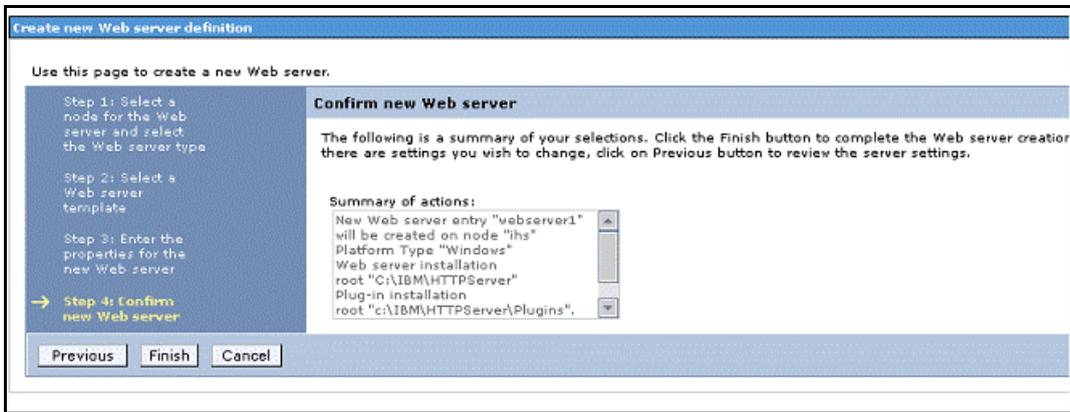


Figure 128. Confirm new web server

10. Click **Save**.

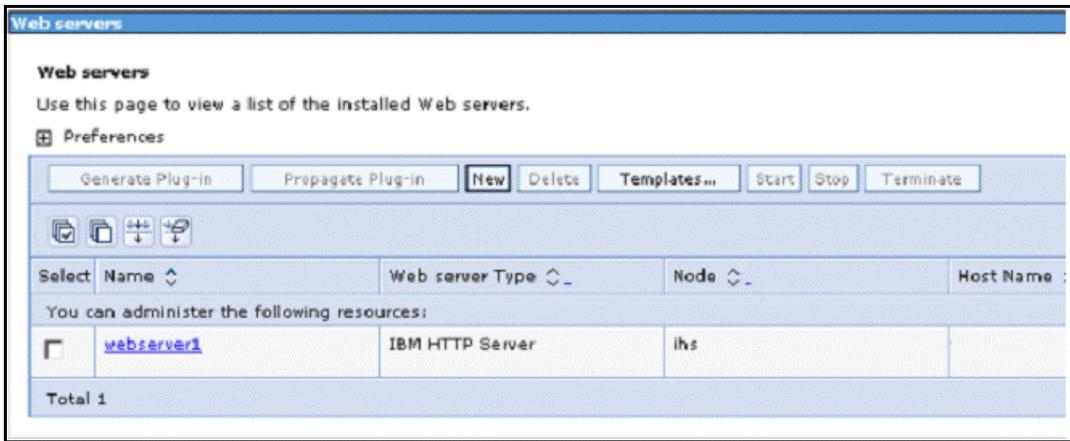


Figure 129. Web servers: List of the installed web servers

11. Start IBM HTTP Server and IBM HTTP Server administration in Windows service.



Figure 130. IBM HTTP Server and IBM HTTP Server administration in Windows service

Configuring IBM HTTP Server for SSL

Follow these steps to configure IBM HTTP Server for SSL:

- ___ 1. Start iKeyman on IBM HTTP Server computer.

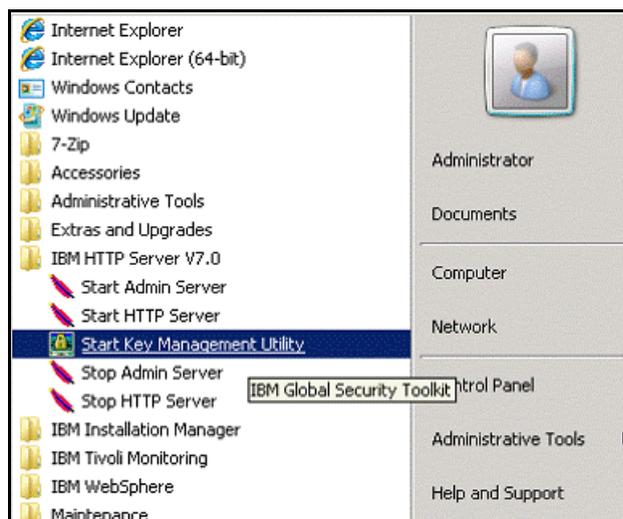


Figure 131. Key Management Utility

- ___ 2. Open `plugin-key.kdb` under `C:\IBM\HTTPServer\Plugins\config\webserver1`, which the default plug-in webserver1 uses that you defined in WebSphere Application Server console.

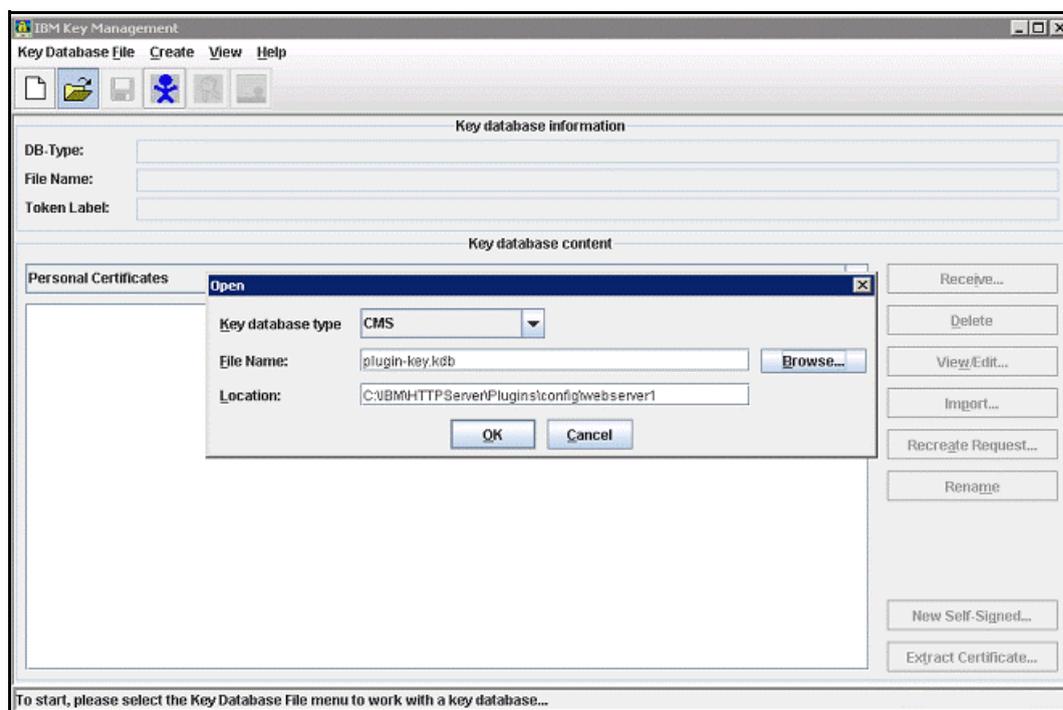


Figure 132. IBM Key Management

3. The default password is **WebAS**.

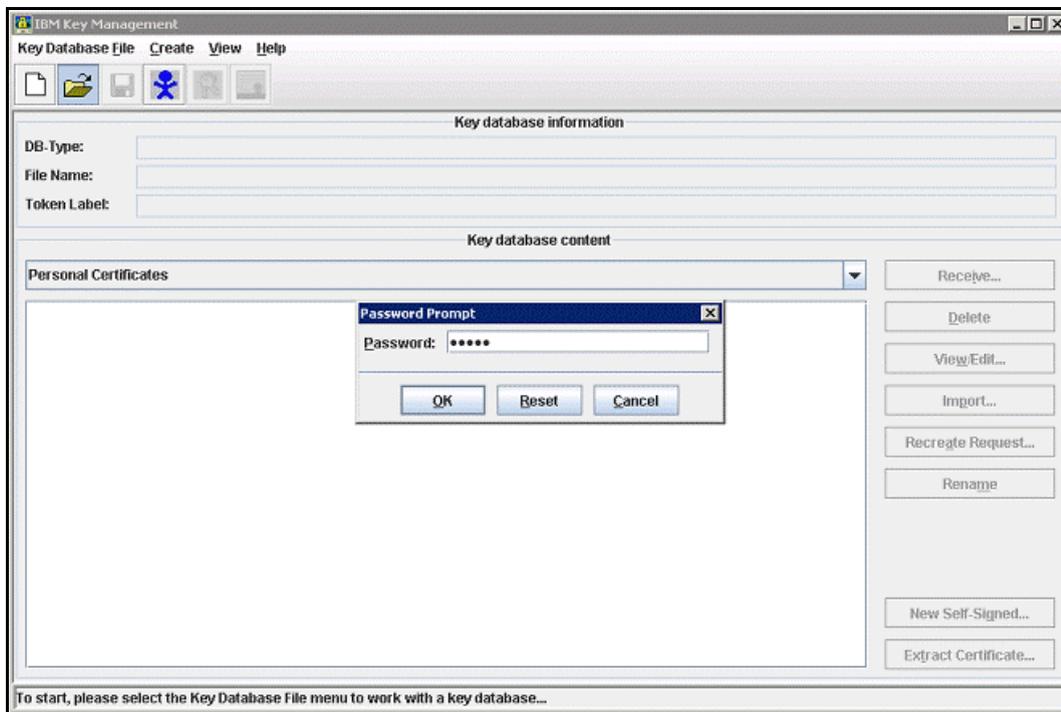


Figure 133. IBM Key Management: Password Prompt

4. Click **New Self_signed...**, input a label name and set the validity period to be as long as you want, and no longer than 9999 days.

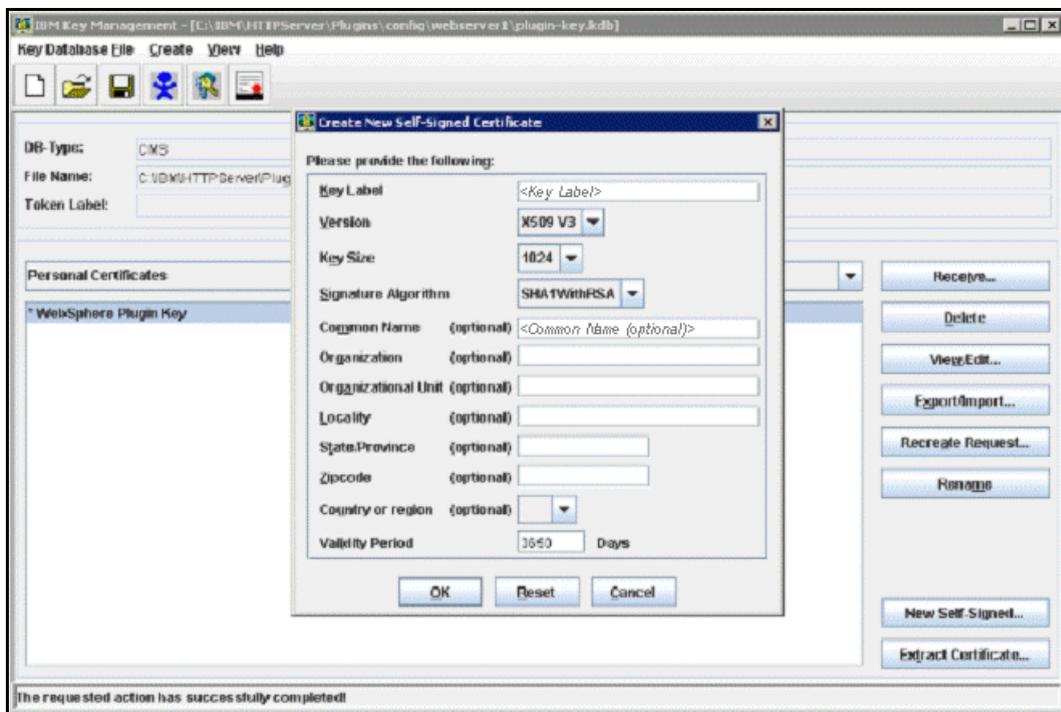


Figure 134. IBM Key Management: Create New Self-Signed Certificate

- ___ 5. Click **OK** and you can set this key to be default key.

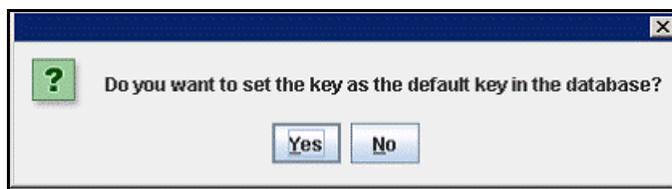


Figure 135. Setting the key as the default key in the database

- ___ 6. Close iKeyman.
- ___ 7. Find the file `httpd.conf` under `C:\IBM\HTTPServer\conf`, open with your favorite text editor. At the end of the file, add the following lines for example:

```
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName connections.example.com
#DocumentRoot C:\IBM\HTTPServer\htdocs
SSLEnable
</VirtualHost>
</IfModule>
SSLDisable
Keyfile C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb
SSLStashFile C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.sth
```

- ___ 8. Restart HTTP server in Windows service.

IBM HTTP Administration 7.0	IBM_HTTP...	Started	Manual	Local System
IBM HTTP Server 7.0	IBM_HTTP...	Started	Manual	Local System

Figure 136. Restarting HTTP server in Windows service

- 9. Verify you can access `https://<your IHS host>` and get IBM HTTP Server page successfully.

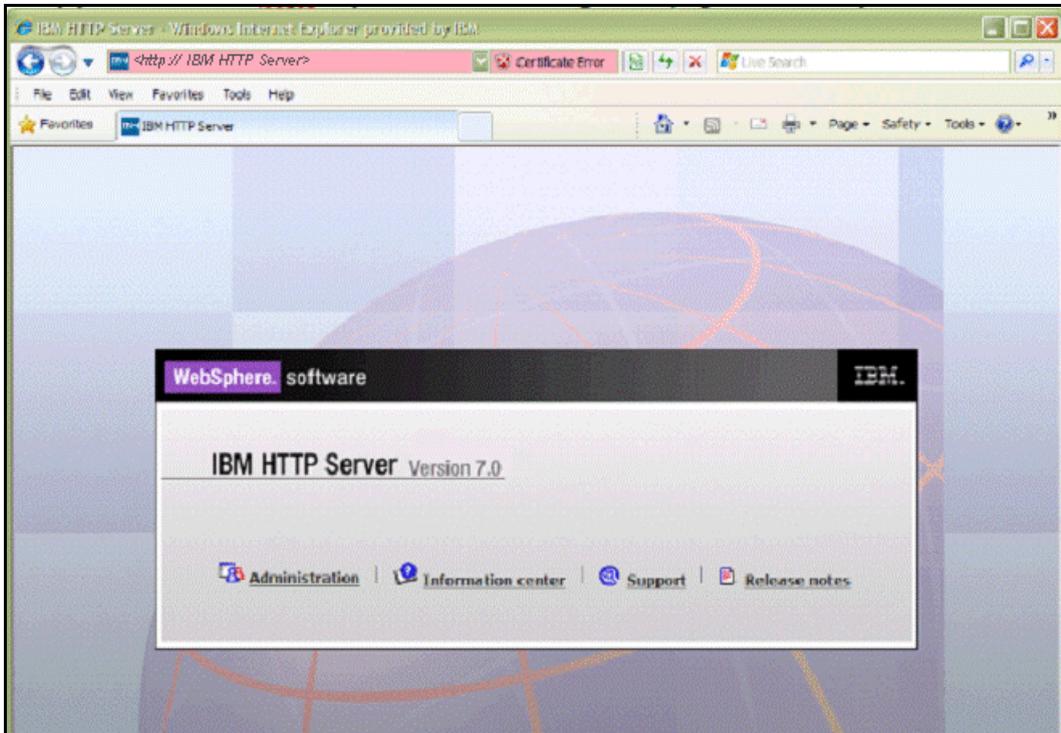


Figure 137. IBM HTTP Server Version 7.0

Adding certificates to the WebSphere truststore

Follow these steps to add certificates to the WebSphere truststore:

- 1. Go to **Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates.**

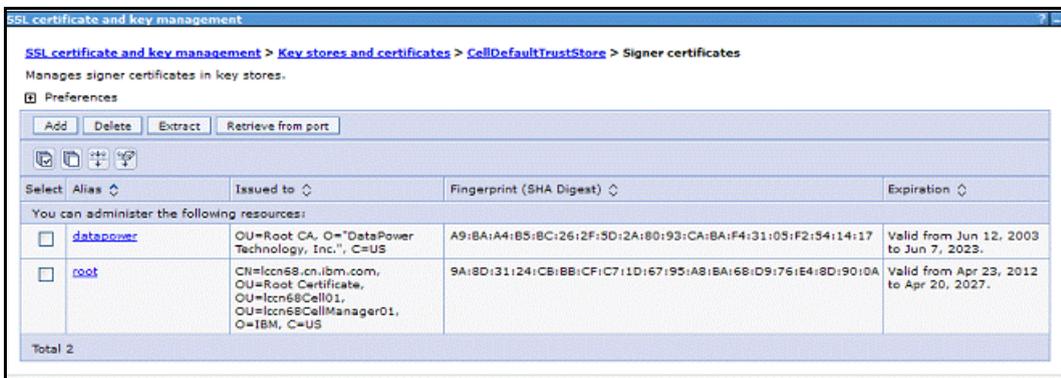


Figure 138. SSL certificate and key management

- ___ 2. Click **Retrieve signer information** from port, input host name, and port number.

Figure 139. General properties: Retrieve signer information

- ___ 3. Click **OK** and then **Save**.

Import WebSphere Application Server root certificate to HTTP server

Follow these steps to import WebSphere Application Server root certificate to HTTP server:

- ___ 1. Stay on **Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates**, check the box before root certificate and click **Extract**.

Select	Alias	Issued to	Fingerprint (SHA Digest)	Expiration
<input type="checkbox"/>	datapower	OU=Root CA, O="DataPower Technology, Inc.", C=US	A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17	Valid from Jun 12, 2003 to Jun 7, 2023.
<input type="checkbox"/>	https	CN=lccn68.cn.ibm.com	FC:21:E6:F1:BA:75:76:A5:31:A4:9E:3F:E5:8E:62:B8:1A:06:BC:E6	Valid from Apr 23, 2012 to Apr 23, 2022.
<input checked="" type="checkbox"/>	root	CN=lccn68.cn.ibm.com, OU=Root Certificate, OU=lccn68Cell01, OU=lccn68CellManager01, O=IBM, C=US	9A:8D:31:24:CB:BB:CF:C7:1D:67:95:A8:BA:68:D9:76:E4:8D:90:0A	Valid from Apr 23, 2012 to Apr 20, 2027.

Figure 140. SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates

2. Save to disk as a certificate file.



Figure 141. Saving the certificate file

3. Start iKeyman and open C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb again. Select the signer certificates tab.

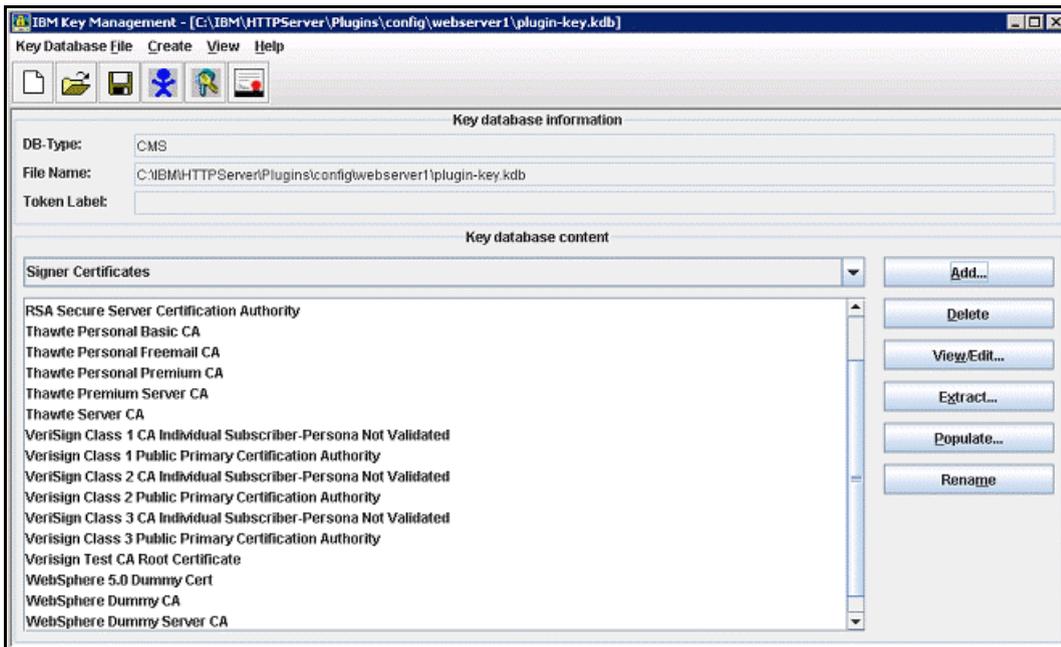


Figure 142. IBM Key Management

4. Click **Add** and browser to the certificate file you just extracted.

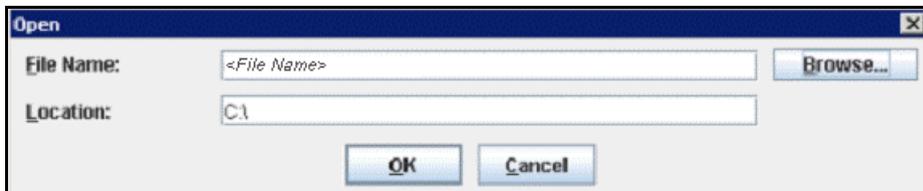


Figure 143. Browsing to the certificate extracted

- ___ 5. Input a label name and click **OK**.



Figure 144. Entering a label

- ___ 6. Exit iKeyman.

Updating web addresses in IBM HTTP Server

Follow these steps to update web addresses in IBM HTTP Server:

- ___ 1. Open `LotusConnections-config.xml` under
`c:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\ConnectionsCell01\LotusConnections-config` with your favorite text editor.
- ___ 2. Find each URL with a postfixed port number, and replace such URL with any port, for example:

```
<sloc:serviceReference acf_config_file="acf-config-nf.xml" bootstrapHost=""
bootstrapPort="" clusterName="LCcluster" enabled="true"
person_card_service_name_js_eval="generalrs.label_personcard_activitieslink"
person_card_service_url_pattern="/service/html/mainpage#dashboard%2Cmyactivities%2C
userid%3D{userid}%2Cname%3D{displayName}" serviceName="activities"
ssl_enabled="true">
    <sloc:href>
        <sloc:hrefPathPrefix>/activities</sloc:hrefPathPrefix>
        <sloc:static href="http://connections.example.com"
ssl_href="https://connections.example.com"/>
        <sloc:interService href="https://connections.example.com"/>
    </sloc:href>
</sloc:serviceReference>
```



Important

After the modification, make sure you cannot find any URL with port number for any Connections application in the `LotusConnections-config.xml` file. The exception is for other third-party URLs which is covered later.

Creating initial server index

From Connections 4.0, the administrator does not need to perform more actions to create initial server index. After you make sure that the search directory in the shared folder is equally accessible to each server, and you have enough space in local folder, the search index building

task kicks off automatically each 15 minutes. The initial index is completed on one node and is copied automatically to any other node to finish the whole initial index building task.

To verify initial index, go to each local folder and find `INDEX.READY` file under `c:\IBM\LCLocal\search\index`.

Configuring ReplyTo feature

Configure Forums so that users can reply to forum topics by email.

When a reply is added to a forum topic, an email is sent to followers of that forum and that topic. After you enable and configure notification replies, users who receive that email can respond by email. The content of that response is added as a new reply in the forum after the original.

When users reply to notifications, a mail server uses a rule or trigger to direct the reply emails to a mailbox dedicated for this purpose. The IBM® Connections server uses a WebSphere® Application Server mail session to process this mailbox periodically, adding content to the forums.

For it to work, an administrator must configure the mail server and mail session, and then enable the feature. Users must specify their email settings in IBM Connections. For a user to receive notifications that they can reply to, the Notifications feature must be enabled on the server. The email notification reply feature must also be enabled on the server in the `news-config.xml` file. Each user who wants to receive email reply notifications must then have the feature enabled on their Settings screen.

Configuring the mail session requires some simple steps in the WebSphere Application Server administrative console. Configuring the mail server requires creating the dedicated mailbox, and creating a rule or trigger to direct replies to it. Steps for creating the rule or trigger vary depending on the mail server. For example, in Microsoft Exchange you create a transport rule; in Domino® you create a trigger.

IBM Connections supports the Simple Mail Transfer Protocol (SMTP) for sending notifications, and the Internet message access protocol (IMAP) and secure Internet message access protocol (IMAPS) for notification replies. Any mail server that uses these protocols can direct notifications and notification replies.



Note

In deployments with multiple IBM Connections servers, the different servers cannot use the same mailbox. However, they can use different mailboxes on the same mail server, in which case each would require its own direction rules.

Create a ReplyTo user on Domino mail server

Follow these steps to create a ReplyTo user on Domino mail server:

- ___ 1. Open Domino admin and connect to Domino mail server you plan to use.
- ___ 2. On People & Group view, click the **People** tab on the right panel.
- ___ 3. Click **Register**, input the certifier's password for Domino server.

