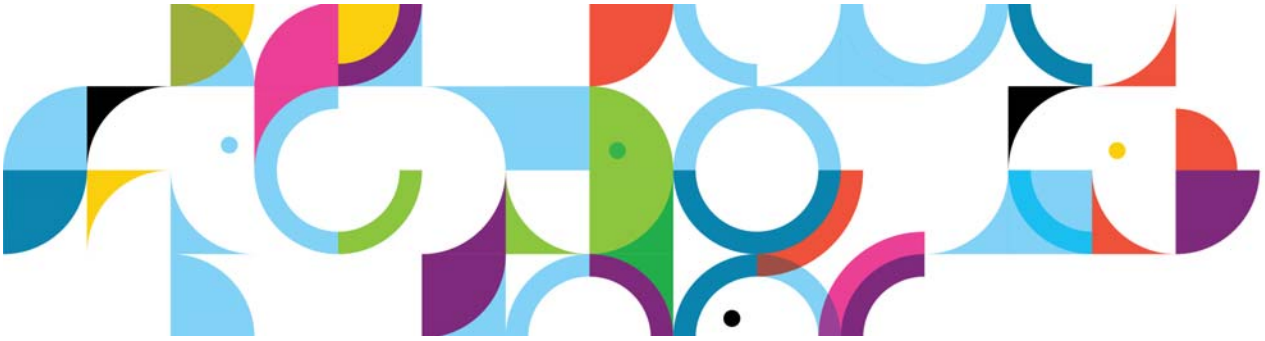
IBM Connections 4 Public Deployment Scenarios

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

IBM Connections 4: PDS Tivoli Access Manager configuration

About the author

Devon Clark comes from the Connections System Verification Test (SVT) Team in Dublin and has two years' experience working on Connections with four years' experience testing Lotus Notes & Domino and IBM Quickr-Domino overall. The author is also familiar with integrating other IBM portfolios with Connections such as Quickr-Domino, Sametime, and Microsoft SharePoint, with third-party security systems, Tivoli Access Manager, and CA SiteMinder products. His involvement includes from conception to installation, configuration, administration of infrastructure, and troubleshooting to any issues that might arise. Devon can be reached at `clarkdev@ie.ibm.com`.

Overview

This scenario explains how to deploy IBM® Connections 4.0 in a network deployment that involves multiple computers with one IBM WebSphere® cell that contains two nodes, both of which host IBM® Connections 4.0. This scenario is typical of an enterprise-level production deployment. This article is an end-to-end guide to deploying this type of configuration with all prerequisites. You can also follow this guide in situations in which more than two nodes are being deployed.

Table 1: Computers in scenario

Host name	Applications	Version number	OS version	RAM / CPU	HW or VM
Deployment Manager + IHS.mycompany.com	Deployment Manager + HTTP	7.0.0.21	Windows 2008 R2 Enterprise Server 64-bit	4 GB / 2 x CPU	VM
Node 1.mycompany.com	Node 1	7.0.0.21	Windows 2008 R2 Enterprise Server 64-bit	4 GB / 2 x CPU	VM
Node 2.mycompany.com	Node 2	7.0.0.21	Windows 2008 R2 Enterprise Server 64-bit	4 GB / 2 x CPU	VM
DB Server+TDI.mycompany.com	MS-SQL + Tivoli Directory Integrator	MS-SQL 2008 + Tivoli Directory Integrator 7.1 FP5	Windows 2008 R2 Enterprise Server 64-bit	4 GB / 2 x CPU	VM
LDAP.mycompany.com	IBM Tivoli Directory Server	Tivoli Directory Server 6.3	Windows 2008 R2 Enterprise Server	4 GB / 2 x CPU	VM
QRD.mycompany.com	Quickr Domino	8.5.1 FP5	Windows 2003 SP2 Server	4 GB / 2 x CPU	VM
Sametime-SSC+DB2.mycompany.com	Sametime System Console	8.5.2 IFR1 + DB2 v9.7	RedHat 6 Linux 64-bit	4 GB / 2 x CPU	VM

Table 1: Computers in scenario

Host name	Applications	Version number	OS version	RAM / CPU	HW or VM
Sametime-SC+Domino.mycompany.com	Sametime Community + Domino Server	8.5.2 IFR1	RedHat 6 Linux 64-bit	4 GB / 2 x CPU	VM
Sametime-SP.mycompany.com	Sametime Proxy Server	8.5.2 IFR1	RedHat 6 Linux 64-bit	4 GB / 2 x CPU	VM
SharePoint.mycompany.com	SharePoint Server	SharePoint 2010	Windows 2008 SP1 Enterprise Server	4 GB / 2 x CPU	VM

- **SSC:** Sametime System Console
- **SC:** Sametime Community Server
- **SP:** Sametime Proxy Server

Scenario description

This scenario is designed as an end-to-end guide to deploying IBM Connections 4.0 in a network environment with two nodes. Full system specifications and a list of software that is used in this configuration are outlined in the environment Hardware and Software specifications topic in this article. The following properties describe the environment in more detail:

- **Operating system**

  Microsoft® Windows® Server 2008 Enterprise Edition x86-64 Bit.