4. Check the **Advanced** box and input information as in the following image:

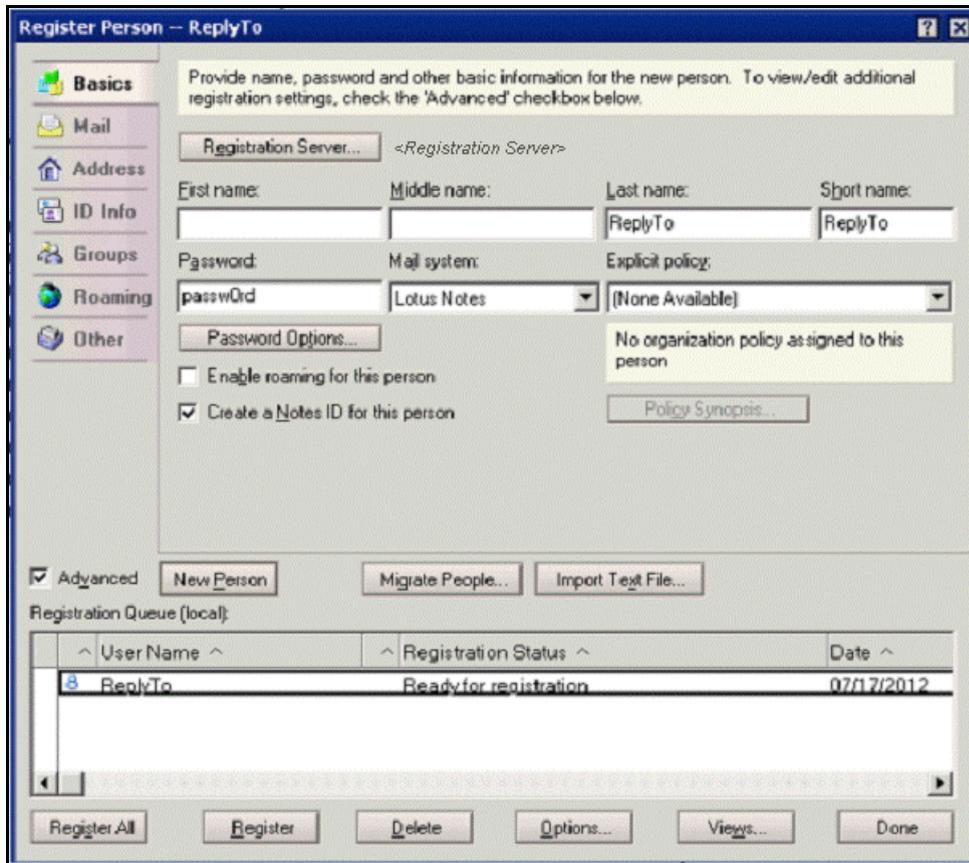


Figure 145. Register Person: ReplyTo

- ___ 5. The mail domain value might be set to the real domain you use:

Register Person -- ReplyTo

Mail Internet Address Information

Internet address: ReplyTo@us.ibm.com Internet Domain: us.ibm.com

Address name format: FirstName LastName Separator: None

Supply internet address format settings for the selected people or person. The Internet address is created using the person's name, the internet domain and internet address format components. It must be unique in the address book.

Advanced New Person Migrate People... Import Text File...

Registration Queue (local):

	^ User Name ^	^ Registration Status ^	Date ^
8	ReplyTo	Ready for registration	07/17/2012

Register All Register Delete Options... Views... Done

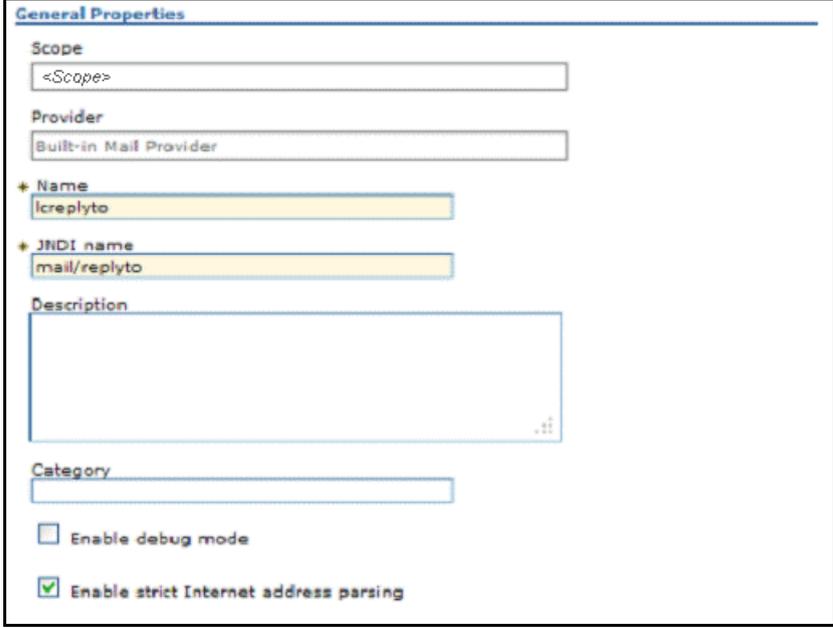
Figure 146. Register Person: ReplyTo: Setting the real domain

- ___ 6. Click **Register** to complete the registration.

Configuring WebSphere Application Server for email notification replies

Follow these steps to configure WebSphere Application Server for email notification replies:

1. Open WebSphere Application Server console and go to **Resources > Mail > Mail Sessions**.
2. If you enabled mail-in during Connections installation, you see a mail session that is named as `lcreplyto`. If not, select the cell scope and create a mail session as in the following figure:

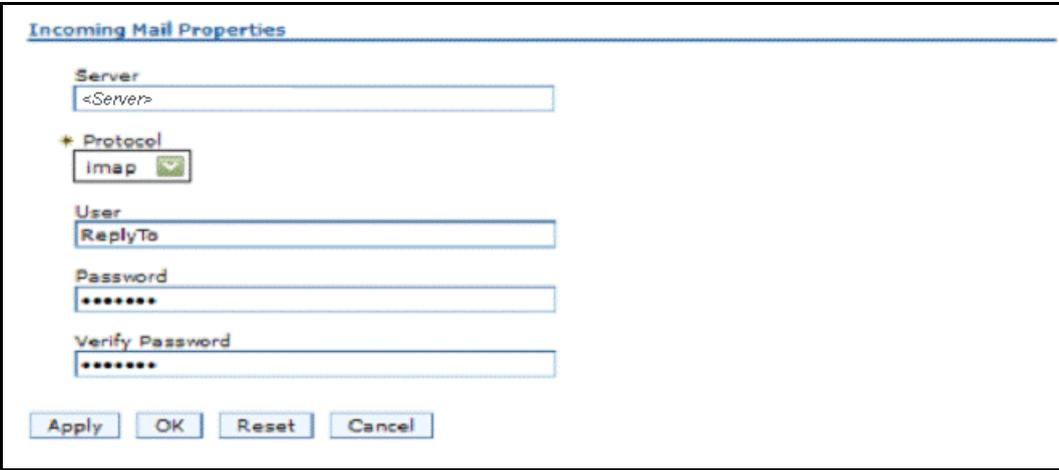


The screenshot shows the 'General Properties' dialog box for creating a mail session. The fields are as follows:

- Scope: `<Scope>`
- Provider: Built-in Mail Provider
- Name: `lcreplyto`
- JNDI name: `mail/replyto`
- Description: (Empty text area)
- Category: (Empty text field)
- Enable debug mode:
- Enable strict Internet address parsing:

Figure 147. Creating a mail session (1 of 2)

3. Click **OK** and **Save**.



The screenshot shows the 'Incoming Mail Properties' dialog box for creating a mail session. The fields are as follows:

- Server: `<Server>`
- Protocol: `imap` (with a dropdown arrow)
- User: `ReplyTo`
- Password: `*****`
- Verify Password: `*****`

Buttons at the bottom: Apply, OK, Reset, Cancel

Figure 148. Creating a mail session (2 of 2)

Configuring Domino for email notification replies

Follow these steps to configure Domino for email notification replies:

- ___ 1. Open Domino Admin and click the **Configuration** tab.
- ___ 2. Expand Messaging in the navigator, and then click **Configuration**.

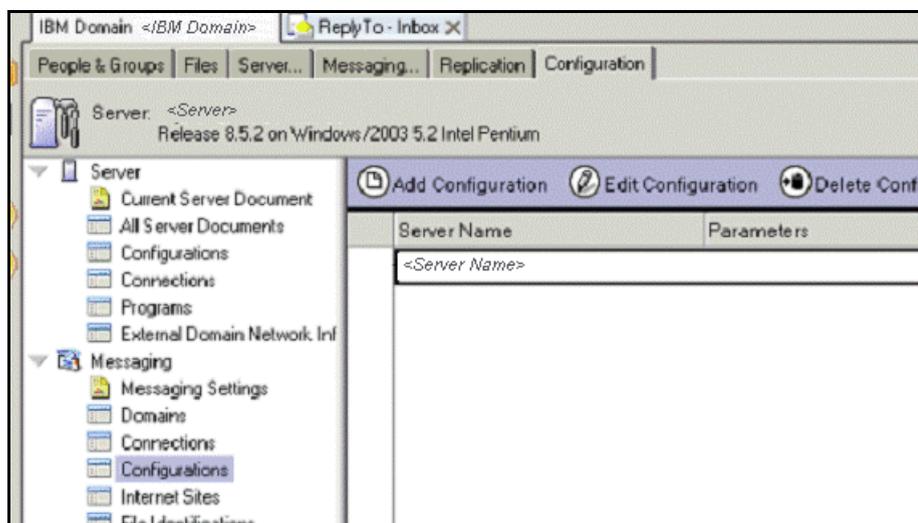


Figure 149. Domino Admin

- ___ 3. Select the messaging server and click Edit Configuration.
- ___ 4. Click the **Router/SMTP** tab. Then, click the Restrictions and Controls tab, and then click the Rules tab.



Figure 150. Router/SMTP tab

- ___ 5. Click **New Rule** and create a rule that moves emails that contain lcreplyto_ in the **To** field to the mailbox, for example:

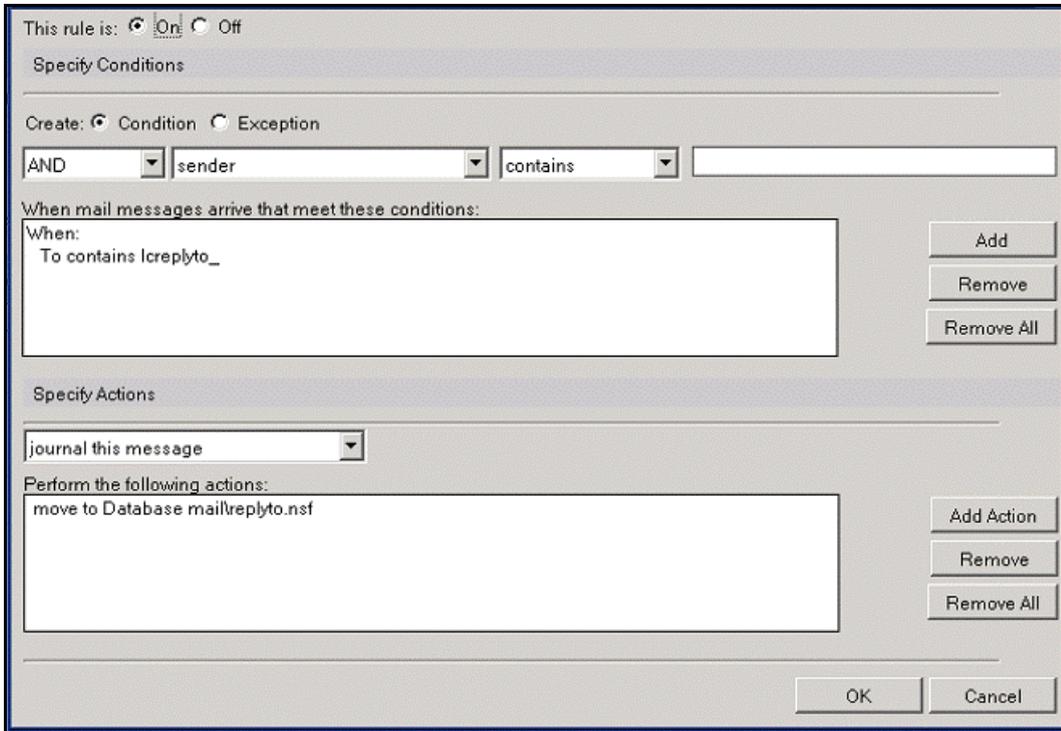


Figure 151. Creating a rule

- ___ 6. Go back to **People & Groups** tab, expand **PeoplebyOrganization**.
- ___ 7. Edit the account of the user that is used to direct reply mail.

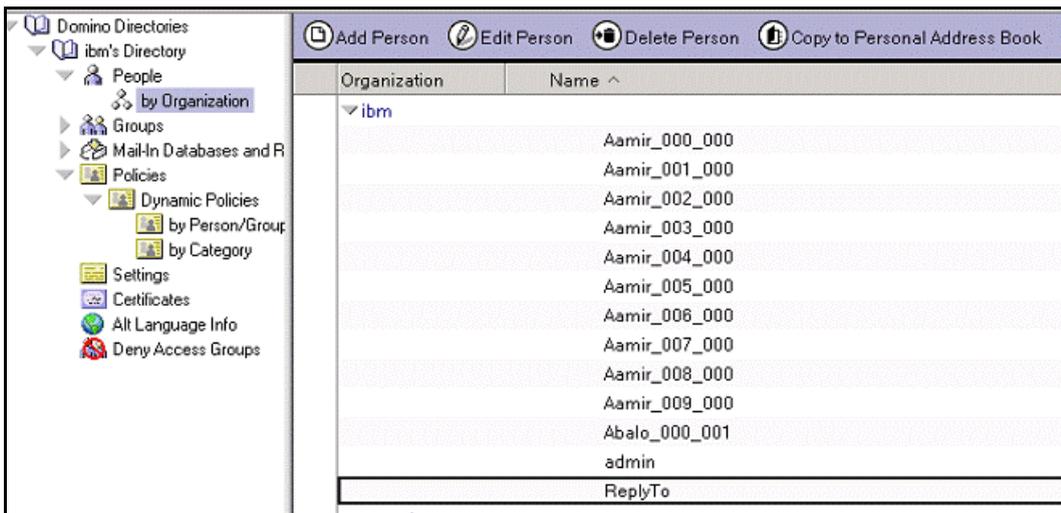


Figure 152. Editing user's account

- ___ 8. Click **Open Mail File**.

___ 9. Select the **View > Agents** menu item.

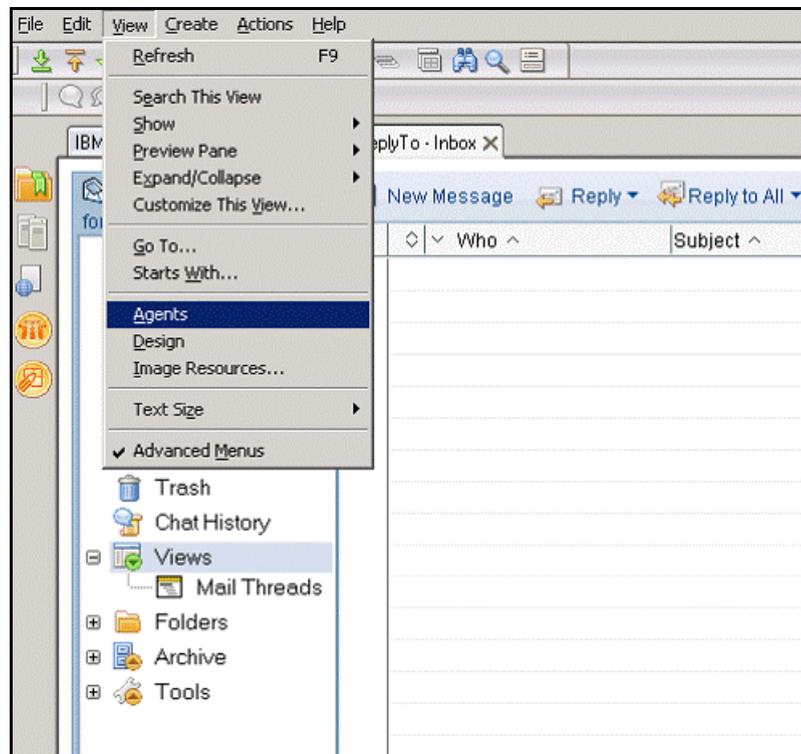


Figure 153. Selecting Agents

___ 10. Click **New Agent**.

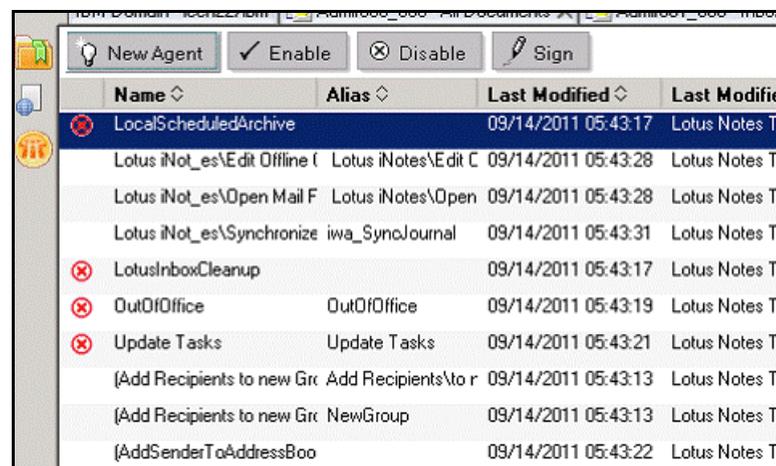


Figure 154. New Agent

___ 11. Add the following LotusScript to the agent:

```
Sub Initialize
  Dim session As New NotesSession
  Dim db As NotesDatabase
  Dim view As NotesView
  Dim doc As NotesDocument
```

```

Set db = session.CurrentDatabase
  Set view = db.getView("$Sent")
Set doc = view.GetFirstDocument()
  While Not(doc Is Nothing)
    Call doc.PutInFolder("$inbox")
    Set doc = view.GetNextDocument(doc)
  Wend
End Sub

```

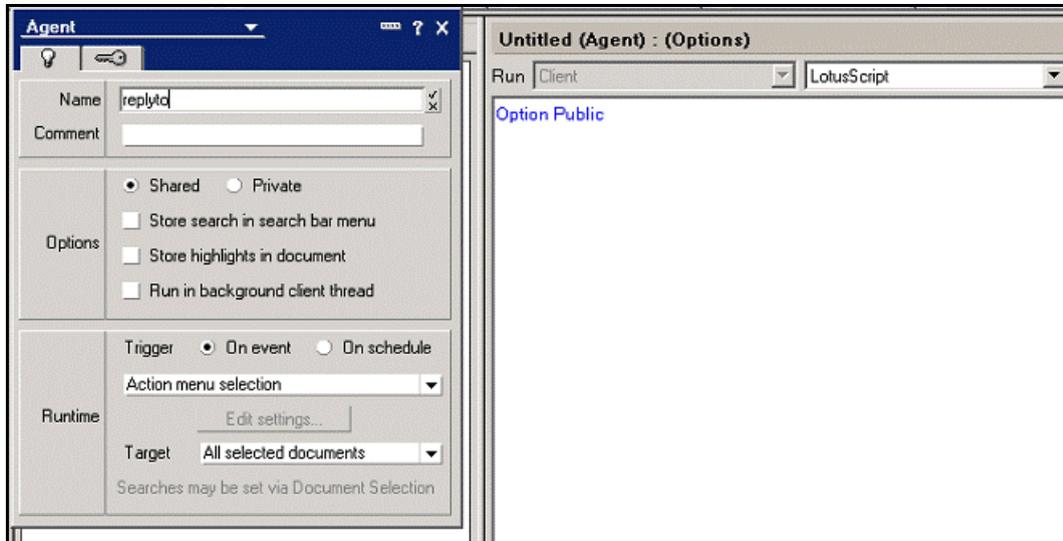


Figure 155. Adding LotusScript to the agent (1 of 2)

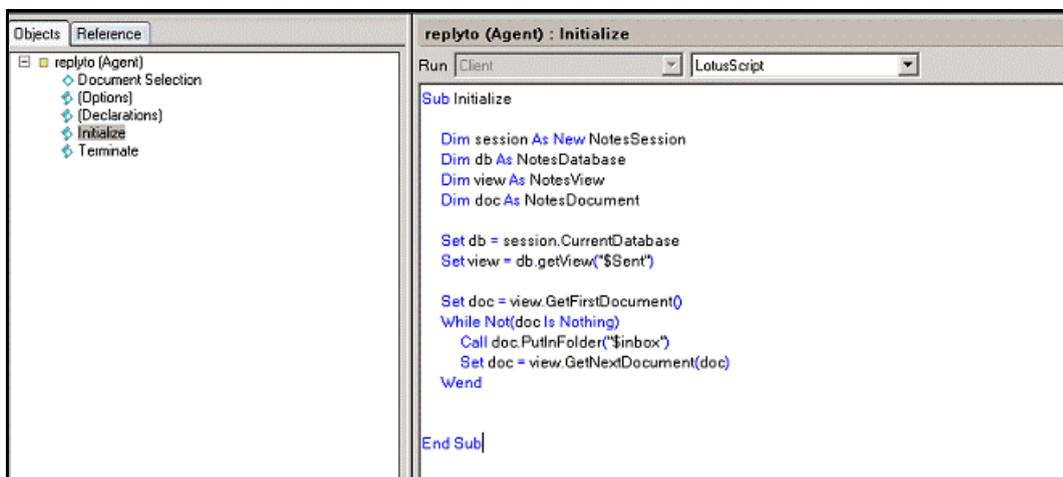


Figure 156. Adding LotusScript to the agent (2 of 2)

___ 12. Save your changes.



Figure 157. Save changes

___ 13. Open the agent again to set properties:

___ 14. In the Options section, select **Shared**.

___ 15. In the Runtime section, select **On schedule**, and then select **More than once a day**.

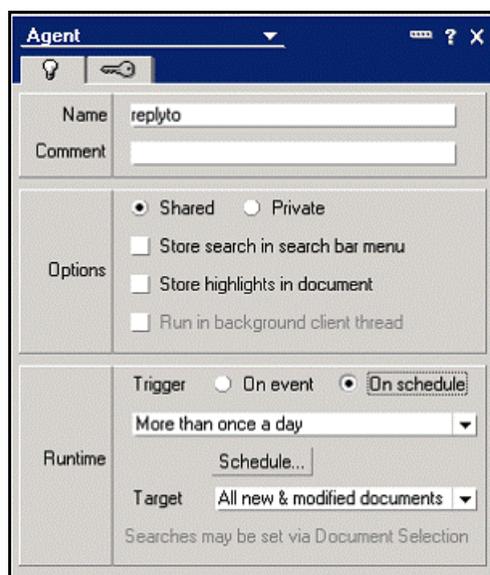


Figure 158. Selecting run time

___ 16. In the Target field, select **All new & modified documents**.

___ 17. Set a schedule, for example have it run every 5 minutes, all day.

___ 18. If you encounter the warning below, ensure that you have adequate permissions to run the agent:



Figure 159. IBM Domino Administrator warning message

- ___ 19. To fix it, open the server configuration from **Configuration > Server > All server documents** and edit it.

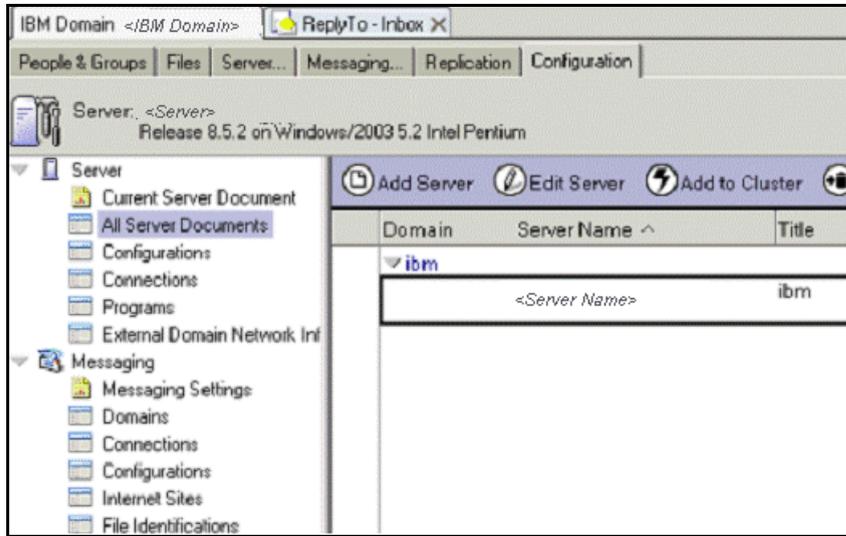


Figure 160. Editing All server documents

- ___ 20. On the Security tab, add administrator authorization for admin and domino/ibm as shown in the following figure:

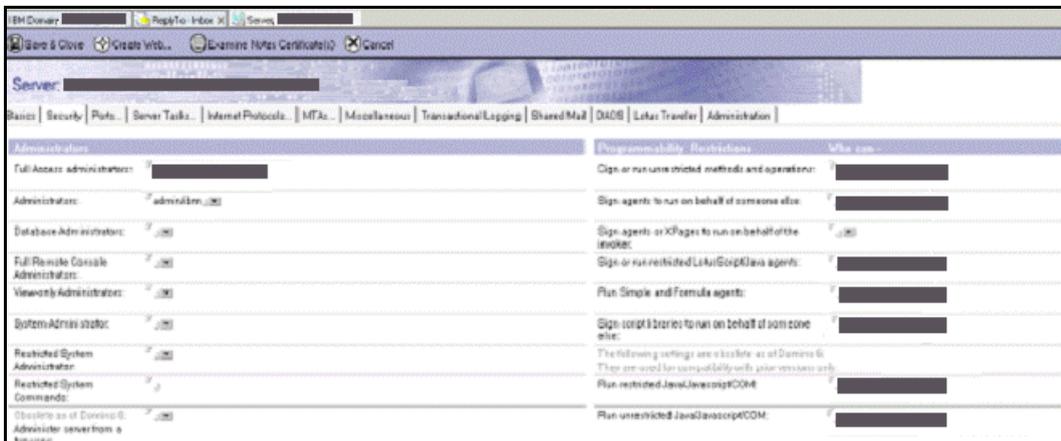


Figure 161. Adding administrator authorization for admin and domino/ibm

- ___ 21. **Save and Close.**

Enabling notification replies

Follow these steps to enable notification replies:

- ___ 1. Open news-config.xml under
 c:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\ConnectionsCell01\LotusConnections-config with you favorite text editor.

__ 2. Set mail-in section as follows:

```
<mailin enabled="true">
  <replyto enabled="true">

    <!-- A special ReplyTo address is added to notifications where
         the user can reply to the notification to respond/comment.
         The domain may be a dedicated domain for connections bound
         mails. Or it could be existing domain, in which case a prefix
         of suffix should be provided also. -->
    <replytoAddressFormat>
      <domain>us.ibm.com</domain>
      <!-- A prefix OR suffix (not both) may also be provided.
           This is necessary if an existing domain (with other
           email addresses) is being used.
           There is a 28 character limit for the affix. -->
      <!--
      <affix type="suffix">_lcreplyto</affix>
      <affix type="prefix">lcreplyto_</affix>
      -->
      <affix type="prefix">lcreplyto_</affix>
    </replytoAddressFormat>
  </replyto>
</mailin>
```

__ 3. Save it.

__ 4. Sync to nodes and restart servers.



Note

After you finish all post-installation steps, you can use Connections 4.0 freely with HTTPS enabled.

4. Configuring Tivoli Access Manager security for Connections with Domino SSO



Visit this webpage to get further information about how to configure Tivoli Access Manager security for Connections with Domino SSO:

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_single_signon_for_Tivoli_Access_Manager_ic40&content=pdcontent

Installing Tivoli Access Manager 6.1.1

First, decide the Tivoli Access Manager server installation topology; for example, install WebSEAL server and policy server in the same computer or in different computers. In this case, Tivoli Access Manager policy server and WebSEAL server are both installed in the same computer where the LDAP server is located.

Installing IBM Global Security Kit (GSKit)

Follow these steps to install IBM Global Security Kit (GSKit):

1. Run SETUP.EXE under C:\software\TAM6.1.1\CZG8MML\windows\GSKit as follows:

```
C:\software\TAM6.1.1\CZG8MML\windows\GSKit>SETUP.EXE SETUP_ISS_
```

Figure 162. Setup command

___ 2. The installation wizard opens.

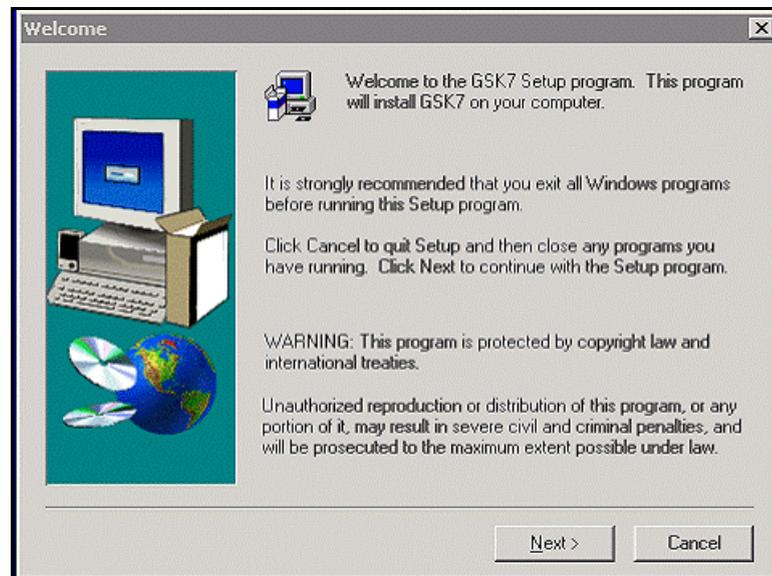


Figure 163. GSK7 Setup program: Welcome screen

___ 3. Choose the destination location for the installation.



Figure 164. GSK7 Setup program: Choose Destination Location screen

___ 4. Click **Finish** when GSK7 is installed.

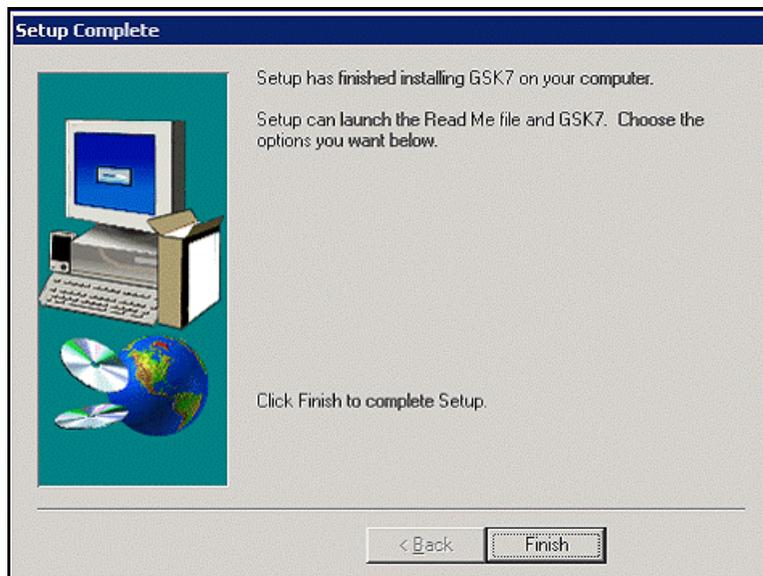


Figure 165. GSK7 Setup program: Setup complete screen

Installing IBM Tivoli Directory Server client (as needed)

Follow these steps to install IBM Tivoli Directory Server client:

- ___ 1. Run the `install_tds.exe` file under
C:\software\TAM6.1.1\CZG8LML\windows\tds_client64.
- ___ 2. Select the language for the wizard.



Figure 166. Selecting the wizard language

- ___ 3. On the wizard Welcome screen, click **Next**.



Figure 167. IBM Tivoli Directory Server 6.1: Welcome screen

4. Accept the license agreement and click **Next**.

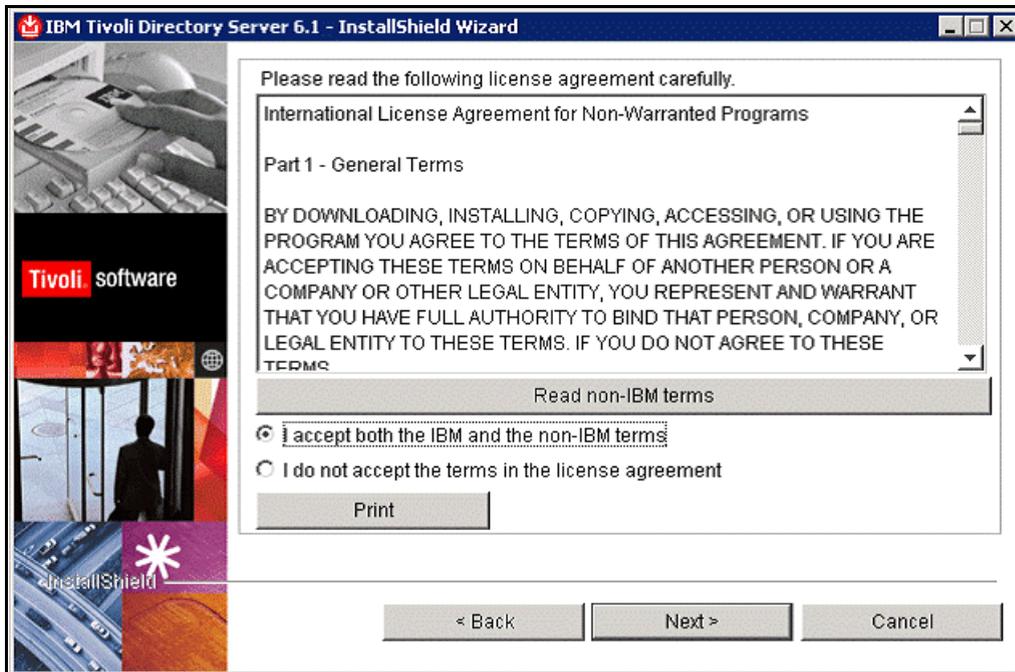


Figure 168. IBM Tivoli Directory Server 6.1: License agreement screen

5. Select the location where you want to install IBM Tivoli Directory Server 6.1.

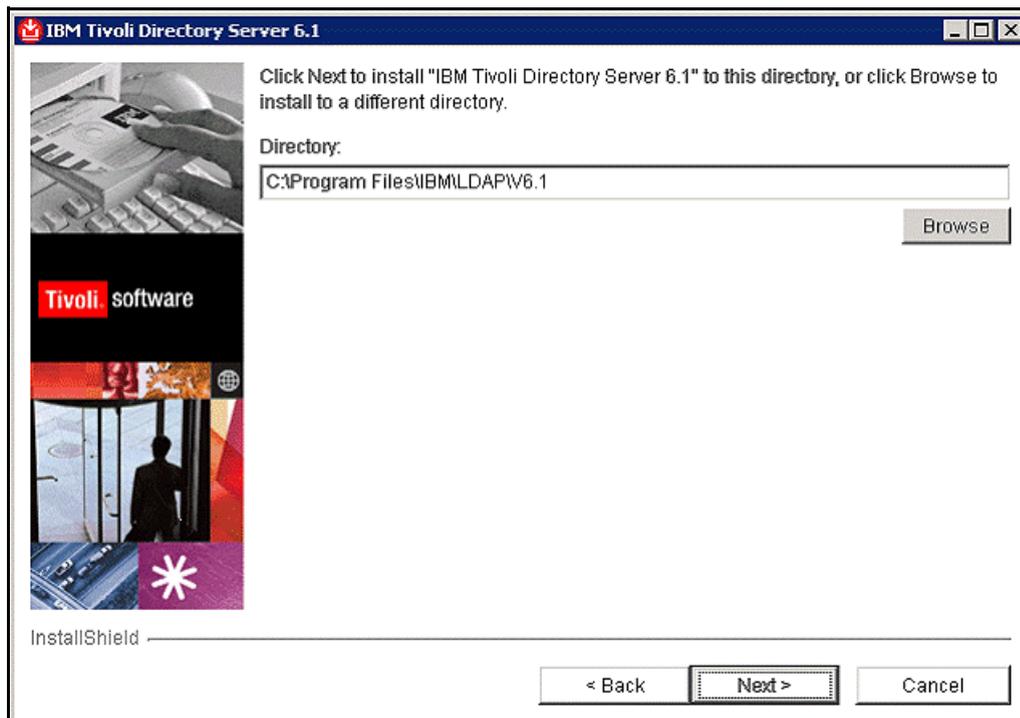


Figure 169. IBM Tivoli Directory Server 6.1: Installation location screen

- ___ 6. Select the features to install and click **Next**.

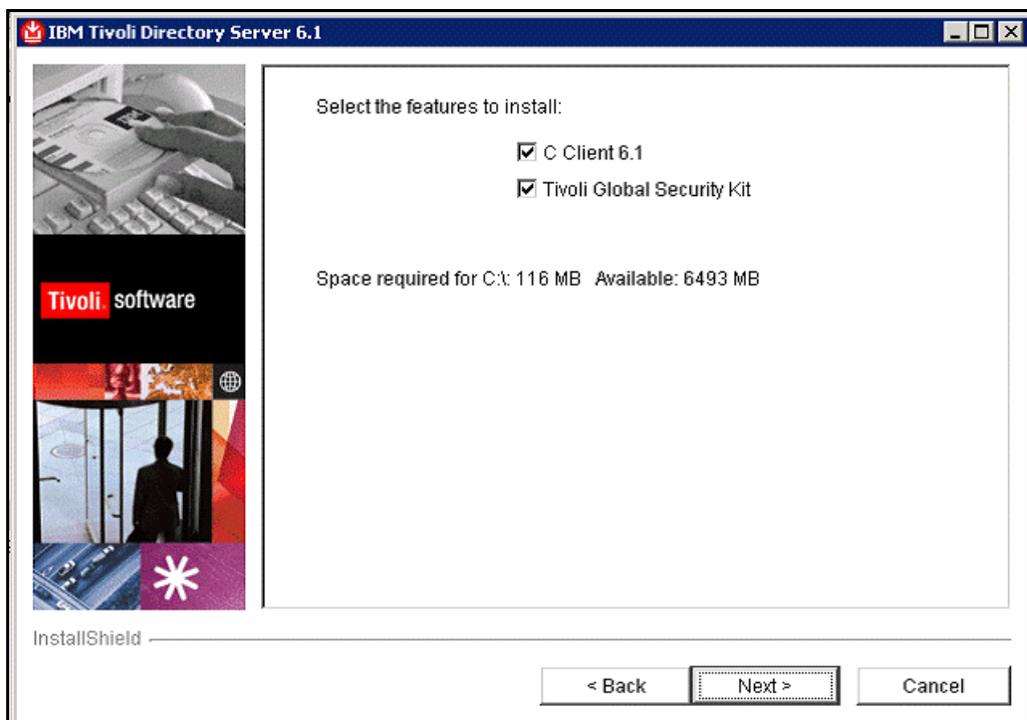


Figure 170. IBM Tivoli Directory Server 6.1: Features to install screen

- ___ 7. Review the installation settings and click **Install**.

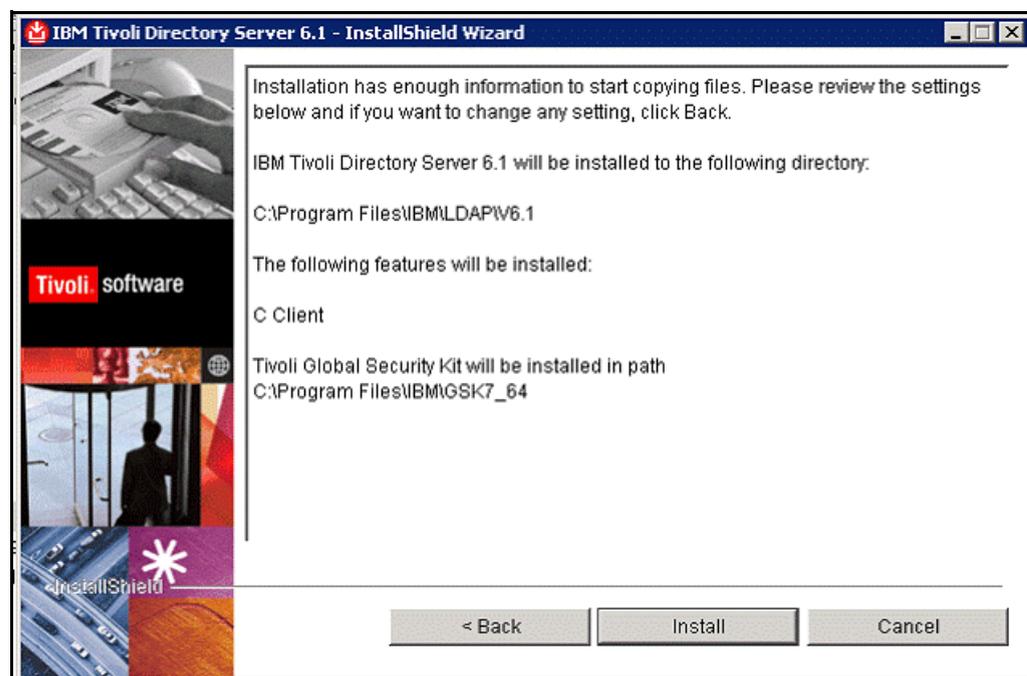


Figure 171. IBM Tivoli Directory Server 6.1: Installation settings summary screen

___ 8. When the installation completes, click **Finish**.

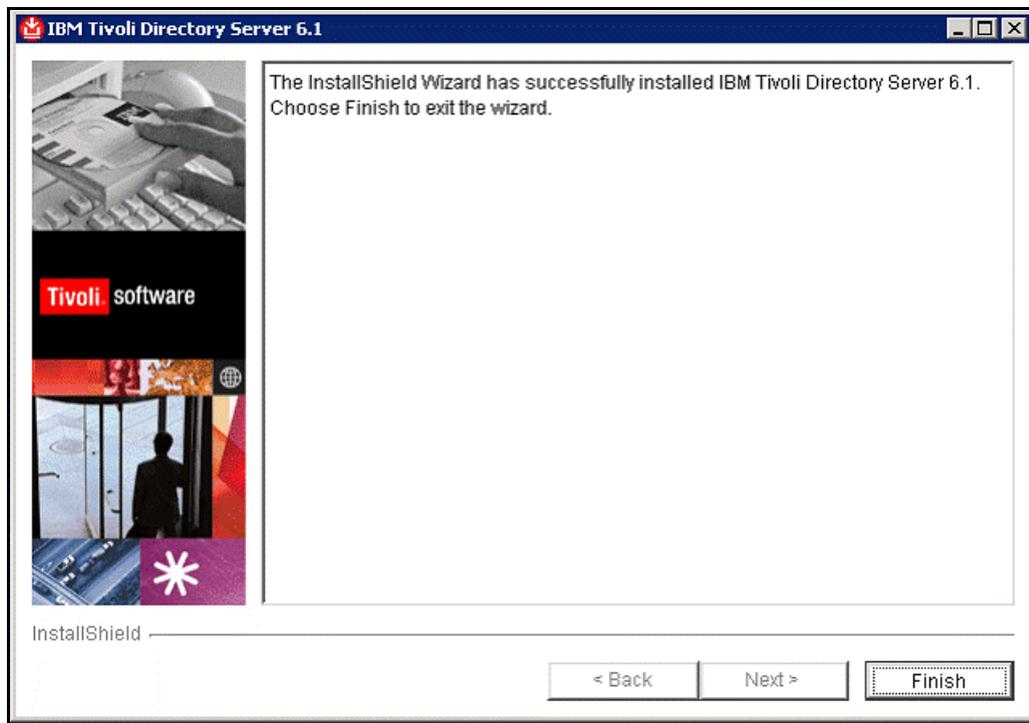


Figure 172. IBM Tivoli Directory Server 6.1: Installation completion screen

Installing Tivoli Security Utilities

Follow these steps to install Tivoli Security Utilities:

1. Run the `setup.exe` file under `C:\software\TAM6.1.1\CZG8LML\windows\TivSecUt1\Disk Images\Disk1`.
2. Choose the language for the installation wizard.

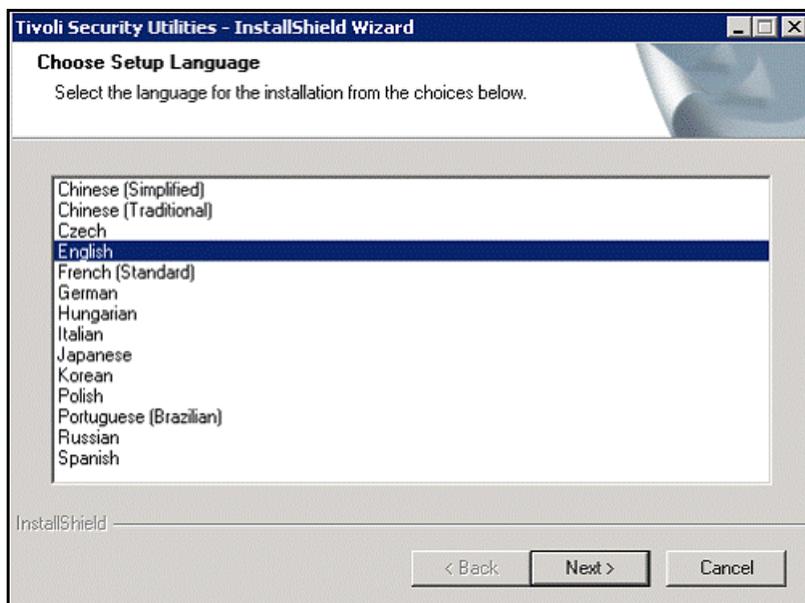


Figure 173. Choosing the language for the installation wizard

3. On the wizard welcome page, click **Next**.

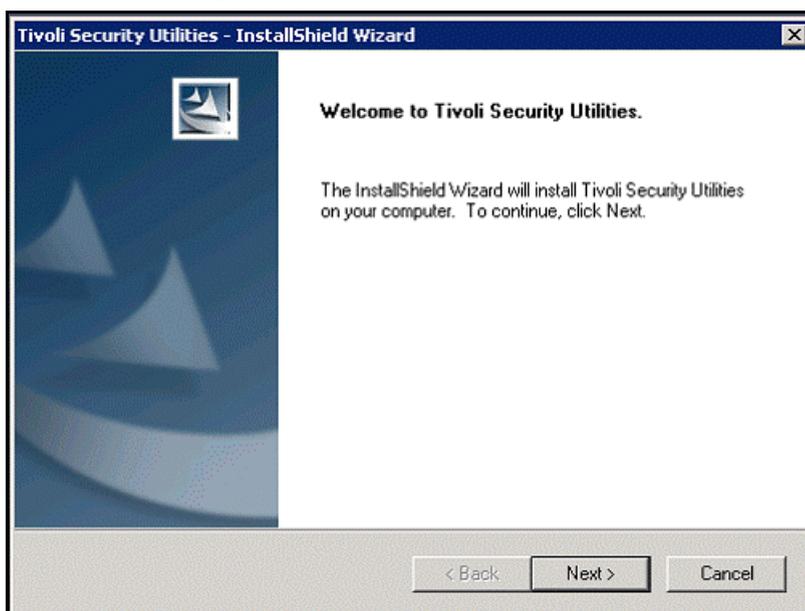


Figure 174. Tivoli Security Utilities installation wizard: Welcome screen

4. Read the license agreement and click **Yes**.

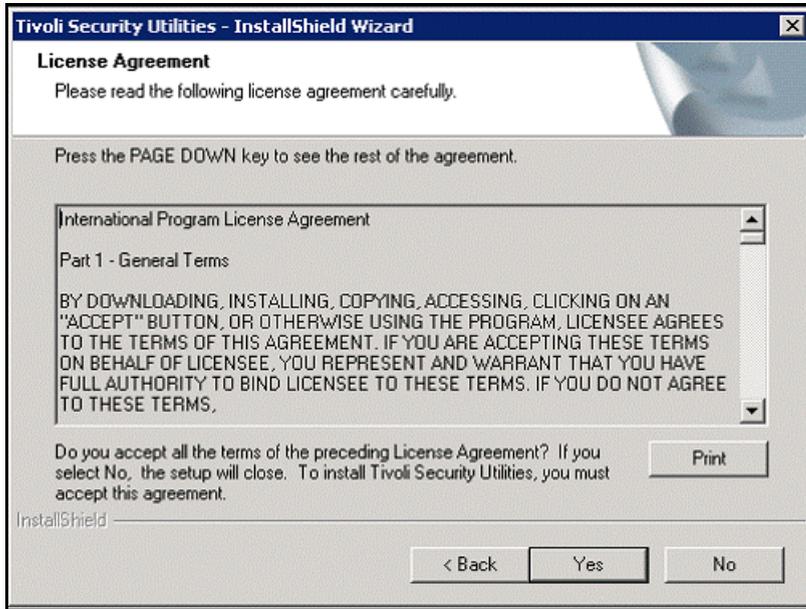


Figure 175. Tivoli Security Utilities installation wizard: License agreement screen

5. Choose the destination location and click **Next**.

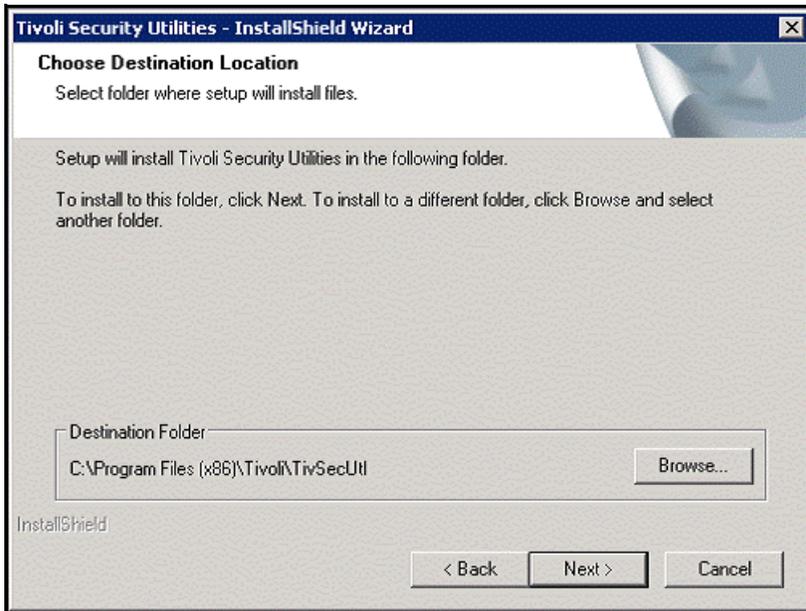


Figure 176. Tivoli Security Utilities installation wizard: Choose Destination Location screen

- ___ 6. Select the option "Yes, I want to restart my computer now" and click **Finish**.