- **Database server**

  Microsoft® SQL Server 2008 R2.

- **User directory**

  IBM Tivoli® Directory Server v7.1.

- **Supported plug-ins**

  All plug-ins are supported in this environment.

- **Secure sockets layer (SSL)**

  SSL is enabled on this deployment for all communication.

- **Third-Party Security**

  Tivoli Access Manager: Tivoli Access Manager v6.x.

- **Other product integrations**

  This scenario describes integration with IBM Quickr Domino® Server 8.5.3, IBM Lotus Sametime®, 8.5.2, SharePoint 2010 Server, and SharePoint plug-in.

Contents

1. Installing WebSphere Deployment Manager and Application Server v7.0.0.0

Deployment Manager

__ 1. On `dm.example.com`, extract the downloaded file into a directory on your hard disk. Go to that directory and run `launchpad.exe`. The following panel is displayed. Click **Launch the installation wizard for WebSphere Application Server Network Deployment** to continue.

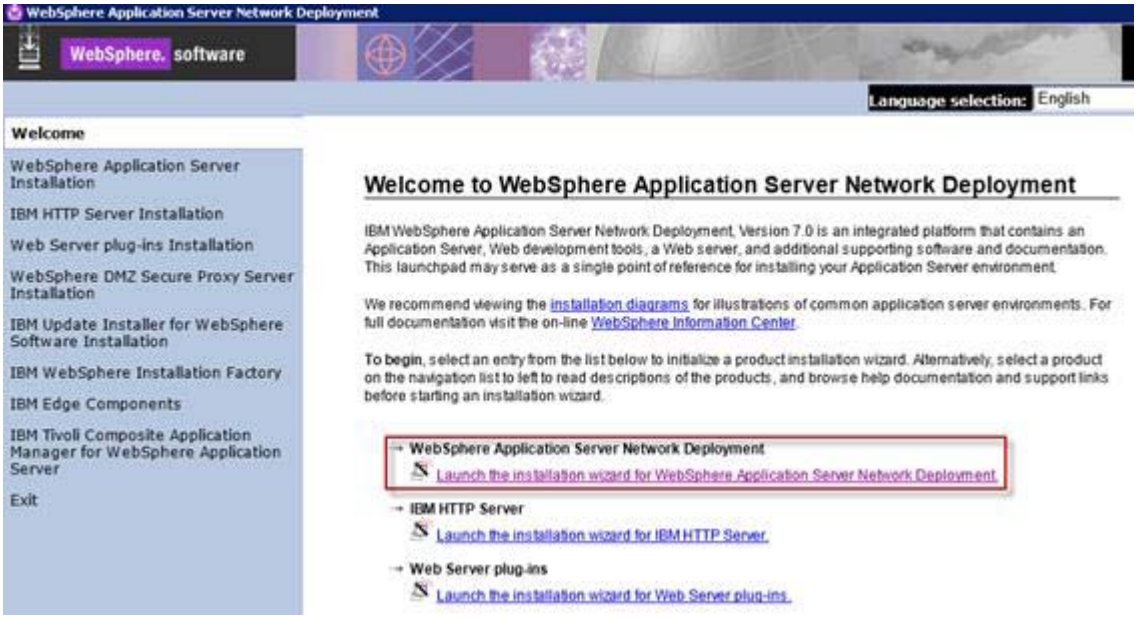


Figure 1. WebSphere Application Server Network Deployment: Welcome

__ 2. Click **Next** to continue.

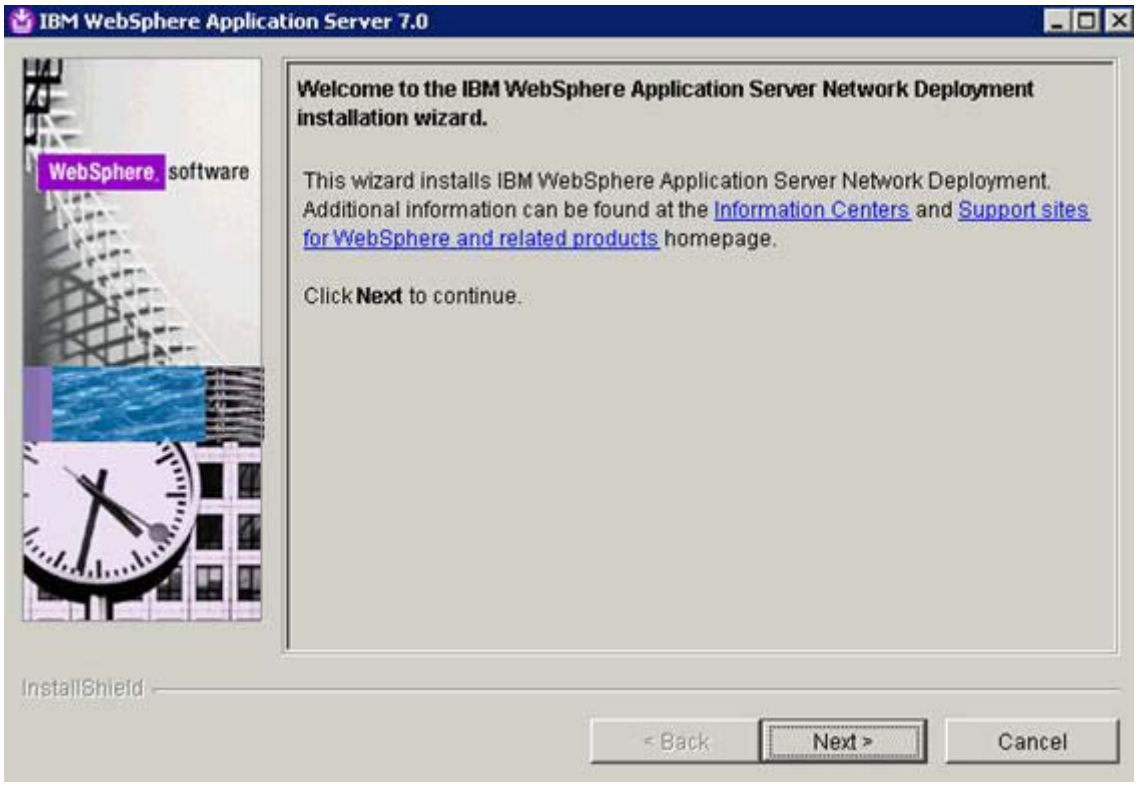