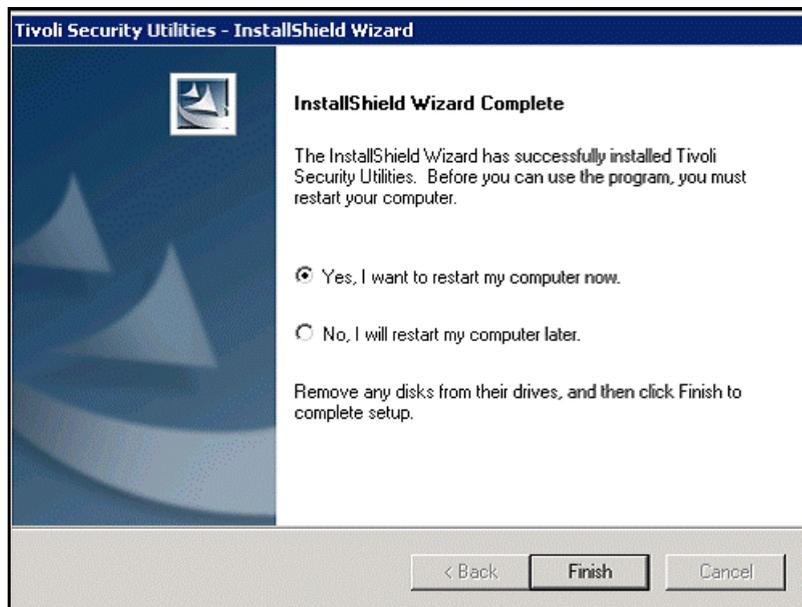


Figure 177. Tivoli Security Utilities installation wizard: InstallShield Wizard Complete



Note

You should restart computer when the installation requires it. Otherwise, you cannot proceed with subsequent steps.

Installing Access Manager Runtime/License/Policy Server

Follow these steps to install Access Manager Runtime/License/Policy server:

- ___ 1. Run the `setup.exe` file under
C:\software\TAM6.1.1\CZG8LML\windows\PolicyDirector\Disk Images\Disk1.
- ___ 2. Choose the language for the installation wizard.

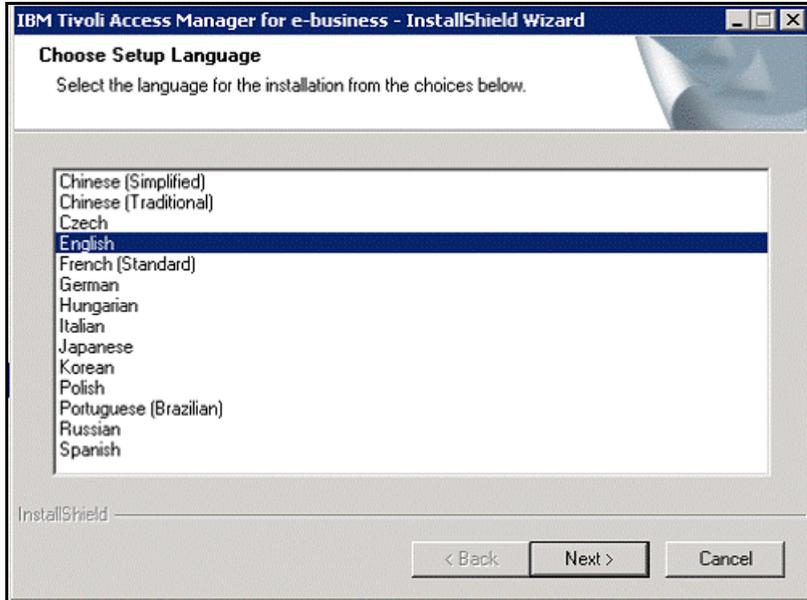


Figure 178. Choosing setup language

- ___ 3. On the wizard welcome screen, click **Next**.

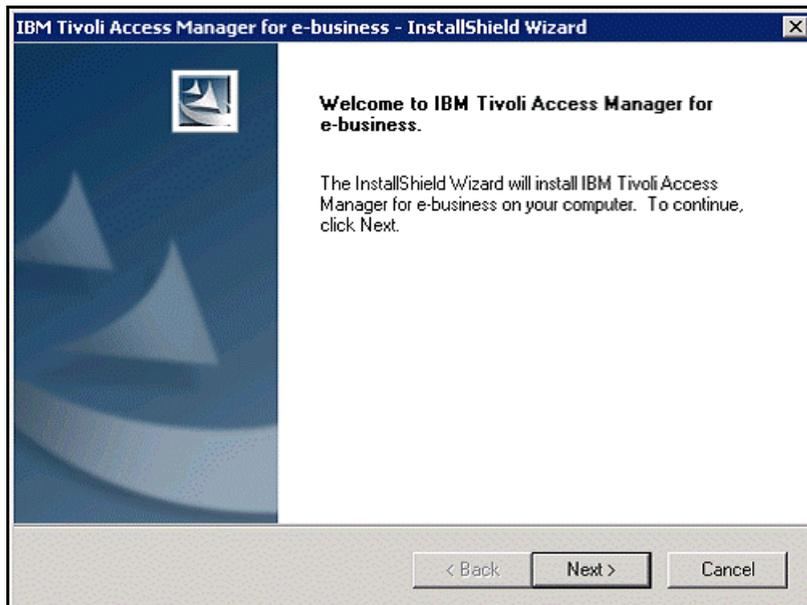


Figure 179. IBM Tivoli Access Manager for e-business: Welcome screen

- ___ 4. Read the license agreement and click **Yes**.

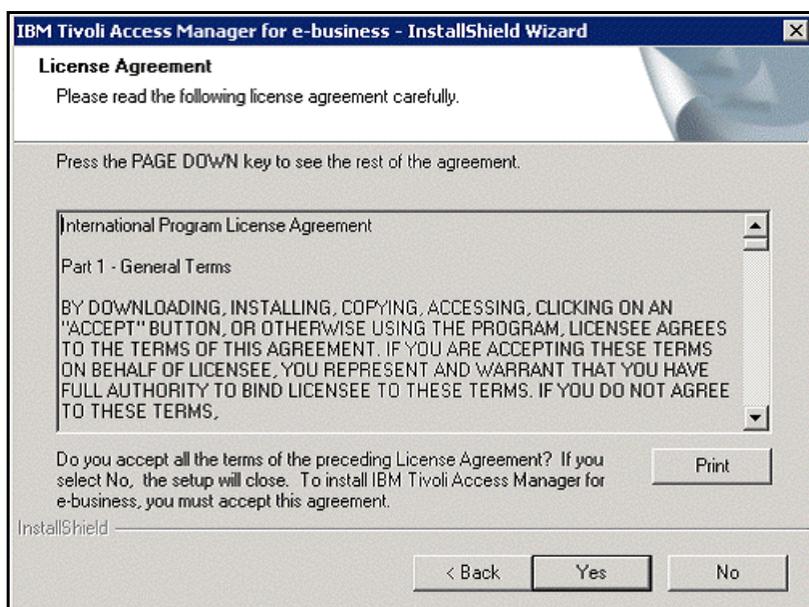


Figure 180. IBM Tivoli Access Manager for e-business: License agreement screen

- ___ 5. Select the access packages to install.

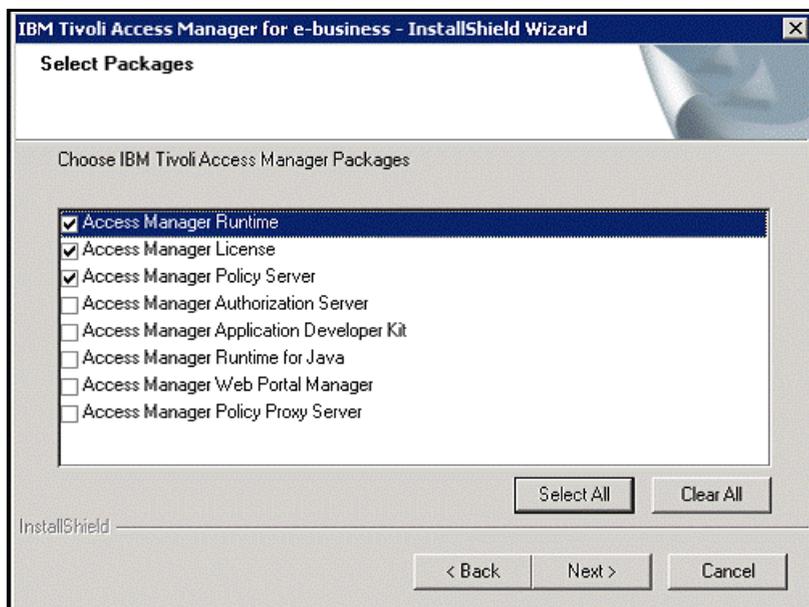


Figure 181. IBM Tivoli Access Manager for e-business: Select Packages screen

___ 6. On the welcome screen of the installation wizard for Access Manager License, click **Next**.

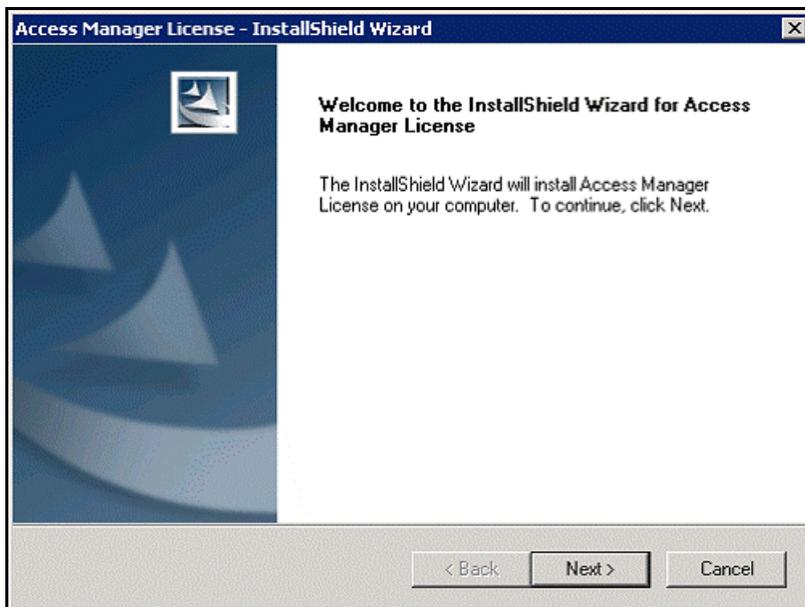


Figure 182. Access Manager License: Welcome screen

___ 7. Choose the destination location and click **Next**.

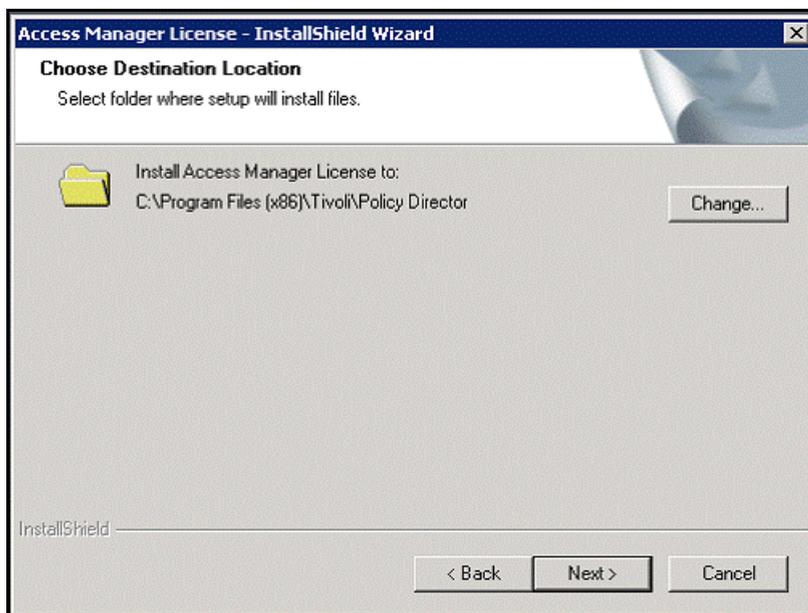


Figure 183. Access Manager License: Choose Destination Location screen

- ___ 8. Click **Install** to start the installation.

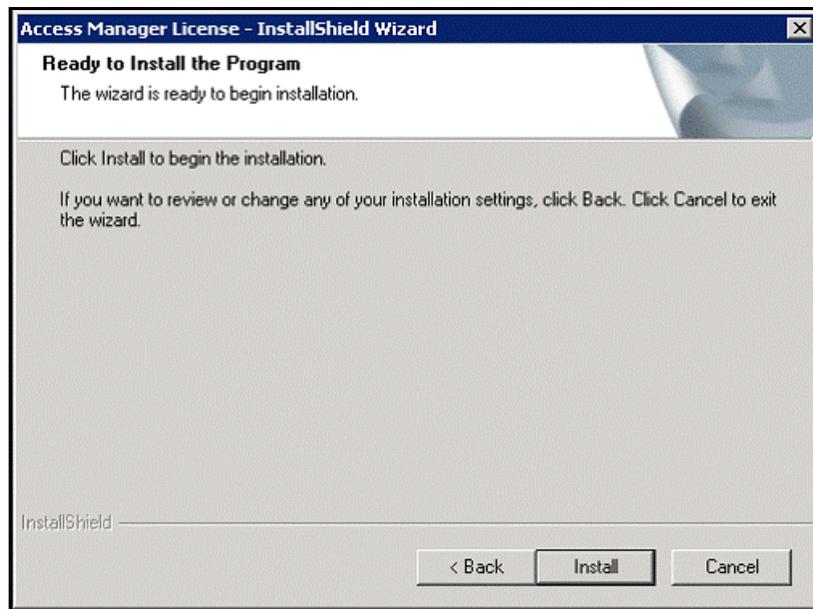


Figure 184. Access Manager License: Ready to Install the Program screen

- ___ 9. Select the option "Yes, I want to restart my computer now" and click **OK**.



Figure 185. Access Manager Installation Complete

Installing Access Manager Web Security Runtime/WebSEAL

Follow these steps to install Access Manager Web Security Runtime/WebSEAL:

- ___ 1. Run the `setup.exe` file under
C:\software\TAM6.1.1\CZG8MML\windows\PolicyDirector\Disk Images\Disk1.
- ___ 2. Choose the language for the installation wizard.

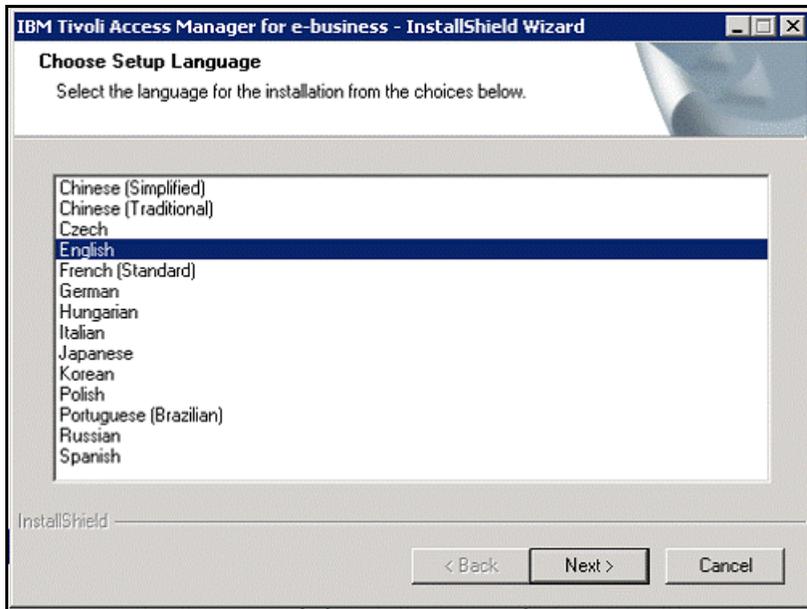


Figure 186. Choosing setup language

- ___ 3. On the wizard welcome screen, click **Next**.

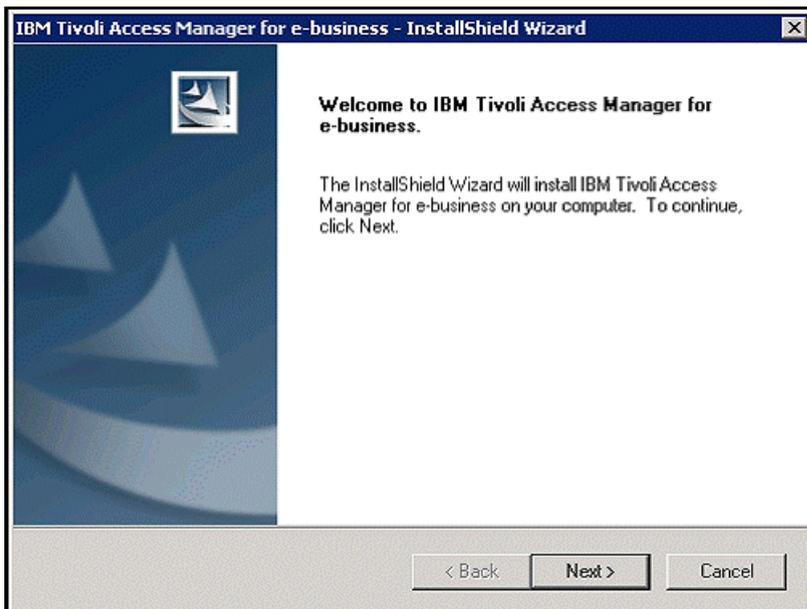


Figure 187. IBM Tivoli Access Manager for e-business: Welcome screen

- ___ 4. Read the license agreement and click **Yes**.

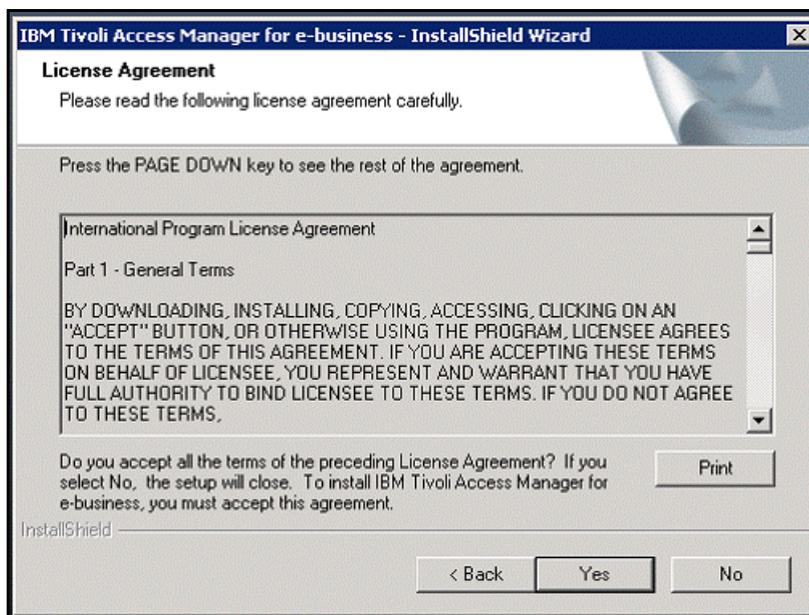


Figure 188. IBM Tivoli Access Manager for e-business: License agreement screen

- ___ 5. Select the access manager packages to install.

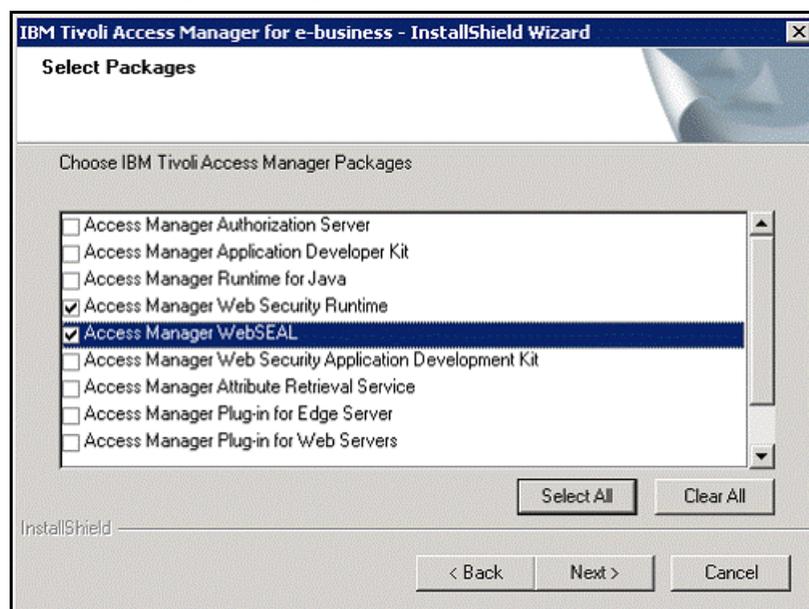


Figure 189. IBM Tivoli Access Manager for e-business: Select Packages screen

___ 6. On the welcome screen of the installation wizard for Access Manager WebSEAL, click **Next**.

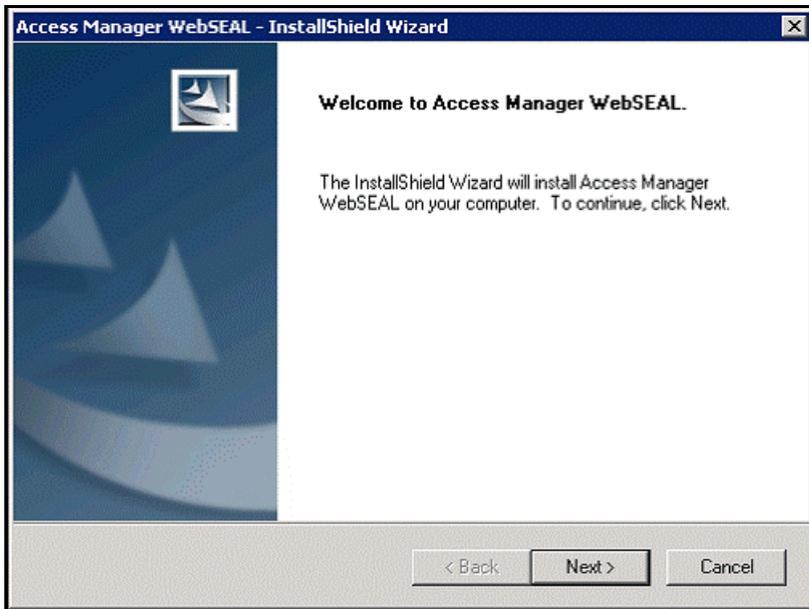


Figure 190. Access Manager WebSEAL: Welcome screen

___ 7. Read the license agreement and click **Yes**.

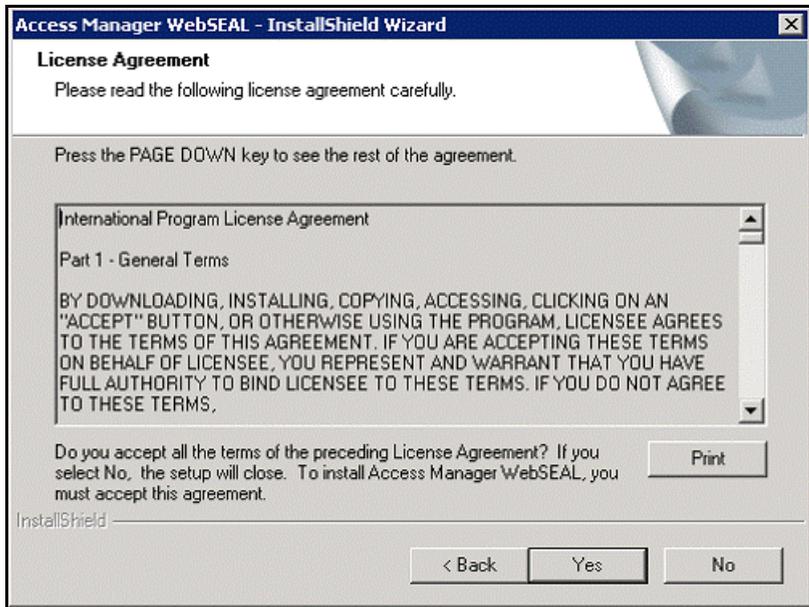


Figure 191. Access Manager WebSEAL: License agreement screen

- ___ 8. Choose the destination location and click **Next**.

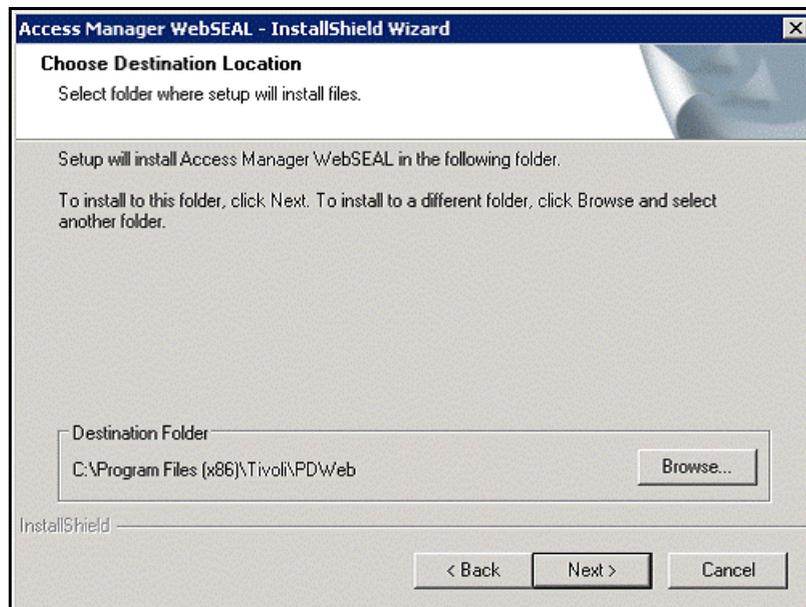


Figure 192. Access Manager WebSEAL: Choose Destination Location screen

- ___ 9. Click **OK** to exit the installation completion message.

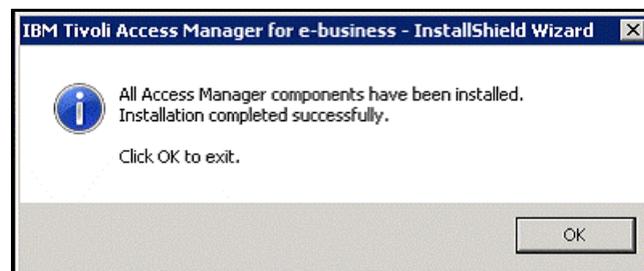


Figure 193. IBM Tivoli Access Manager for e-business: Installation completion message

- ___ 10. Restart your computer.

Configuring Tivoli Access Manager server

Follow these steps to configure Tivoli Access Manager server:

- ___ 1. Make sure that Domino Admin is installed on Tivoli Access Manager server and can connect to the Domino server which hosts LDAP successfully.

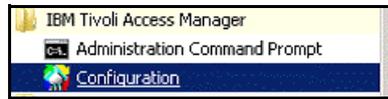


Figure 194. IBM Tivoli Access Manager -Configuration

- ___ 2. Configure Access Manager Runtime.
 - ___ a. Select Access Manager Runtime in the Access Manager Configuration wizard and click **Configure**.

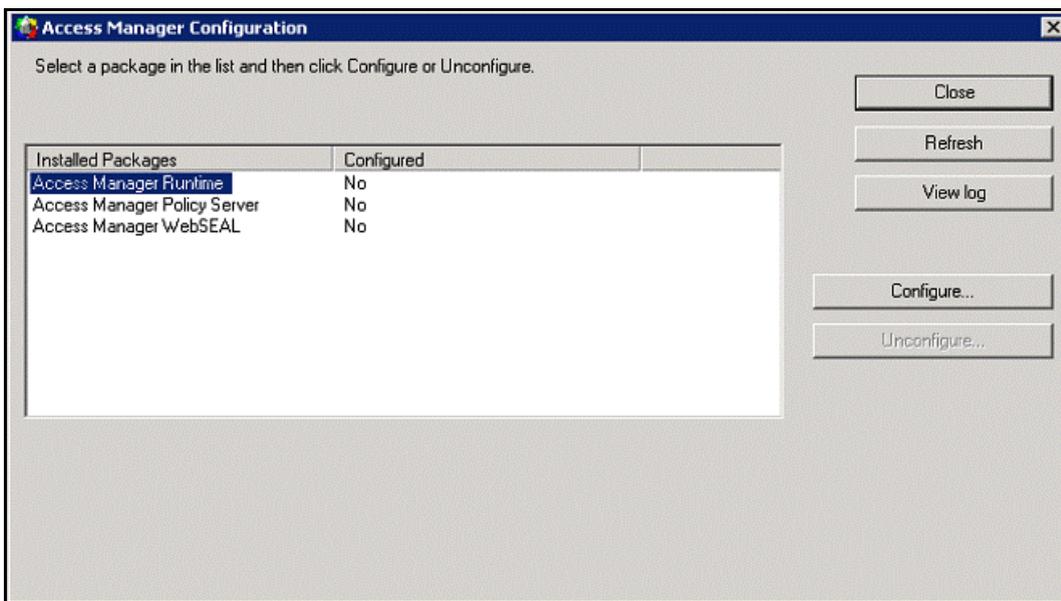


Figure 195. Access Manager Configuration: Access Manager Runtime

- ___ b. Make sure that Domino is selected and click **Next**.

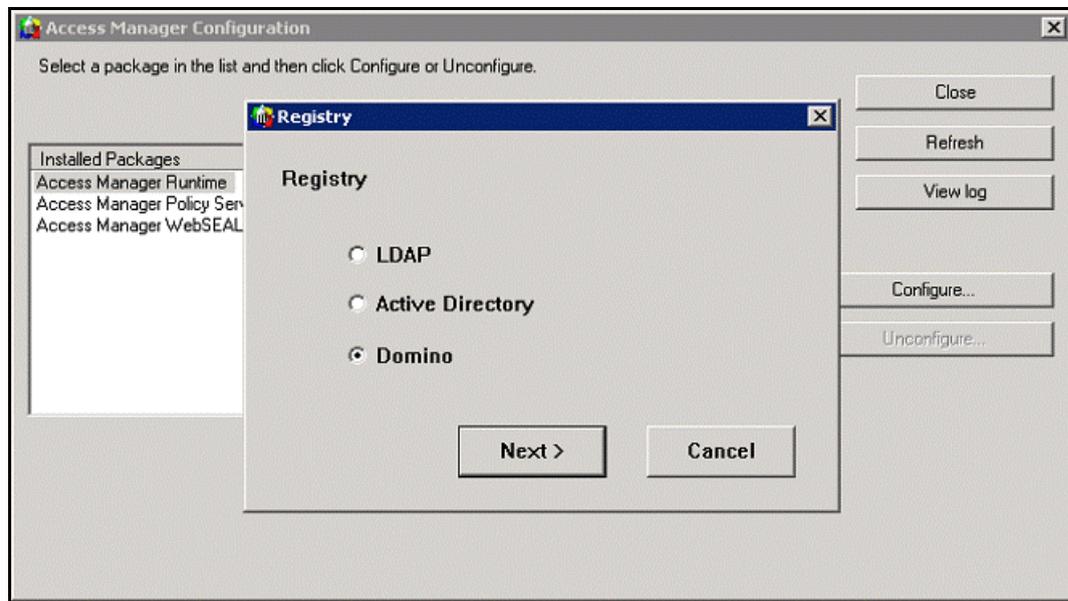


Figure 196. Access Manager Runtime: Registry

- ___ c. In the Domino server information, enter the domino server name and click **Next**.

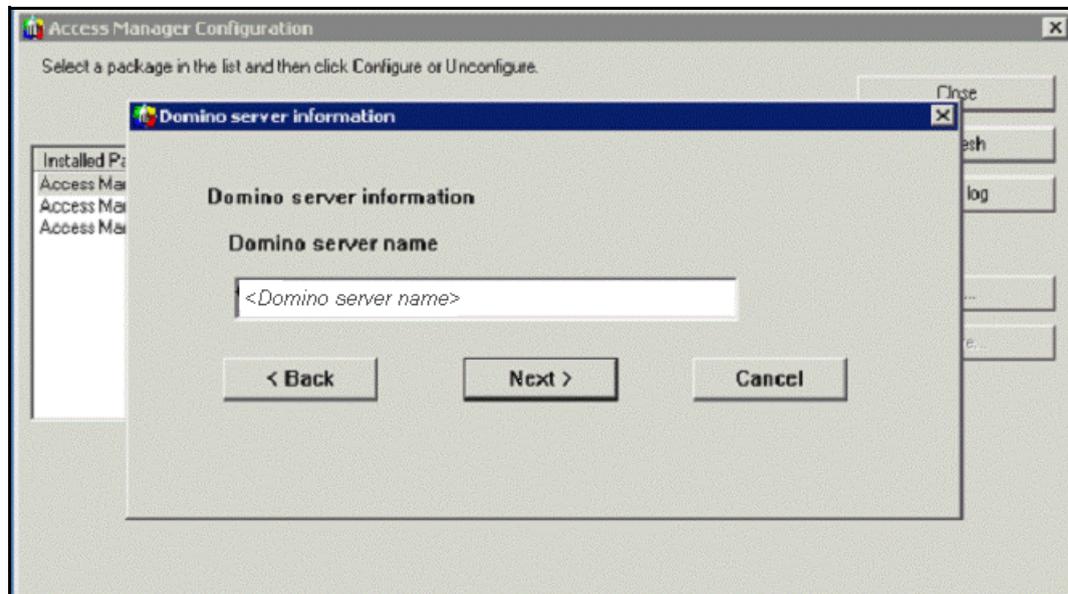


Figure 197. Access Manager Runtime: Domino server information

- ___ d. Enter the Notes client password and click **Next**.

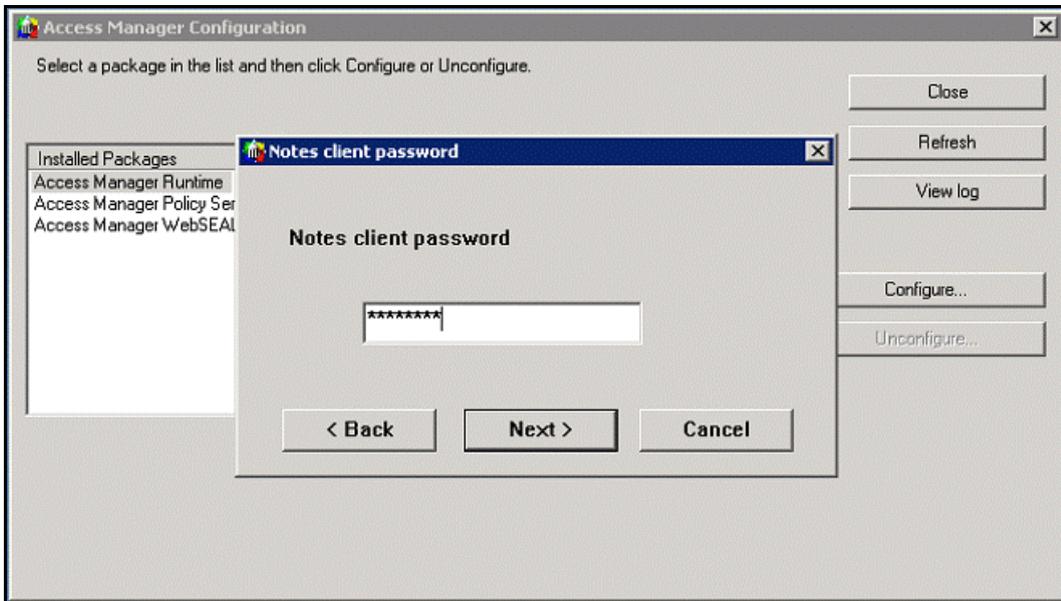


Figure 198. Access Manager Runtime: Notes client password

- ___ e. Ensure that the notes address book and the Access Manager database names are correct and click **Next**.

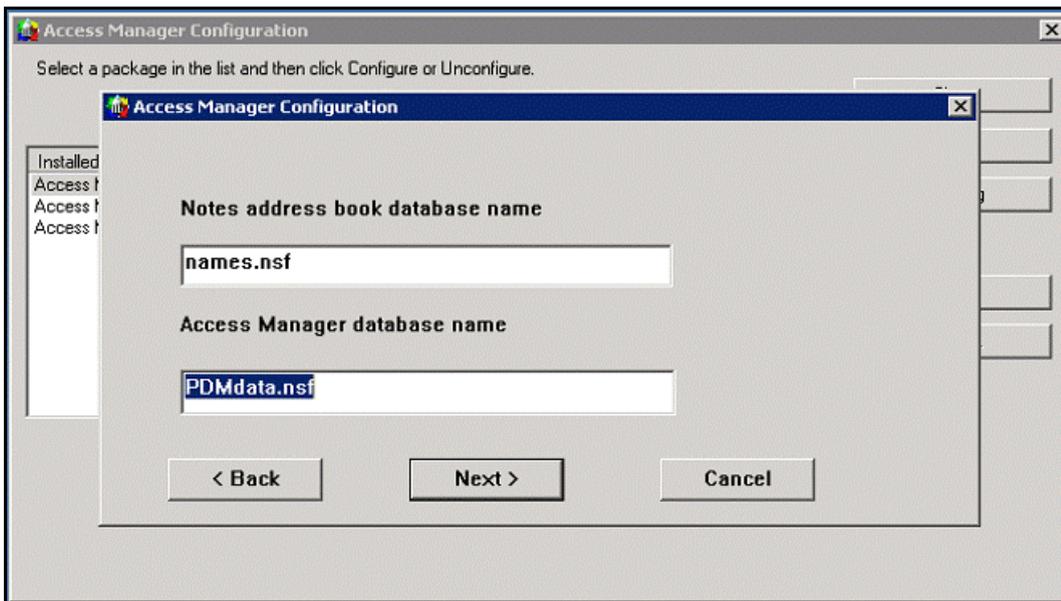


Figure 199. Access Manager Runtime: Notes address and database names

- ___ f. A window for configuring Tivoli Common Directory logging is displayed. If wanted, select Enable Tivoli Common Directory for logging and click **Next**.

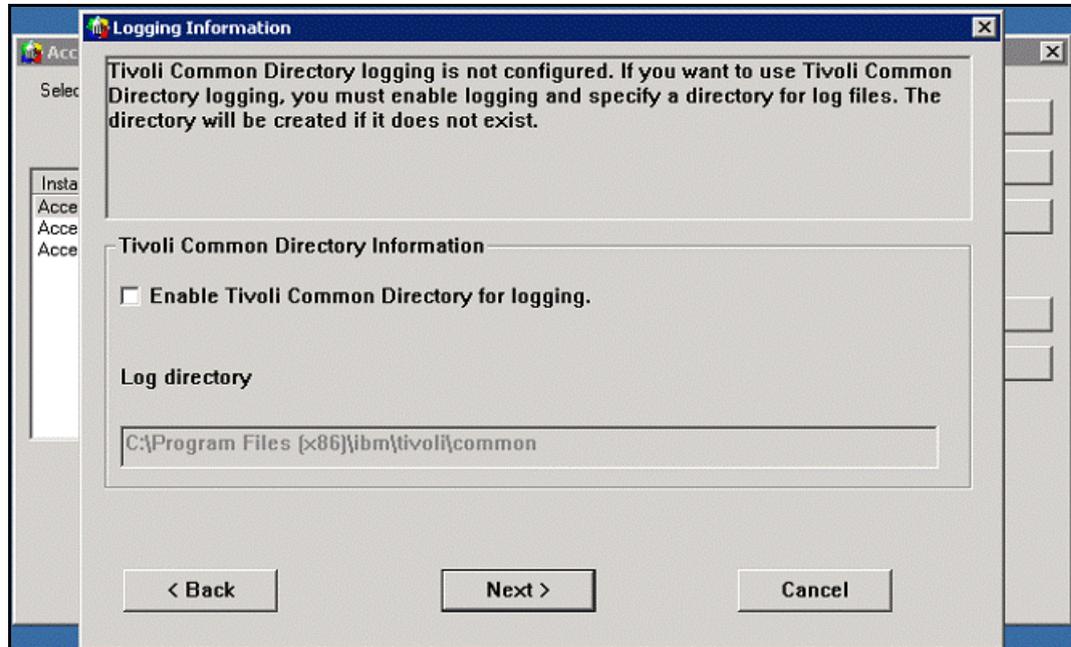


Figure 200. Access Manager Runtime: Logging information

- ___ g. Check the Access Manager Configuration review and click **Finish**.

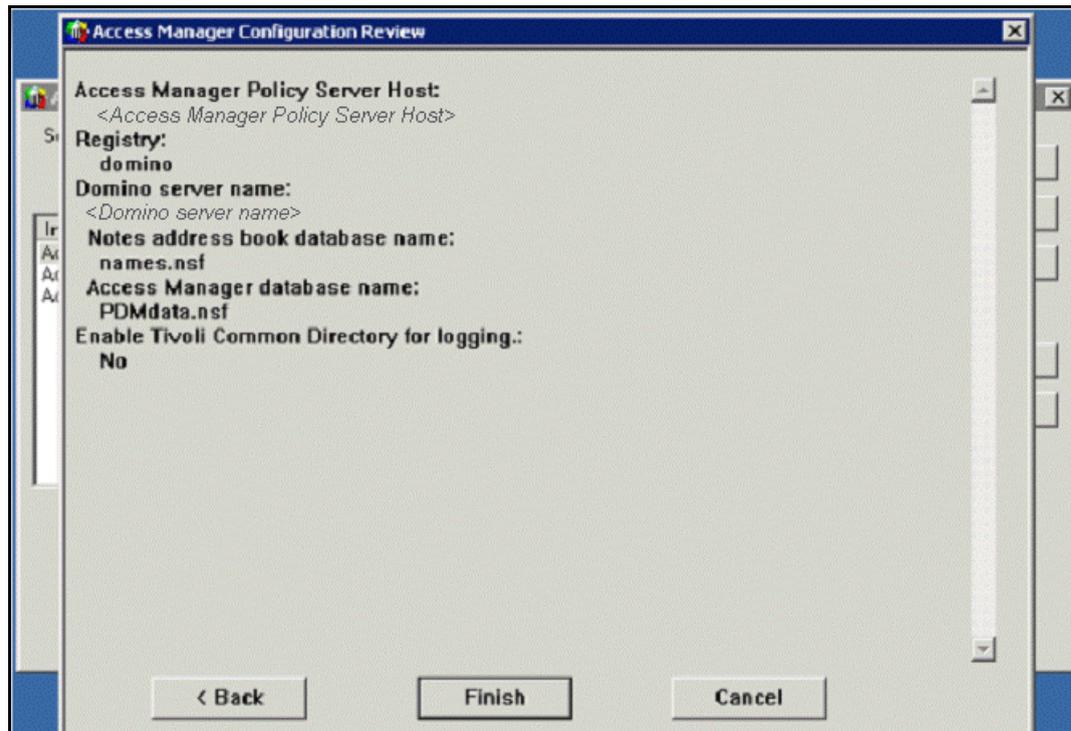


Figure 201. Access Manager Runtime: Configuration review

___ 3. Configure Access Manager Policy Server.

- ___ a. Select Access Manager Policy Server in the Access Manager Configuration wizard and click **Configure**.

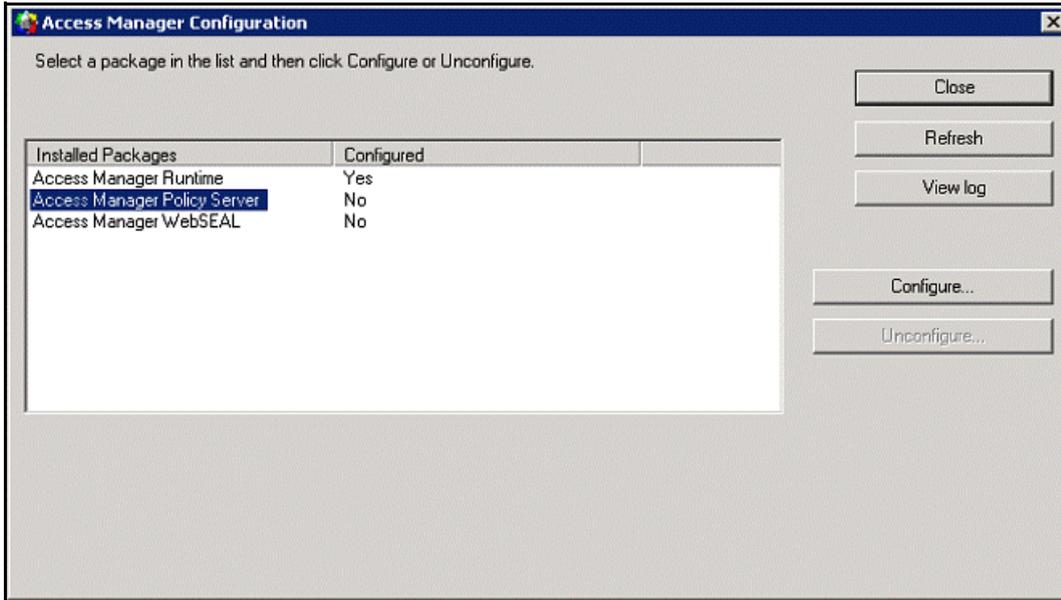


Figure 202. Access Manager Configuration: Access Manager Policy Server

- ___ b. Enter the ID and password for the Access Manager administrator and click **OK**.

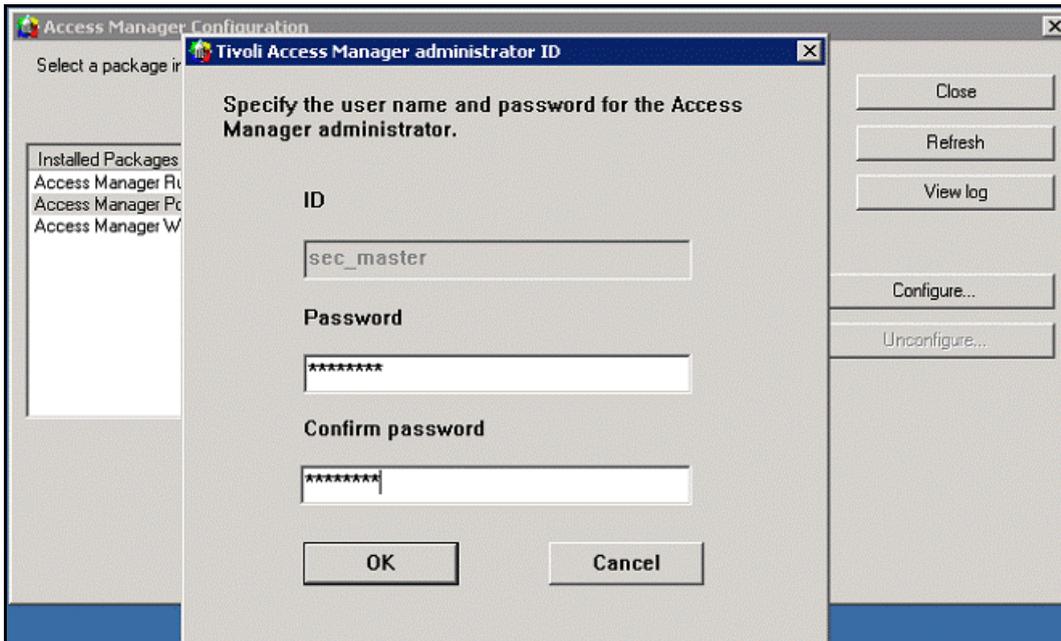


Figure 203. Access Manager Policy Server: Administrator ID

- ___ c. Specify the SSL connection parameters as shown in the figure and click **OK**.

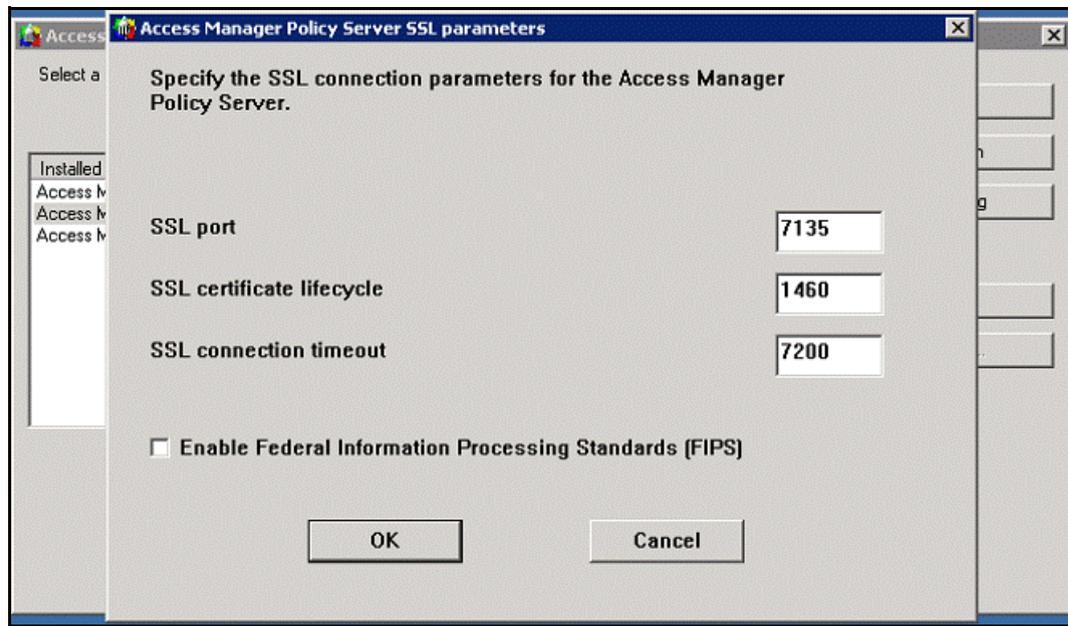


Figure 204. Access Manager Policy Server: SSL parameters

Access Manager Policy Server starts configuring.

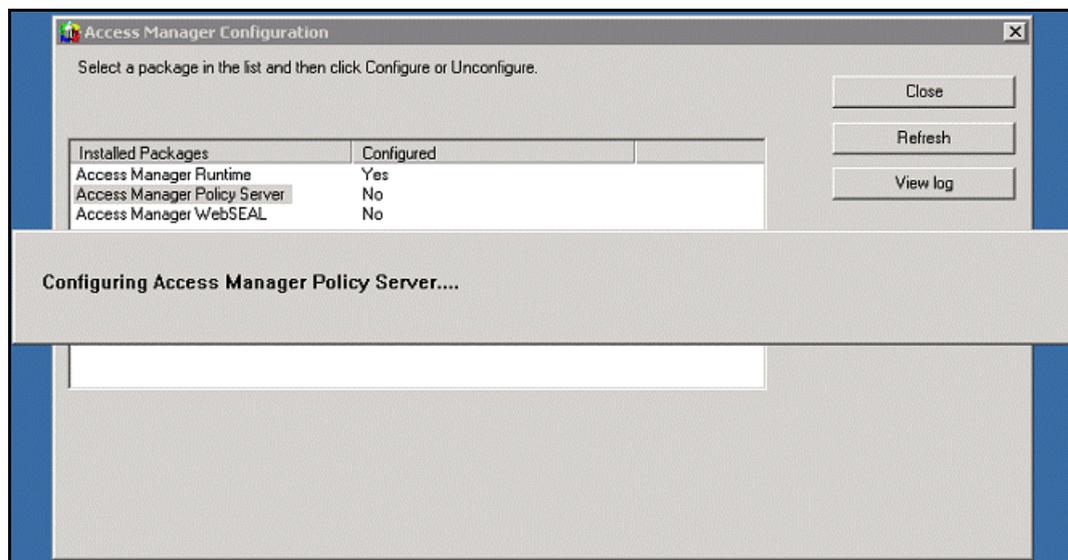


Figure 205. Access Manager Policy Server: Starting configuration

- ___ d. A configuration completion message is displayed. Click **OK** to close it.

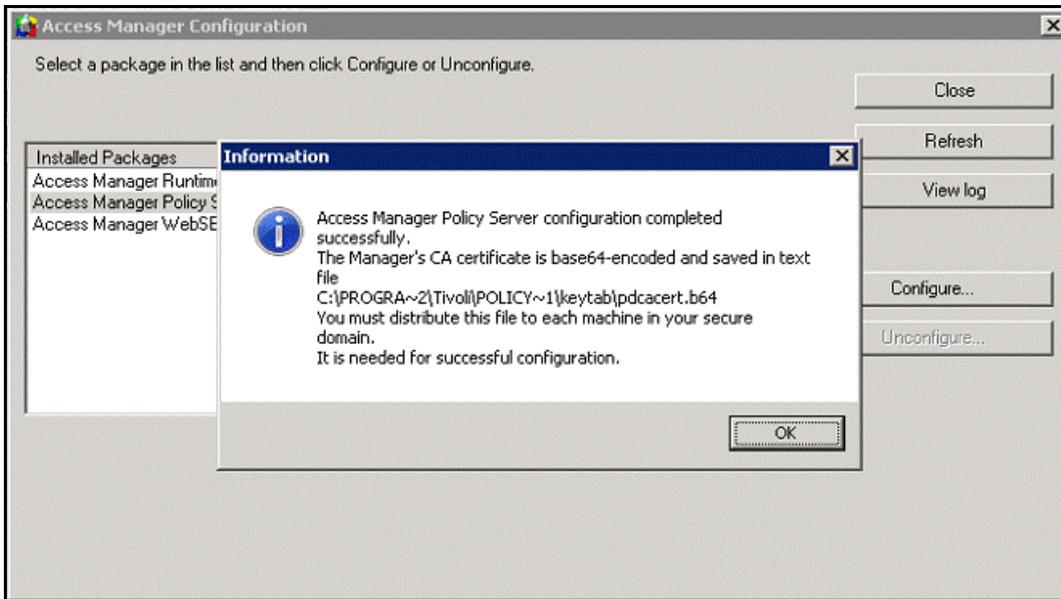


Figure 206. Access Manager Policy Server: Configuration completed

___ 4. Configure Access Manager WebSEAL.

- ___ a. Select Access Manager WebSEAL in the Access Manager Configuration wizard and click **Configure...**

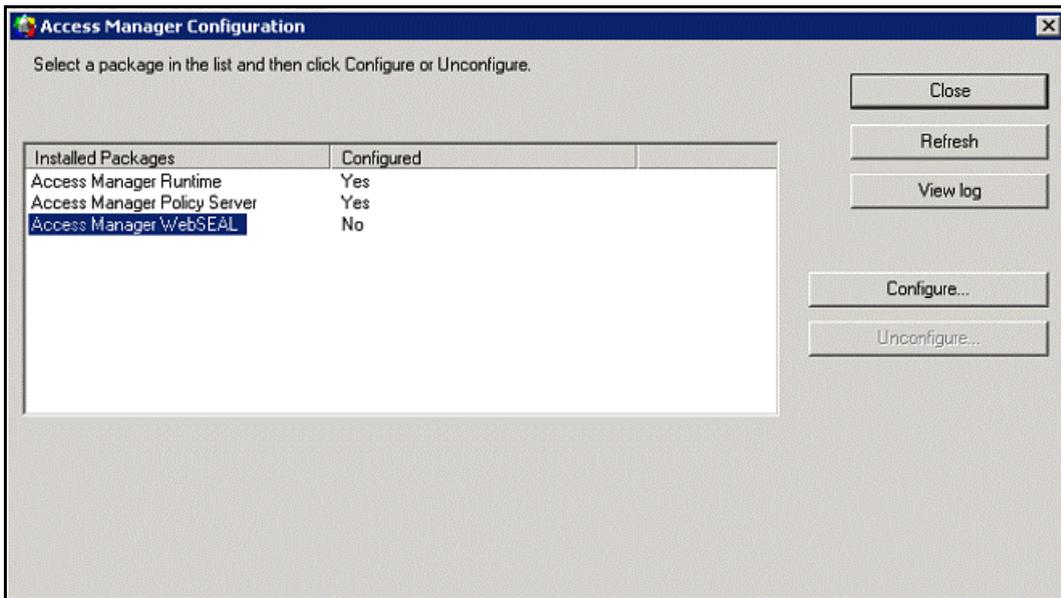


Figure 207. Access Manager Configuration: Access Manager WebSEAL

- ___ b. In the Access Manager WebSEAL Configuration screen, click **Configure...**

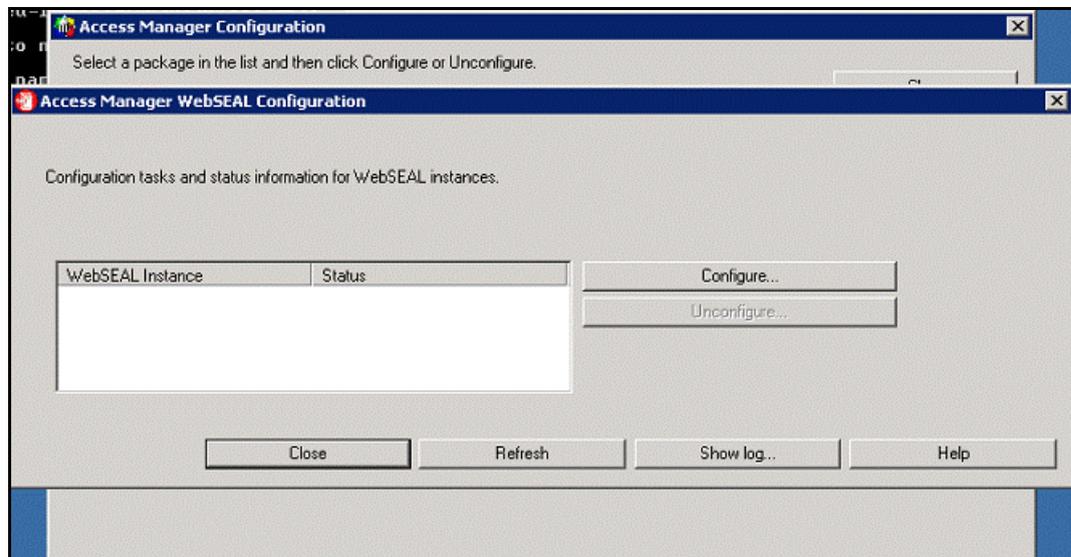


Figure 208. Access Manager WebSEAL: Configuring WebSEAL instances

- ___ c. Enter a name for the WebSEAL instance and click **Next**.

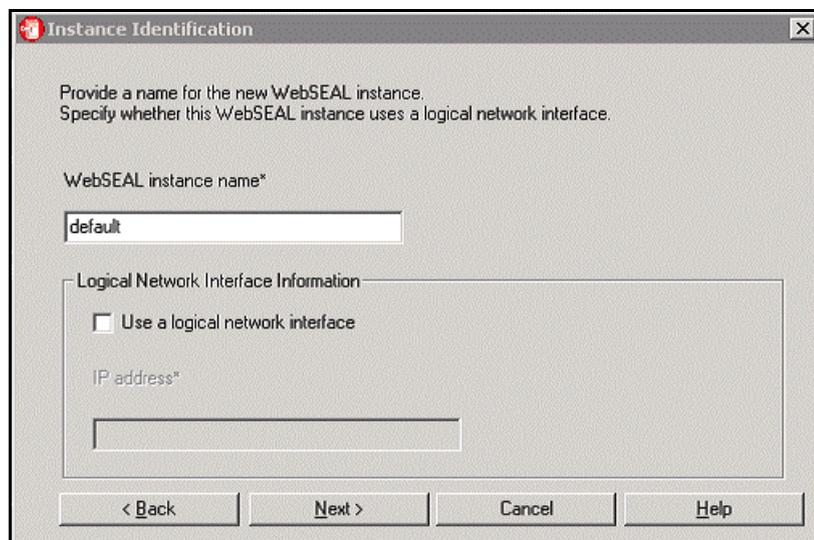


Figure 209. Access Manager WebSEAL: WebSEAL instance name

___ d. Enter the host name and the Listening port and click **Next**.

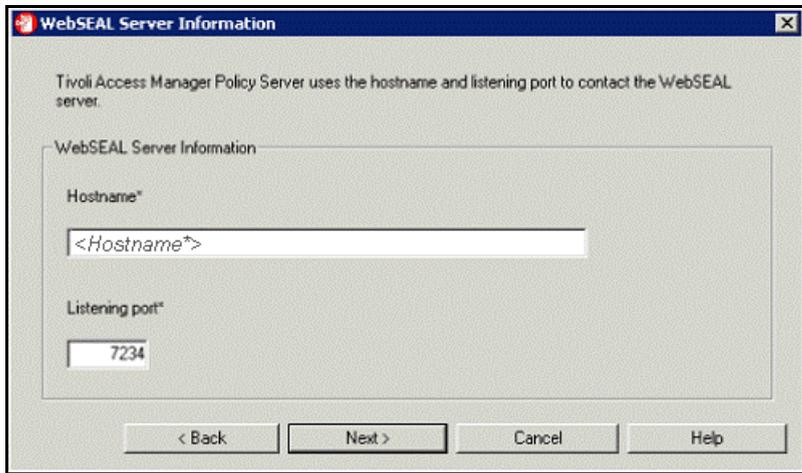


Figure 210. Access Manager WebSEAL: WebSEAL instance host name and listening port

___ e. Enter valid Administrator ID and password and click **Next**.

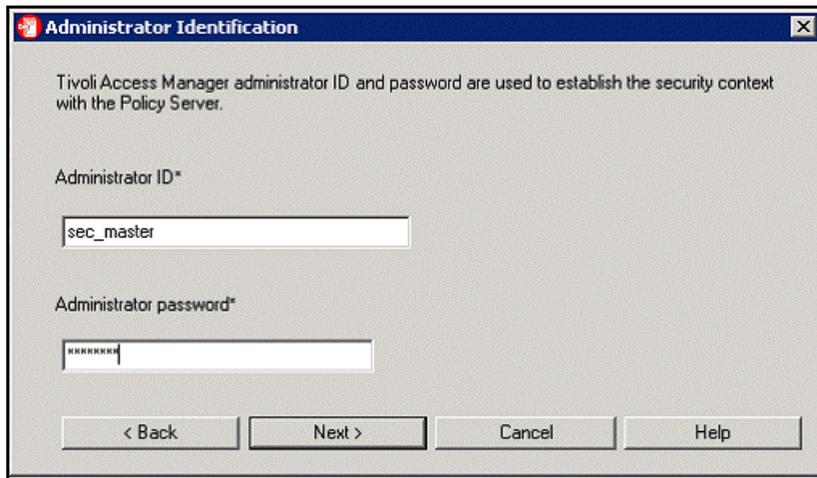


Figure 211. Access Manager WebSEAL: Administrator Identification

- ___ f. Specify whether you want to allow HTTP and HTTPS access and click **Finish**.

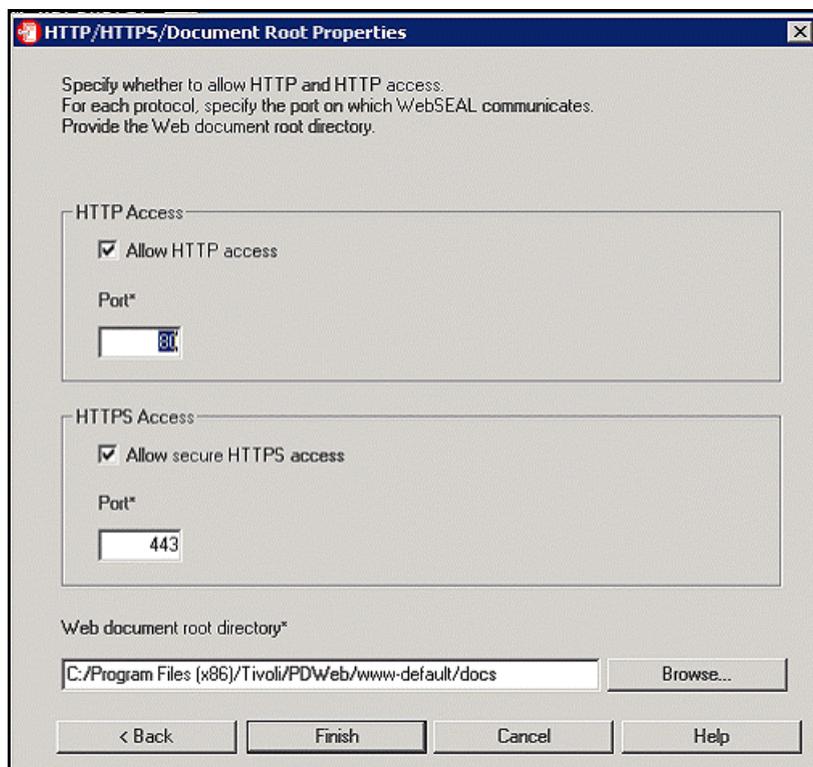


Figure 212. Access Manager WebSEAL: HTTP/HTTPS/DOcument Root Properties

- ___ g. As you can see in the figure, the WebSEAL instance status is started. Click **Close**.

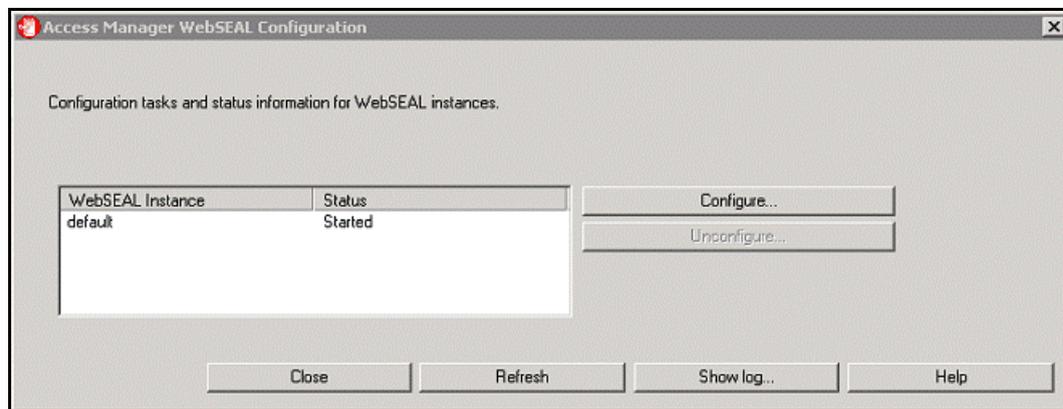


Figure 213. Access Manager WebSEAL: WebSEAL instance configured

Access Manager Runtime, Access Manager Policy Server, and Access Manager WebSEAL are successfully configured.

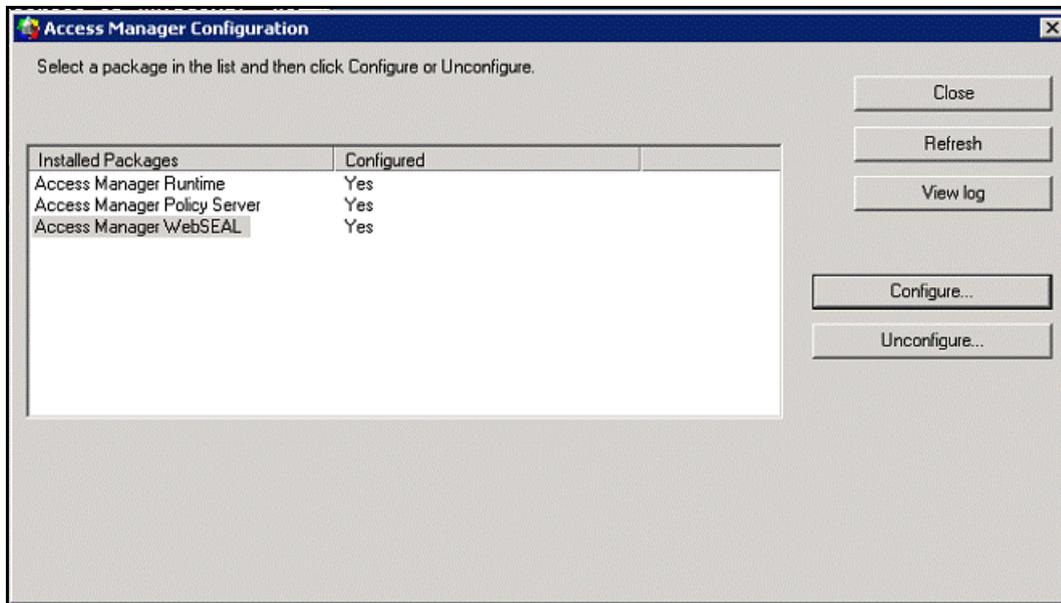


Figure 214. Access Manager Runtime, Policy Server, and WebSEAL successfully configured

Configuring Connections with Tivoli Access Manager SSO



Note

For more information about how to configure Connections with Tivoli Access Manager SSO, see http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Enabling_single_signon_for_Tivoli_Access_Manager_ic40&content=pdcontent.

Import LDAP users to the WebSEAL that you configured

Follow these steps to import LDAP users to the WebSEAL:

1. Create a `import.txt` file and the content should include the import commands for all the users you want with full DN name in LDAP, for example:

```
user import Aamir_000_000 "CN=Aamir
Aamir_000_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_001_000 "CN=Aamir
Aamir_001_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_002_000 "CN=Aamir
Aamir_002_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_003_000 "CN=Aamir
Aamir_003_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_004_000 "CN=Aamir
Aamir_004_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_005_000 "CN=Aamir
Aamir_005_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_006_000 "CN=Aamir
Aamir_006_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_007_000 "CN=Aamir
Aamir_007_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_008_000 "CN=Aamir
Aamir_008_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
user import Aamir_009_000 "CN=Aamir
Aamir_009_000,OU=Person,OU=SharedLDAP,OU=Lotus,O=ibm"
....
```

2. From a command window, start to import users by using the command such as follows:

```
C:\TAM config>pdadmin -a sec_master -p Password import.txt
```

Figure 215. Command window: Importing users command

___ 3. Create another `valid.txt` with the content such as follows:

```
user modify Aamir_000_000 account-valid yes
user modify Aamir_001_000 account-valid yes
user modify Aamir_002_000 account-valid yes
user modify Aamir_003_000 account-valid yes
user modify Aamir_004_000 account-valid yes
user modify Aamir_005_000 account-valid yes
user modify Aamir_006_000 account-valid yes
user modify Aamir_007_000 account-valid yes
user modify Aamir_008_000 account-valid yes
user modify Aamir_009_000 account-valid yes
```

From a command window, start to validate users by using the command such as follows:

```
G:\TAM config>pdadmin -a _sec_master -p Password valid.txt
```

Figure 216. Command window: Validating users command

___ 4. Verify that you can access `https://tam.example.com` by entering the username and password that you imported into WebSEAL.

Exporting WebSphere Application Server LTPA key from WebSphere Application Server console

- ___ 1. Go to **Global security > LTPA**.
- ___ 2. Input and confirm a password.
- ___ 3. Input a location to save output key and then click **Export keys**.

Cross-cell single sign-on

Single sign-on across cells can be provided by sharing keys and passwords. To share the keys and password, log on to one cell, and click Export keys. Then, log on to the other cell, specify the key file, and click Import keys.

* Password

* Confirm password

Fully qualified key file name
c:\Connections.key

Import keys Export keys

Figure 217. Cross-cell single sign-on

Use available authentication data when an unprotected URI is accessed

- ___ 1. On the Global security page, expand Web and SIP security, and then click **General settings**.
- ___ 2. Click Authenticate only when the URI is protected and select **Use available authentication data** when an unprotected URI is accessed, if it is not already selected.
- ___ 3. Click **Apply** and then click **OK**.

[Global security](#) > [Web security - General settings](#)
Specifies the settings for Web authentication.

[General Properties](#)

Web authentication behavior

Authenticate only when the URI is protected
 Use available authentication data when an unprotected URI is accessed

Authenticate when any URI is accessed

Default to basic authentication when certificate authentication for the HTTPS client fails

Figure 218. Global Security > Web security: General settings

Import your IBM HTTP Server certificate into the Tivoli Access Manager keystore

1. Copy the WebSEAL certificate key file to the system where IBM HTTP Server is installed. For example: Copy C:\Program Files\Tivoli\PDWeb\www-default\certs\pdsrv.kdb on the Tivoli Access Manager server to C:\pdsrv.kdb on the system where IBM HTTP Server is installed.
2. Start iKeyman on IBM HTTP Server server and open plugin-key.kdb that is used by the web server. The default password is **WebAS**.

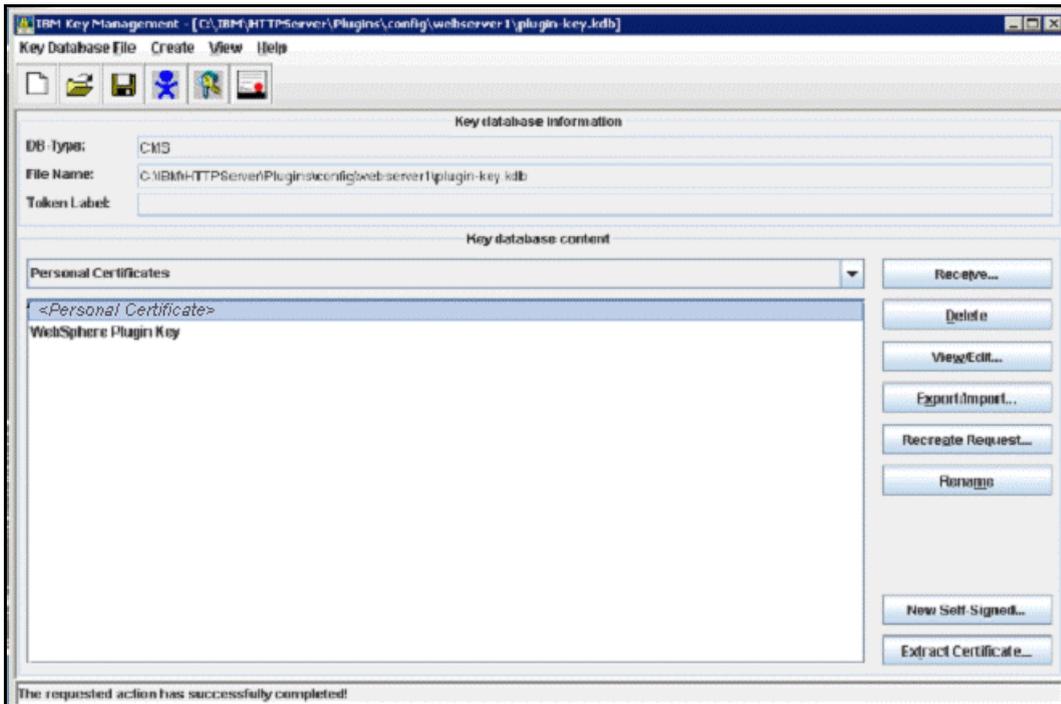


Figure 219. IBM Key Management

3. Select the certificate that you are using, click **Extract Certificate** and specify a file name and location for storing the certificates.

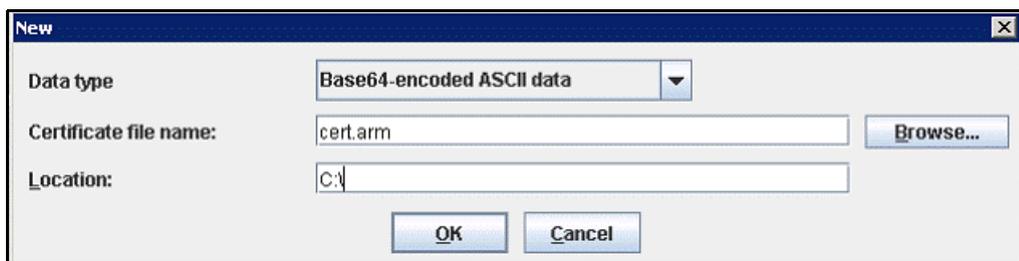


Figure 220. Name and location for the certificate

- ___ 4. Using the iKeyman to open `c:\pdsrv.kdb` you copied, the default password is **pdsrv**. Click **OK**.

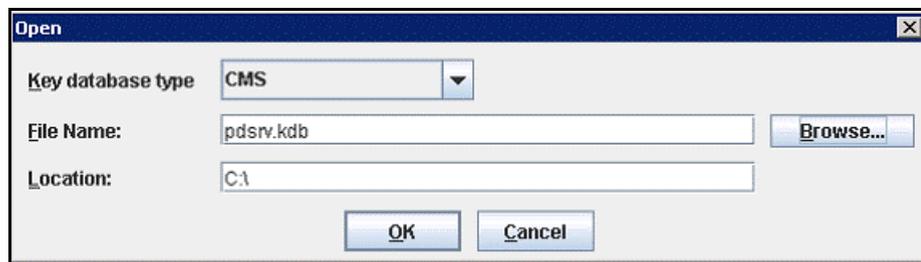


Figure 221. Opening the certificate

The IBM Key Management is displayed.

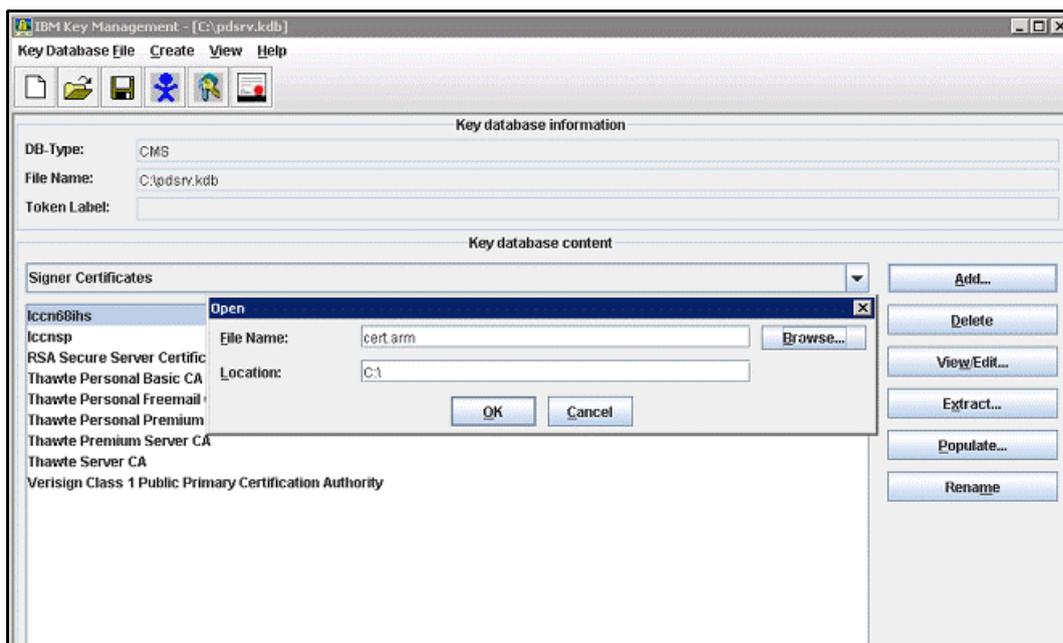


Figure 222. IBM Key Management

- ___ 5. Under Key database content, select **Signer Certificates**.
- ___ 6. Click **Add** and then locate the extracted IBM HTTP Server certificate file.
- ___ 7. Enter a label for this certificate.
- ___ 8. Close the iKeyman and copy the `c:\pdsrv.kdb` back to the WebSEAL computer where it originally locates, for example: `C:/Program Files/Tivoli/PDWeb/www-default/certs/pdsrv.kdb`.

9. Restart WebSEAL instance from windows service.

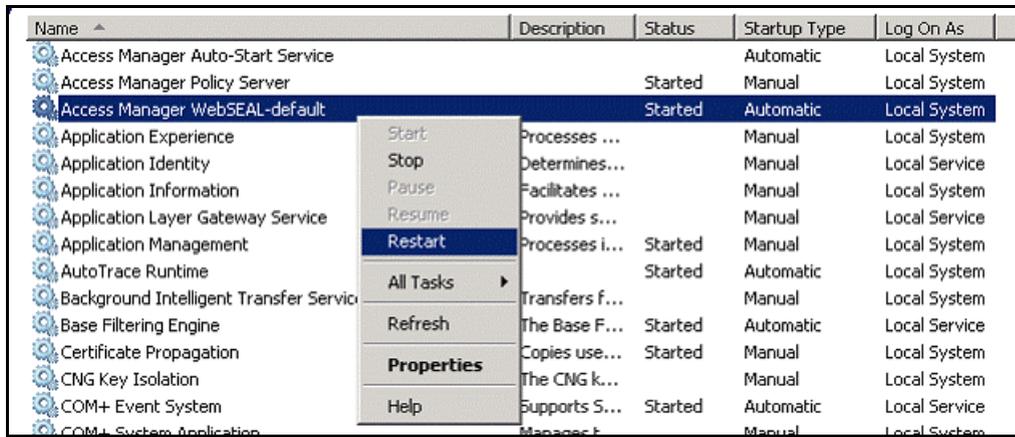


Figure 223. Restarting the WebSEAL instance

Creating junctions for Connections on WebSEAL

- ___ 1. Copy the LTPA key that you exported in step 4.3.2, from IBM HTTP Server computer to Tivoli Access Manager computer, for example, copy at c:\Connections.key.
- ___ 2. Create a junctions.txt with content such as follows:

```
server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /activities

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /blogs

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /communities

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /connections

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /cognos

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /dogear

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /files

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /forums

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /help

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /homepage

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /metrics

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /mobile

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /moderation

server task default-webseald-tam.example.com create -t ssl -h
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z
passwd /news
```

```
server task default-webseald-tam.example.com create -t ssl -h  
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z  
passwd /profiles
```

```
server task default-webseald-tam.example.com create -t ssl -h  
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z  
passwd /search
```

```
server task default-webseald-tam.example.com create -t ssl -h  
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z  
passwd /wikis
```

```
server task default-webseald-tam.example.com create -t ssl -h  
Connections.example.com -x -p 443 -i -b ignore -f -A -2 -k -F c:\Connections.key -Z  
passwd /oauth2
```

___ 3. From a command window, start to create junctions by using the command such as follows:

```
C:\TAM config>pdamin -a sec_master -p Password Junctions.txt
```

Figure 224. Command window: Creating junctions

Creating default ACL and attaching default ACL

1. Create a defaultacl.txt with content such as follows:

```
acl create connections-acl-default
acl modify connections-acl-default set user sec_master TcmdbsvaBRLrx
acl modify connections-acl-default set any-other Tmdrx
acl modify connections-acl-default set unauthenticated T
acl modify connections-acl-default set group iv-admin TcmdbsvaBRrxl
acl modify connections-acl-default set group webseal-servers Tgmdbsrxl

acl attach /WebSEAL/tam.example.com-default/activities connections-acl-default
acl attach /WebSEAL/tam.example.com-default/blogs connections-acl-default
acl attach /WebSEAL/tam.example.com-default/communities connections-acl-default
acl attach /WebSEAL/tam.example.com-default/dogear connections-acl-default
acl attach /WebSEAL/tam.example.com-default/files connections-acl-default
acl attach /WebSEAL/tam.example.com-default/forums connections-acl-default
acl attach /WebSEAL/tam.example.com-default/homepage connections-acl-default
acl attach /WebSEAL/tam.example.com-default/mobile connections-acl-default
acl attach /WebSEAL/tam.example.com-default/moderation connections-acl-default
acl attach /WebSEAL/tam.example.com-default/news connections-acl-default
acl attach /WebSEAL/tam.example.com-default/profiles connections-acl-default
acl attach /WebSEAL/tam.example.com-default/search connections-acl-default
acl attach /WebSEAL/tam.example.com-default/wikis connections-acl-default

acl attach /WebSEAL/tam.example.com-default/activities/seedlist/myserver
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/activities/service/atom2/communityEvent
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/activities/service/atom2/forms
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/activities/service/download/forms
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/activities/service/getnonce/forms
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/blogs/seedlist/myserver
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/dogear/seedlist/myserver
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/connections/opensocial/rest
connections-acl-default
acl attach /WebSEAL/tam.example.com-default/communities/calendar/seedlist/myserver
connections-acl-default
```

```
acl attach /WebSEAL/tam.example.com-default/communities/forum/service/atom/forms
connections-acl-default

acl attach /WebSEAL/tam.example.com-default/communities/service/atom/forms
connections-acl-default

acl attach /WebSEAL/tam.example.com-default/forums/atom/forms
connections-acl-default

acl attach /WebSEAL/tam.example.com-default/forums/seedlist/myserver
connections-acl-default

acl attach /WebSEAL/tam.example.com-default/metrics connections-acl-default

acl attach /WebSEAL/tam.example.com-default/cognos connections-acl-default

acl attach /WebSEAL/tam.example.com-default/profiles/atom/forms
connections-acl-default

acl attach /WebSEAL/tam.example.com-default/profiles/atom2/forms
connections-acl-default
```

- ___ 2. From a command window, start to attach default `acl` by using the command such as follows:

```
C:\TAM config>pdadmin -a sec_master -p Password defaultacl.txt
```

Figure 225. Command window: Attaching command

Creating bypass ACL and attaching bypass ACL

- ___ 1. Create a `bypassacl.txt` with content such as follows:

```

acl create connections-acl-bypass
acl modify connections-acl-bypass set user sec_master TcmdbsvaBRlrx
acl modify connections-acl-bypass set any-other Tmdrx
acl modify connections-acl-bypass set unauthenticated Tmdrx
acl modify connections-acl-bypass set group iv-admin TcmdbsvaBRrxl
acl modify connections-acl-bypass set group webseal-servers Tgmdbsrxl

acl attach /WebSEAL/tam.example.com-default/activities/auth connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/authverify
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/images connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/mainpage
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/oauth connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/images
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/servermetrics
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/serverstats
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/static connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/styles
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/service/html/themes
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/activities/serviceconfigs
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/static connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/oauth connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/serviceconfigs
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/bookmarklet/tagslike/proxy
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/oauth connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/peoplelike connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/serviceconfigs
connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/static connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/tagslike connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/tagrecs connections-acl-bypass

```

```
acl attach /WebSEAL/tam.example.com-default/communities/calendar/Calendar.xml
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/calendar/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/images
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/recomm/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/atom/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/opensocial/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/serviceconfigs
connections-acl-bypass

acl attach
/WebSEAL/tam.example.com-default/communities/service/html/community/autoCompleteMembers.do connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/static
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/stylesheet
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/core/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/resources/web
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/resources/ic
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/nav/common connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/app connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/basic/anonymous/api
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/basic/anonymous/cmisis
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/basic/anonymous/opensocial
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/form/anonymous/api
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/form/anonymous/cmisis
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/form/anonymous/opensocial
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/forums/oauth connections-acl-bypass
```

```
acl attach /WebSEAL/tam.example.com-default/forums/serviceconfigs
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/forums/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/search connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/serviceconfigs
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/web/updates/
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/metrics/service/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/metrics/service/eventTracker
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/cognos/servlet connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/moderation/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/help connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/microblogging/isPermitted.action
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/follow/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/serviceconfigs
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/sharebox/config.action
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/oauth2 connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/images connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/serviceconfigs
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/search/atom/search/*
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/search/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/search/oauth connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/anonymous/rest
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/common
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/gadgets
connections-acl-bypass
```

```
acl attach /WebSEAL/tam.example.com-default/connections/opensocial/ic
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/oauth
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/rpc
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/social
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/xrds
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/opensocial/xpc
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/wikis/basic/anonymous/api
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/wikis/form/anonymous/api
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/wikis/oauth connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/wikis/static connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/activities/follow/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/activities/service/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/activities/service/atom2
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/activities/service/download
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/activities/service/getnonce
connections-acl-bypass

acl attach
/WebSEAL/tam.example.com-default/activities/service/html/autocompleteactivityname
connections-acl-bypass

acl attach
/WebSEAL/tam.example.com-default/activities/service/html/autocompleteentryname
connections-acl-bypass

acl attach
/WebSEAL/tam.example.com-default/activities/service/html/autocompletemembers
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/api connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/atom connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/issuecategories
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/follow/atom connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/roller-ui/blog
connections-acl-bypass
```

```
acl attach /WebSEAL/tam.example.com-default/blogs/roller-ui/feed
connections-acl-bypass

acl attach
/WebSEAL/tam.example.com-default/blogs/roller-ui/BlogsWidgetEventHandler.do
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/roller-ui/rendering/api
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/roller-ui/rendering/feed
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/services/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/dogear/api/app connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/api/deleted
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/dogear/api/notify connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/atom connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/dogear/people.do connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/connections/opensocial/basic/rest
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/calendar/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/calendar/handleEvent
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/calendar/ical
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/follow/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/forum/service/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/atom/communities/my
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/json
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/communities/service/opensocial
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/basic/api connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/files/basic/api/myuserlibrary/feed
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/basic/cmis connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/files/basic/opensocial
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/files/follow/atom connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/forums/atom connections-acl-bypass
```

```
acl attach /WebSEAL/tam.example.com-default/forums/follow/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/atom/mysearch
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/homepage/atom/search
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/service connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/community
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/newsfeed
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/public
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/save
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/saved
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/statusupdates
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/stories/top
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atom/watchlist
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/news/atomfba/stories/public
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/atom connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/profiles/atom/forms/tagCloud.do
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/follow/atom
connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/profiles/json connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/profiles/vcard connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/profiles/photo.do connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/profiles/audio.do connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/profiles/atom2 connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/wikis/basic/api connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/wikis/follow/atom connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/blogs/blogsfeed connections-acl-bypass
acl attach /WebSEAL/tam.example.com-default/blogs/blogsapi connections-acl-bypass

acl attach /WebSEAL/tam.example.com-default/connections/bookmarklet/tools/blet.js
connections-acl-bypass
```

```
acl attach  
/WebSEAL/tam.example.com-default/connections/bookmarklet/tools/discussThis.js  
connections-acl-bypass  
  
acl attach /WebSEAL/tam.example.com-default/connections/bookmarklet/tools/rlet.js  
connections-acl-bypass
```

- ___ 2. From a command window, start to attach bypass acl by using the command such as follows:

```
C:\IAM config>pdadmin -a sec_master -p Password bypassacl.txt
```

Figure 226. Command window: Attaching bypass command

Specifying a dynamic URL pattern to support the blogs

1. Create a `dynurl` configuration file named `dynurl.conf` with content such as follows:

```
/blogs/blogsfeed          /blogs/*/feed/*
/blogs/blogsapi           /blogs/*/api/*
```

2. Save the file in the `webseal-instance-docroot/lib` directory. For example: `C:\Program Files\Tivoli\PDweb\www-default\lib`.



Note

The related bypass ACL for the previous URLs is included in [Creating bypass ACL and attaching bypass ACL](#).

Modifying `webseald-default.conf` configuration

1. Find `webseald-default.conf` under `C:\Program Files (x86)\Tivoli\PDWeb\etc`.
2. Edit it with your favorite editor and change the following values. Note some comments in `<>`:

```
web-host-name = tam.example.com <your TAM host>
dynurl-allow-large-posts = yes
type = application/atom+xml <add this line>
script-filter = yes
rewrite-absolute-with-absolute = yes
ba-auth = none
forms-auth = both
ltpa-auth = both          <For domino SSO special>
keyfile = c:\Connections.key      <For domino SSO special>
keyfile-password = password      <For domino SSO special>
cookie-name = LtpaToken2        <For domino SSO special, notice the CAP>
cookie-domain = example.com     <For domino SSO special>
use-same-session = yes
domain = example.com
```

3. Save the file and restart WebSEAL default instance.

Updating LotusConnections-config.xml configuration file

- __ 1. Update dynamicHost setting as follows:

```
<dynamicHosts enabled="true">  
  <host href="http://tam.example.com" ssl_href="https://tam.example.com"/>  
</dynamicHosts>
```

- __ 2. Replace all interService URL in lcc.xml to use Tivoli Access Manager host, that is, set all interService URL like:

```
<sloc:interService href="https://tam.example.com"/>
```

- __ 3. Change lcc.xml to use Tivoli Access Manager Authenticator as follows:

```
<customAuthenticator name="TAMAuthenticator"/>
```

- __ 4. Save your changes and sync to nodes.

Modifying HTTP server

1. Find `httpd.conf` under `C:\IBM\HTTPServer\conf`, open it with your favorite editor and add the following rewrite rules into it as follows:

```
LoadModule was_ap22_module
"C:\IBM\HTTPServer\Plugins\bin\32bits\mod_was_ap22_http.dll"
WebSpherePluginConfig "C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-cfg.xml"
LoadModule rewrite_module modules/mod_rewrite.so
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName Connections.example.com
#DocumentRoot C:\IBM\HTTPServer\htdocs
SSLEnable
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
</VirtualHost>
</IfModule>
SSLDisable
Keyfile C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.kdb
SSLStashFile C:\IBM\HTTPServer\Plugins\config\webserver1\plugin-key.sth
```

2. Restart HTTP server.

Importing the Tivoli Access Manager certificate into WebSphere Application Server

1. Go to **Security > SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates**.
2. Click **Retrieve from port**, and input the Tivoli Access Manager host name and port number:

SSL certificate and key management

SSL certificate and key management > Key stores and certificates > CellDefaultTrustStore > Signer certificates > Retrieve from port

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

General Properties

* Host
tam.example.com

* Port
443

SSL configuration for outbound connection
CellDefaultSSLSettings

* Alias
tam

Retrieve signer information

Apply OK Reset Cancel

Figure 227. SSL certificate and key management

3. Click **OK** and then **Save**.
4. Restart your cluster. Stop all application servers and all nodes, and then restart the deployment manager, all the nodes, and all the application servers.

5. Configuring integration with Connections

Configuring Sametime integration



Information

For more information about how to configure integration with Connections, see http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=Adding_Sametime_awareness_through_the_Sametime_server_ic40&content=pdcontent.



Note

Suppose that you have Sametime 8.5.2 installed, with IFR1 and latest test fix.

Configuring SSO between Sametime web proxy server and Connections

- ___ 1. Copy the LTPA key from Connections server to Sametime web proxy server, for example, `c:\Connections.key`.
- ___ 2. Create a Web SSO document on the Sametime Community Server:
 - ___ a. Start the Domino Administration Client. Select **File > Application > Open**, and enter the name of the Sametime Server.
 - ___ b. Open the `Names.nsf` database.
 - ___ c. Select **Configuration**, expand **Web**, and click **Web Configurations**. In there, you find the Web SSO token that Sametime automatically creates.
 - ___ d. Choose to edit the document. Click **Keys > Import WebSphere LTPA Keys**.
 - ___ e. Type the path and the name of the LTPA key file.
 - ___ f. Type the password. The key should be imported. Make sure that the Configuration Name field is `LtpaToken`.
 - ___ g. Enter the DNS domain to your domain name and then set the Map names in LTPA tokens field to `Disabled`.
 - ___ h. Add the Sametime server to the Domino Server Names list.

- ___ i. All the data in the WebSphere Information section will populate automatically after the WebSphere token is imported. You must change the Token format to “LtpaToken and LtpaToken2 (compatible with all releases of Domino)” so that all the community server features are available for user in the `stcenter.nsf`.

The screenshot shows a dialog box titled "Web SSO Configuration for : LtpaToken". It has tabs for "Basics", "Comments", and "Administration". The "Basics" tab is active and contains the following sections:

Token Configuration		Token Expiration	
Configuration Name:	LtpaToken	Expiration (minutes):	30
Organization:			
DNS Domain:	.cn.ibm.com		
Map names in LTPA tokens:	Disabled		
Require SSL protected communication (HTTPS):	Disabled		
Restrict use of the SSO token to HTTP/HTTPS:	Disabled		

Participating Servers

Domino Server Names: <Domino Server Names>

Windows single sign-on integration (if available): Disabled

WebSphere Information

Token Format:	LtpaToken and LtpaToken2 (compatible with all releases of Domino)
LDAP Realm:	defaultWIMFileBasedRealm
LTPA Version:	1.0

Figure 228. Web SSO Configuration for: LtpaToken

- ___ j. Save the document.
- ___ k. Under **Configuration > Servers > All Server Documents**, select your Sametime server name and click **Edit server**.
- ___ l. Click the **Internet Protocol** tab and then the **Domino Web Engine** tab.
- ___ m. Change the Session authentication to Multiple Servers (SSO), and ensure that the Web SSO configuration field is set to LtpaToken.
- ___ n. Save the document and restart the server.



Hint

With SSO configuration, verify by logging in to Connections first and then switch to Sametime URL, and you are automatically logged in.

Enabling ST awareness in IC

1. Open LotusConnections-config.xml with your favorite editor. Change the Sametime integration section as follows:

```
<sloc:serviceReference enabled="true" isConnectClient="false"
serviceName="sametimeProxy" ssl_enabled="false">
  <sloc:href>
    <sloc:hrefPathPrefix/>
    <sloc:static href="http://sametime.example.com:9081"
ssl_href="https://sametime.example.com:9444" isExternal="true"/>
    <sloc:interService href="https://sametime.example.com:9444"/>
  </sloc:href>
</sloc:serviceReference>
```



Note

You must make sure that the URL for Sametime web client is correct and that the isExternal parameter that is marked as bold is added and set as true.

2. Sync all nodes and restart servers.

Configuring QuickrD integration



Information

For more information about how to configure QuickrD integration, see

http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&res_title=IBM_Connections_Connector_for_Lotus_Quickr_ic40&content=pdcontent.

Suppose that you have Quickr Domino 8.5.1 installed.

Configuring SSO between Quickr Domino server and Connections

- ___ 1. Copy the LTPA key from Connections server to Quickr Domino server, for example, `c:\Connections.key`.
- ___ 2. Create a Web SSO document on the Quickr Domino Server:
 - ___ a. Start the Domino Administration Client. Select **File > Application > Open**, and enter the name of the Sametime Server.
 - ___ b. Open the `Names.nsf` database.
 - ___ c. Select **Configuration**, expand **Web**, and click **Web Configurations**. In there is the Web SSO token that Sametime automatically creates.
 - ___ d. Choose to edit the document. Click **Keys > Import WebSphere LTPA Keys**.
 - ___ e. Type the path and the name of the LTPA key file.
 - ___ f. Type the password. The key should be imported. Make sure that the Configuration Name field is `LtpaToken`.
 - ___ g. Enter the DNS domain to your domain name and then set the Map names in LTPA tokens field to `Disabled`.
 - ___ h. Add the Sametime server to the Domino Server Names list.

- ___ i. All the data in the WebSphere Information section will populate automatically after the WebSphere token is imported. You must change the Token format to "LtpaToken and LtpaToken2 (compatible with all releases of Domino)" so that all the community server features are available for user in the `stcenter.nsf`.

The screenshot shows a dialog box titled "Web SSO Configuration for : LtpaToken". It has tabs for "Basics", "Comments", and "Administration". The "Basics" tab is active and contains the following configuration details:

Token Configuration		Token Expiration	
Configuration Name:	LtpaToken	Expiration (minutes):	30
Organization:			
DNS Domain:	.cn.ibm.com		
Map names in LTPA tokens:	Disabled		
Require SSL protected communication (HTTPS):	Disabled		
Restrict use of the SSO token to HTTP/HTTPS:	Disabled		
Participating Servers			
Domino Server Names:	<Domino Server Names>		
Windows single sign-on integration (if available):	Disabled		
WebSphere Information			
Token Format:	LtpaToken and LtpaToken2 (compatible with all releases of Domino)		
LDAP Realm:	defaultWIMFileBasedRealm		
LTPA Version:	1.0		

Figure 229. Web SSO Configuration for: LtpaToken

- ___ j. Save the document.
- ___ k. Under **Configuration > Servers > All Server Documents**, select your Sametime server name and click **Edit server**.
- ___ l. Click the **Internet Protocol** tab and then the **Domino Web Engine** tab.
- ___ m. Change the Session authentication to Multiple Servers (SSO), and ensure that the Web SSO configuration field is set to LtpaToken.
- ___ n. Save the document and restart the server.



Note

With SSO configured, verify by first logging in to Connections and then switching to Lotus Quickr URL, and you are automatically logged in.

Installing Quickr Connector

1. Click `install.bat` under `\LC_Connectors_Quickr_Install_IM\IM\windows`.
2. On the Install Packages screen, click **Next**.

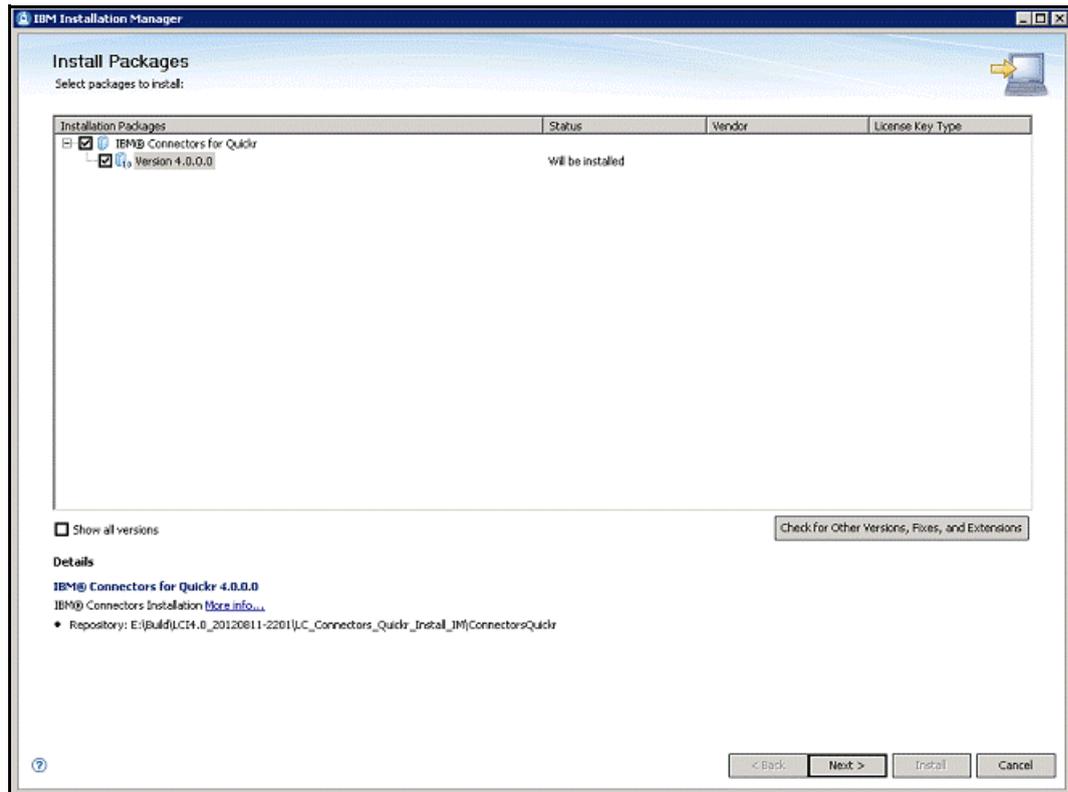


Figure 230. IBM Installation Manager: Install Packages

3. Accept the license agreement and click **Next**.

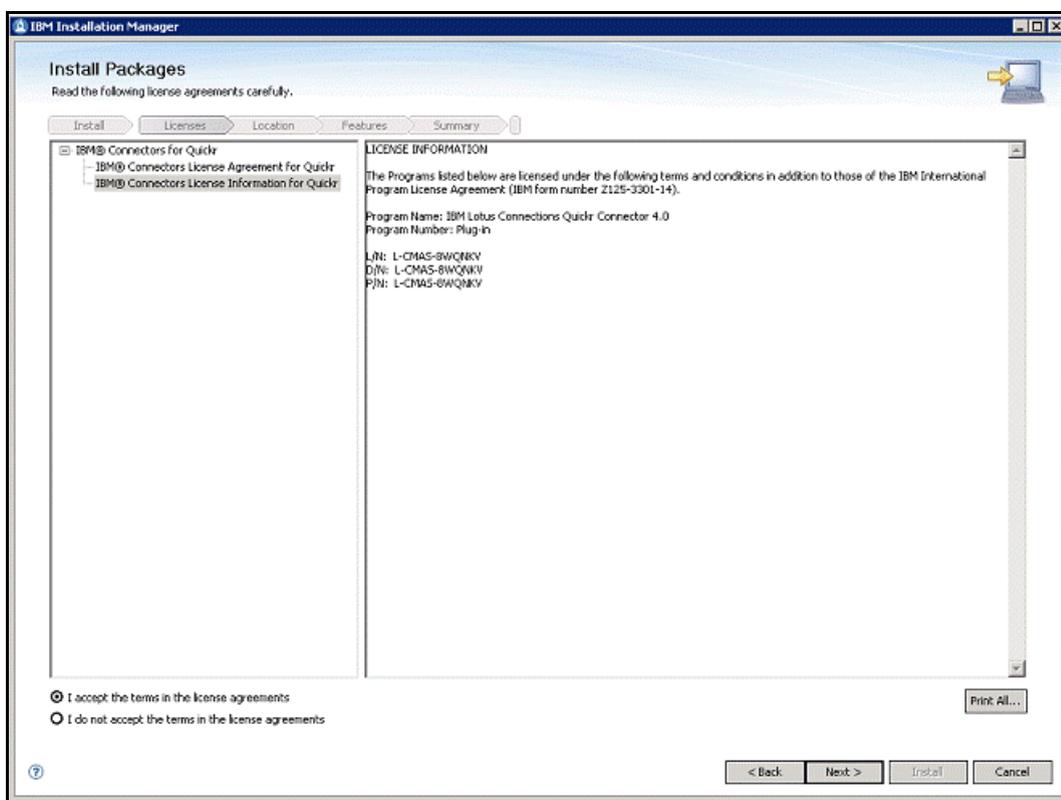


Figure 231. IBM Installation Manager: License agreement screen

4. Select the option "Create a new package group" and click **Next**.

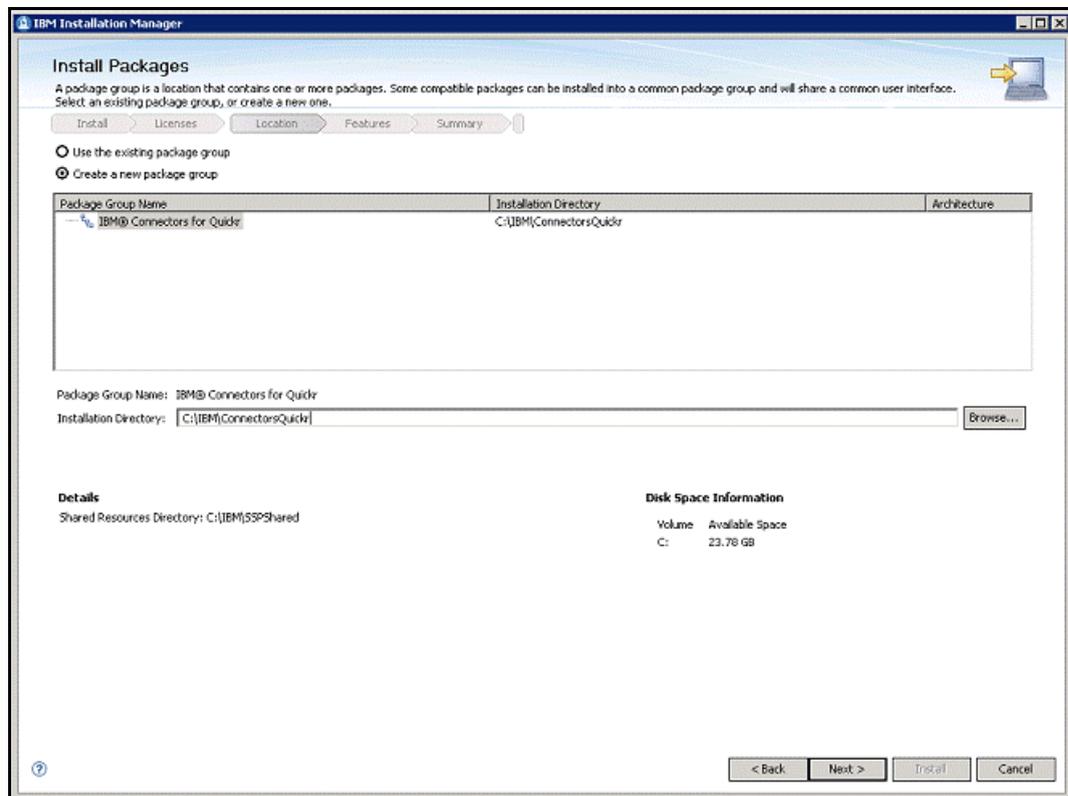


Figure 232. IBM Installation Manager: Creating a package group

5. If applicable, select the features to install and click **Next**.

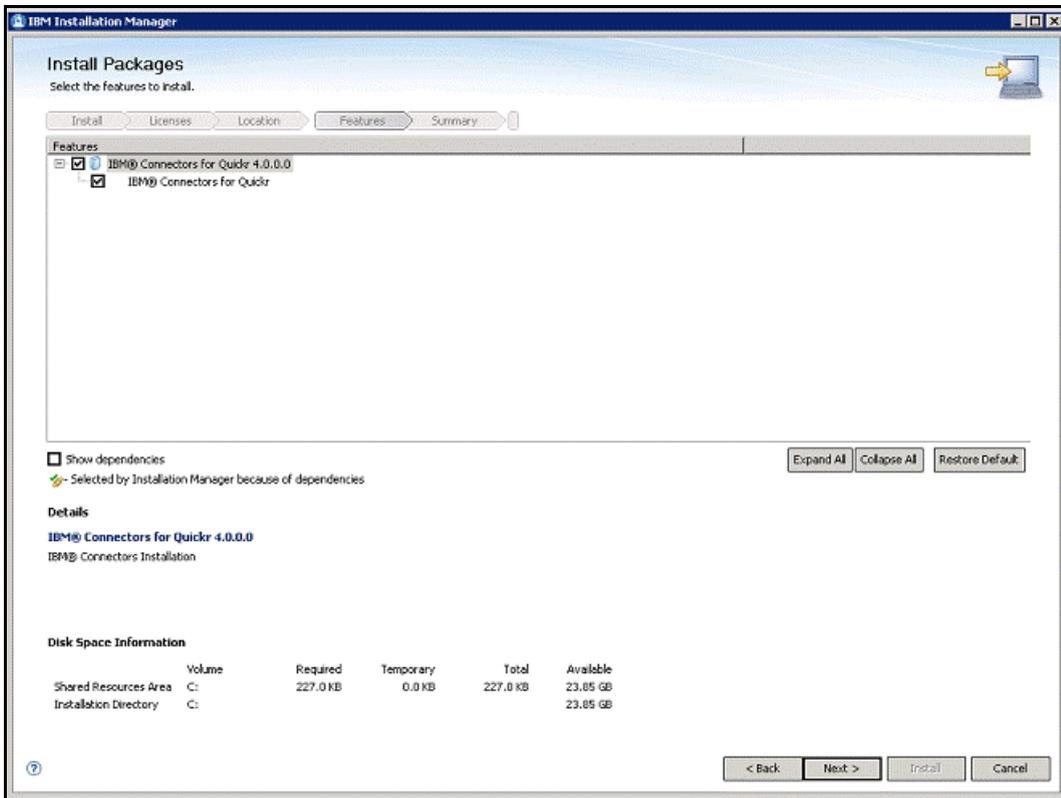


Figure 233. IBM Installation Manager: Features to install screen

6. Complete the configurations for the packages and click **Next**.

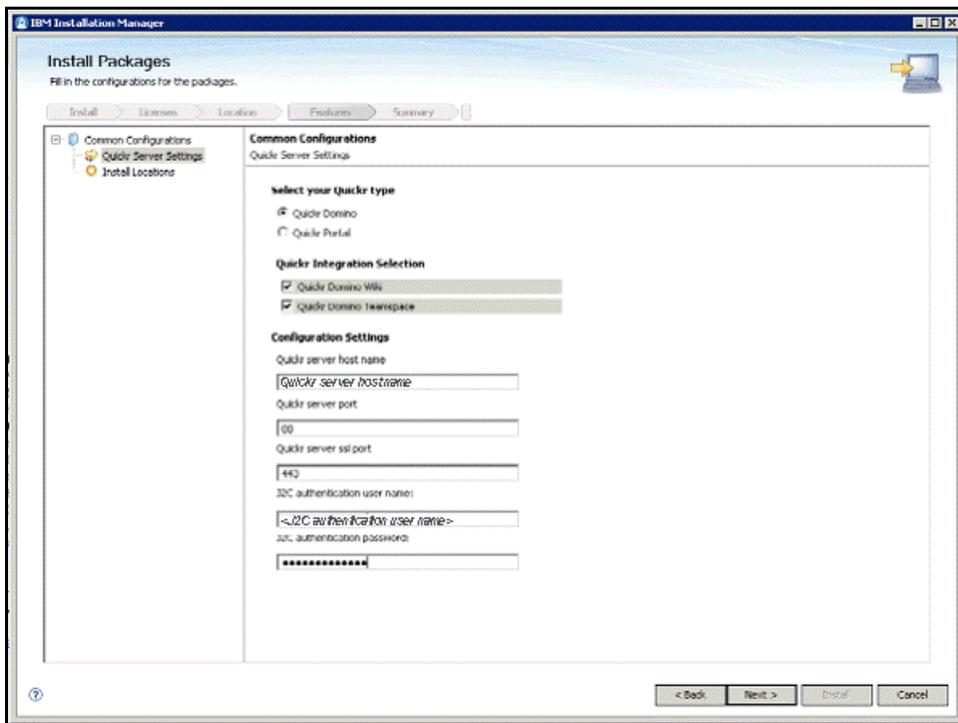


Figure 234. IBM Installation Manager: Configurations for the packages screen

- ___ 7. Select the installation locations for the packages and click **Next**.

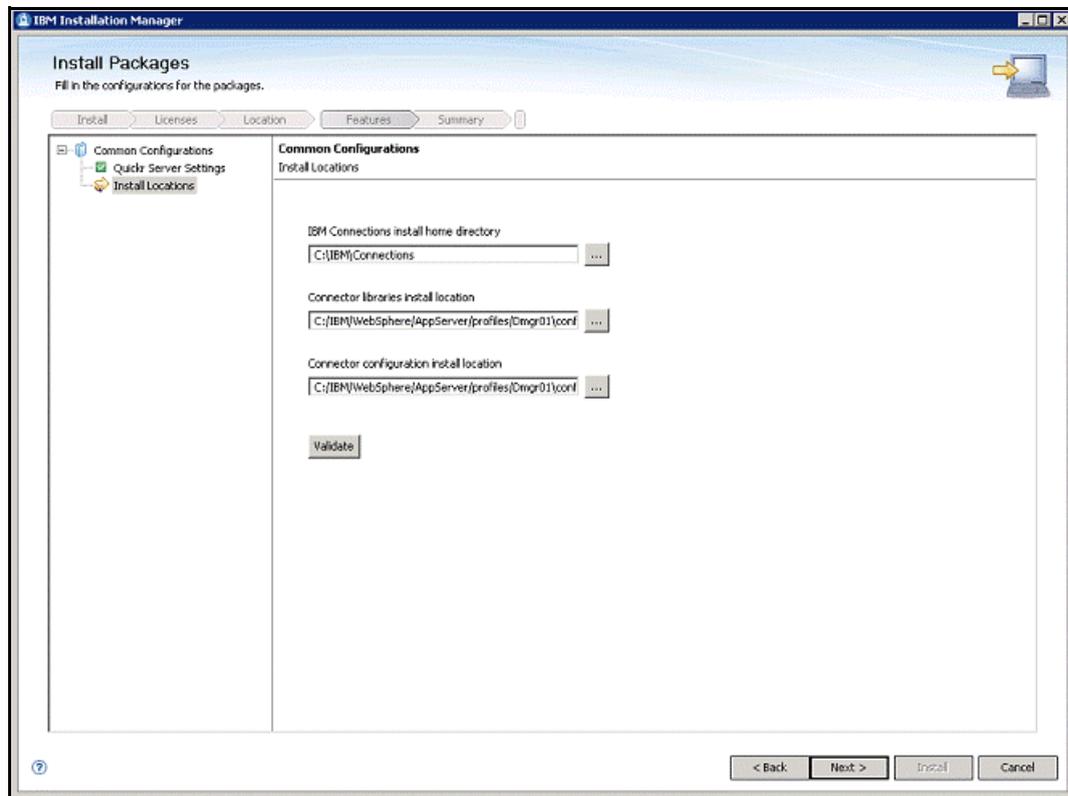


Figure 235. IBM Installation Manager: Install locations screen

8. Review the installation summary information and click **Install**.

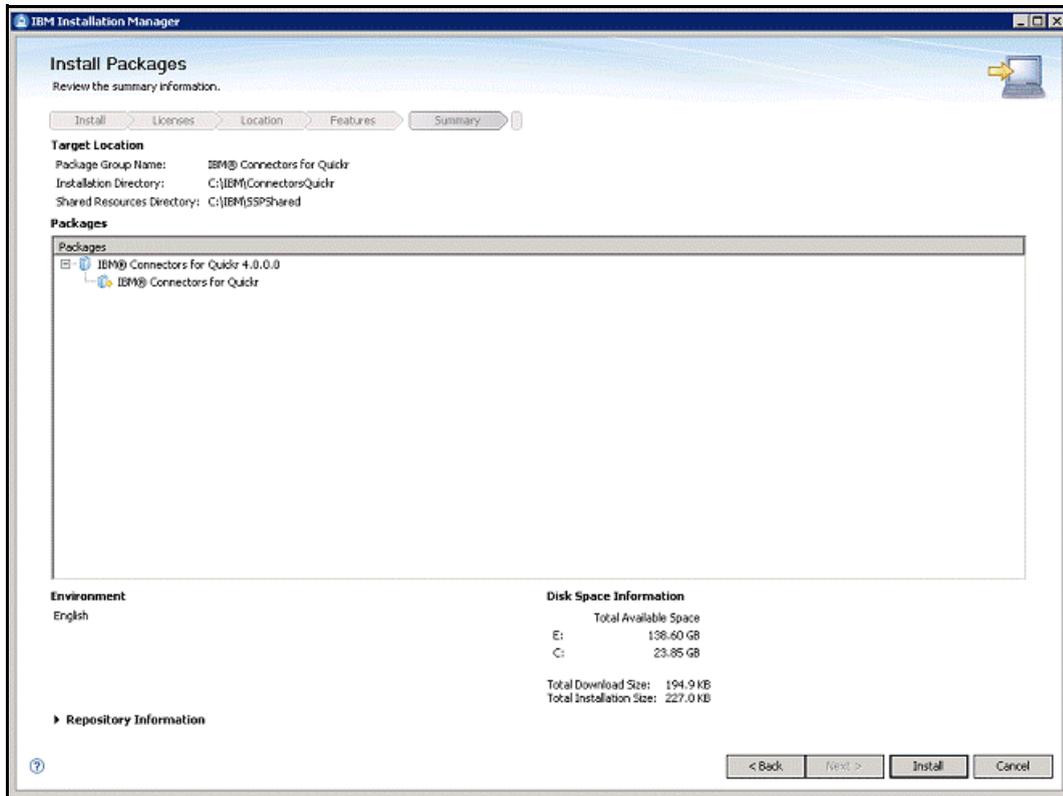


Figure 236. IBM Installation Manager: Install summary information screen

Configuring Quickr integration

Configuring oa-config.xml for Activities

- ___ 1. Open
C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\ConnectionsCell01\LotusConnections-config\oa-config.xml with your favorite editor.
- ___ 2. Change the Quickr integration section such as follows:


```
<PublishFile enabled="true" allowCustomServers="false" requireSSO="true">
  <server>http://quickr.example.com:80</server>
</PublishFile>
```

Adding Quickr server into white list

- ___ 1. Log in to Connections WebSphere Application Server console.
- ___ 2. Go to **Resources > Resource Environment > Resource Environment Providers** and click **QuickrWhitelistProvider**. Then, click **Custom properties** and click **New**.
- ___ 3. Input name as allowquickr.example.com and the value is quickr.example.com:

The screenshot shows the 'Custom properties' configuration page for the 'QuickrWhitelistProvider'. The breadcrumb path is 'Resource environment providers > QuickrWhitelistProvider > Custom properties > New'. A note states: 'Use this page to specify custom properties that your enterprise information system (EIS) requires for configure. For example, most database vendors require additional custom properties for data sources'. The 'Configuration' tab is active. Under 'General Properties', the 'Scope' is set to 'cells:icblade01:Cell01:clusters:Cluster1'. The 'Name' field contains '--Name--' and the 'Value' field contains '--value--'. The 'Description' field is empty. The 'Type' is set to 'java.lang.String'. At the bottom, there are buttons for 'Apply', 'OK', 'Reset', and 'Cancel'.

Figure 237. Resource environment providers > QuickWhitelistProvider > Custom properties

- ___ 4. Click **OK** and then **Save**.

Configuring proxy-config.tpl for Quickr integration

___ 1. Open

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\ConnectionsCell01\LotusConnections-config\proxy-config.tpl with your favorite editor.

___ 2. Add a section for Quickr integration as follows:

```
<proxy:policy url="http://quickr.example.com:80/*" acf="none">
  <proxy:actions>
    <proxy:method>GET</proxy:method>
  </proxy:actions>
  <proxy:headers>
<proxy:header>User-Agent</proxy:header>
    <proxy:header>Accept*</proxy:header>
    <proxy:header>Content*</proxy:header>
    <proxy:header>Authorization*</proxy:header>
  </proxy:headers>
  <proxy:cookies>
    <proxy:cookie>JSESSIONID</proxy:cookie>
    <proxy:cookie>LtpaToken</proxy:cookie>
    <proxy:cookie>LtpaToken2</proxy:cookie>
  </proxy:cookies>
</proxy:policy>
```

___ 3. Sync all nodes and restart servers.

Domino SSO integration with Connections

Suppose that you have a Domino 8.5.2 server installed.

Configure SSO between Domino server and Connections

- ___ 4. Copy the LTPA key from Connections server to Quickr Domino server, for example, `c:\Connections.key`.
- ___ 5. Create a Web SSO document on the Domino Server:
 - ___ a. Start the Domino Administration Client. Select **File > Application > Open**, and enter the name of the Sametime Server.
 - ___ b. Open the `Names.nsf` database.
 - ___ c. Select **Configuration**, expand **Web**, and click **Web Configurations**. In there is the Web SSO token that Sametime automatically creates.
 - ___ d. Choose to edit the document. Click **Keys > Import WebSphere LTPA Keys**.
 - ___ e. Type the path and the name of the LTPA key file.
 - ___ f. Type the password. The key should be imported. Make sure that the Configuration Name field is `LtpaToken`.
 - ___ g. Enter the DNS domain to your domain name and then set the Map names in LTPA tokens field to `Disabled`.
 - ___ h. Add the Sametime server to the Domino Server Names list.

- ___ i. All the data in the WebSphere Information section will populate automatically after the WebSphere token is imported. You must change the Token format to "LtpaToken and LtpaToken2 (compatible with all releases of Domino)" so that all the community server features are available for user in the `stcenter.nsf`.

Token Configuration		Token Expiration	
Configuration Name:	LtpaToken	Expiration (minutes):	30
Organization:			
DNS Domain:	.cn.ibm.com		
Map names in LTPA tokens:	Enabled		
Require SSL protected communication (HTTPS):	Disabled		
Restrict use of the SSO token to HTTP/HTTPS:	Disabled		
Participating Servers			
Domino Server Names:	<Domino Server Names>		
Windows single sign-on integration (if available):	Disabled		
WebSphere Information			
Token Format:	LtpaToken2 (incompatible with Domino 7 and prior releases, but provides SSO security improvements)		
LDAP Realm:	defaultWIMFileBasedRealm		
LTPA Version:	1.0		

Figure 238. Web SSO Configuration for: LtpaToken

- ___ j. Save the document.
- ___ k. Under **Configuration > Servers > All Server Documents**, select your Sametime server name and click **Edit server**.
- ___ l. Click the **Internet Protocol** tab and then the **Domino Web Engine** tab.
- ___ m. Change the Session authentication to Multiple Servers (SSO), and ensure that the Web SSO configuration field is set to LtpaToken.
- ___ n. Save the document and restart the server.



Note

With SSO configured, verify by first logging in to Connections and then switching to Domino web server URL, and you are automatically logged in.

Configuring Domino SSO on Notes client

- ___ 1. Open a Notes client and connect it to the Domino server with SSO for Connections.
- ___ 2. In Activities sidebar preference, input the Connections URL protected by Tivoli Access Manager.
- ___ 3. In advanced dialog, select **Domino SSO** as authentication type and input Domino mail server host as **Domino SSO server**:

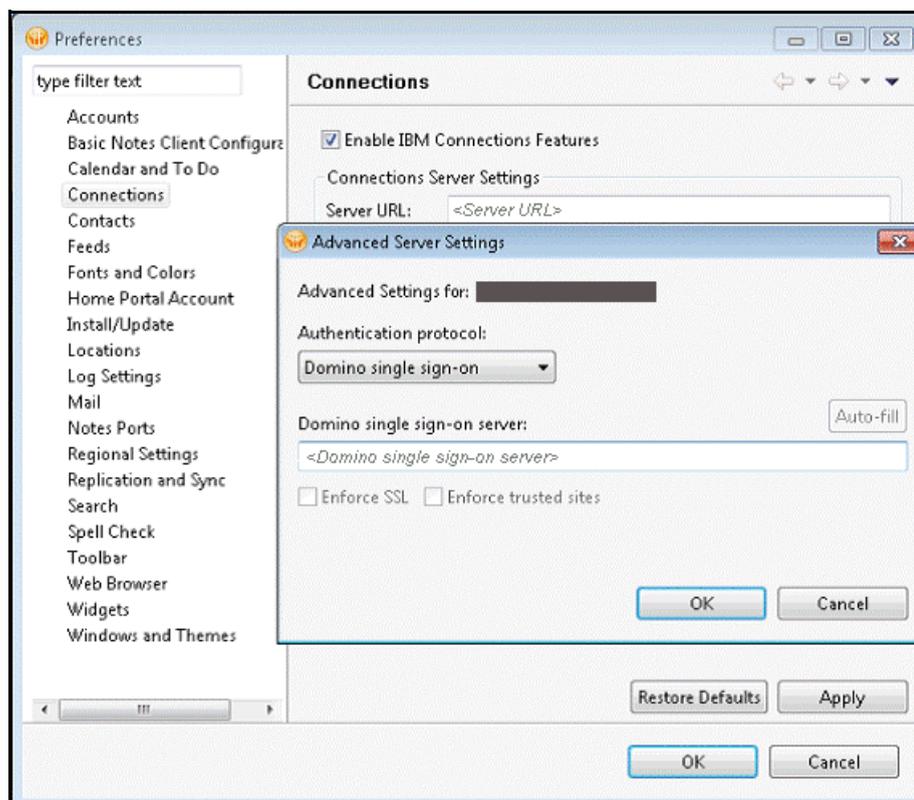


Figure 239. Connections: Advanced Server Settings

- ___ 4. Save your changes and verify that you are automatically logged in to Connections from sidebar without input password.