Figure 2. IBM WebSphere Application Server 7.0: Welcome

__ 3. Accept the IBM terms and click **Next** to continue.

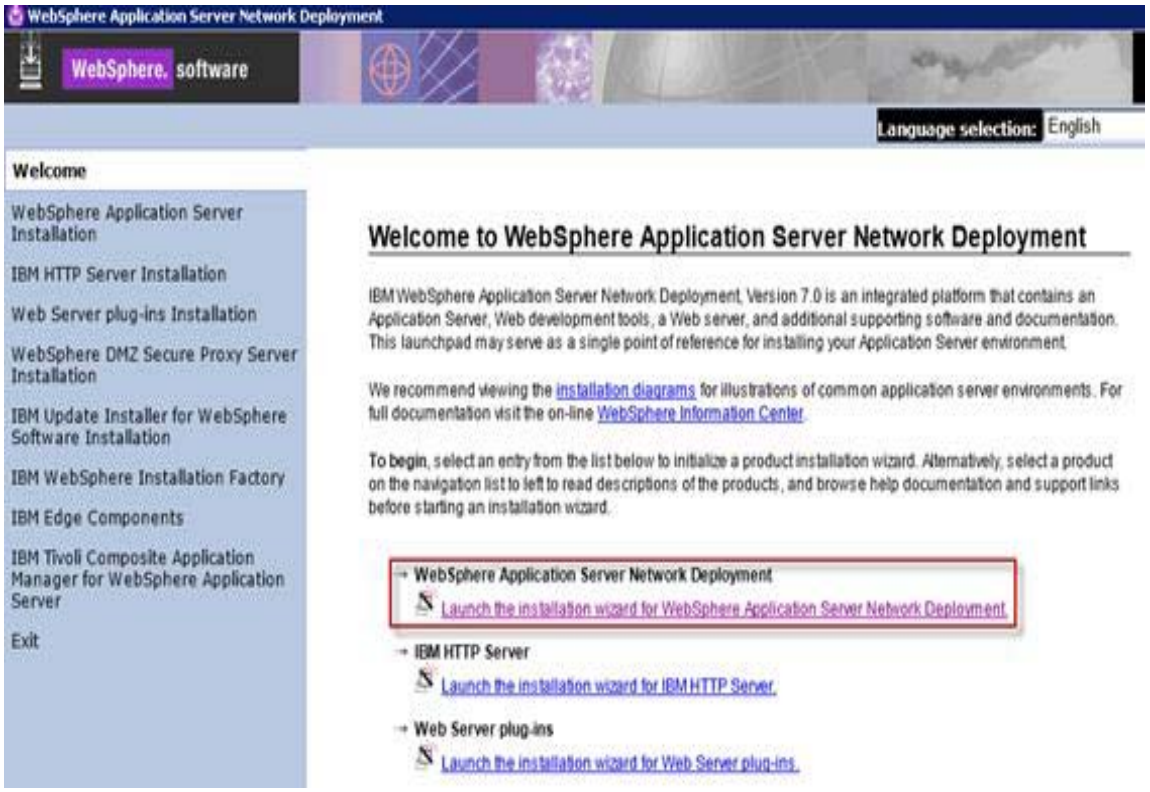


Figure 3. WebSphere Application Server Network Deployment: Software License Agreement

__ 4. Click **Next** to continue when the prerequisite checks are passed.

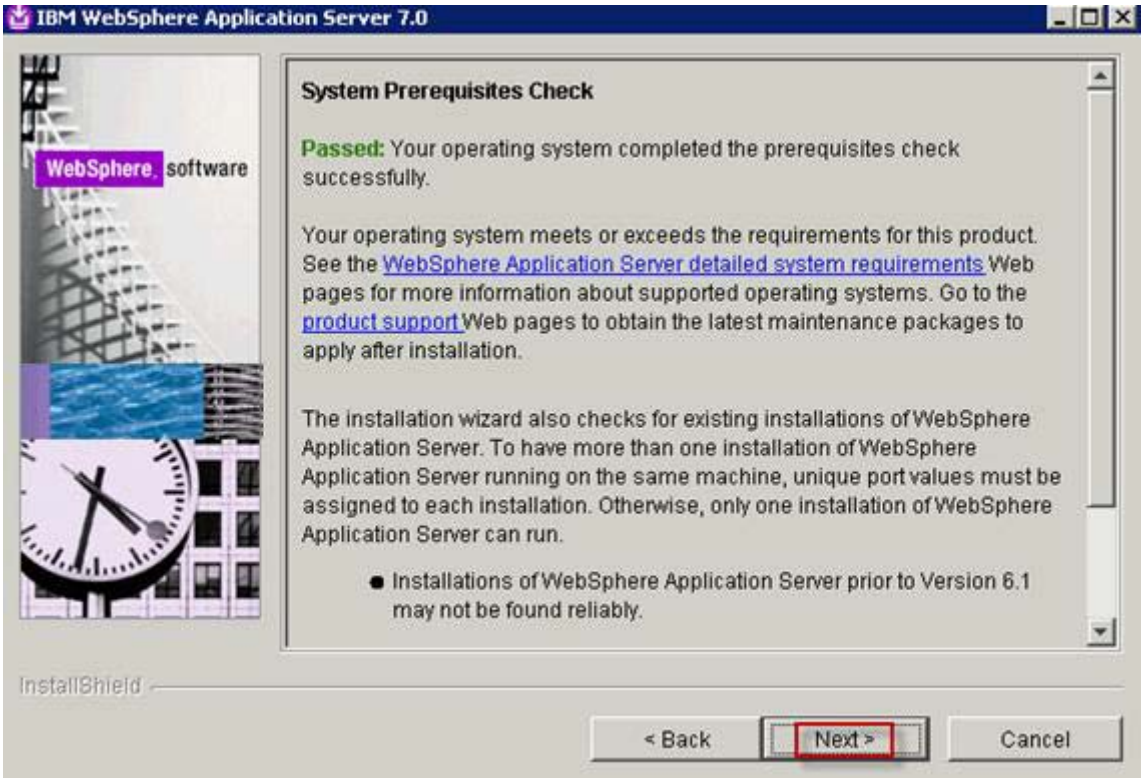


Figure 4. WebSphere Application Server Network Deployment: System Prerequisites Check

__ 5. Accept the defaults and click **Next** to continue.

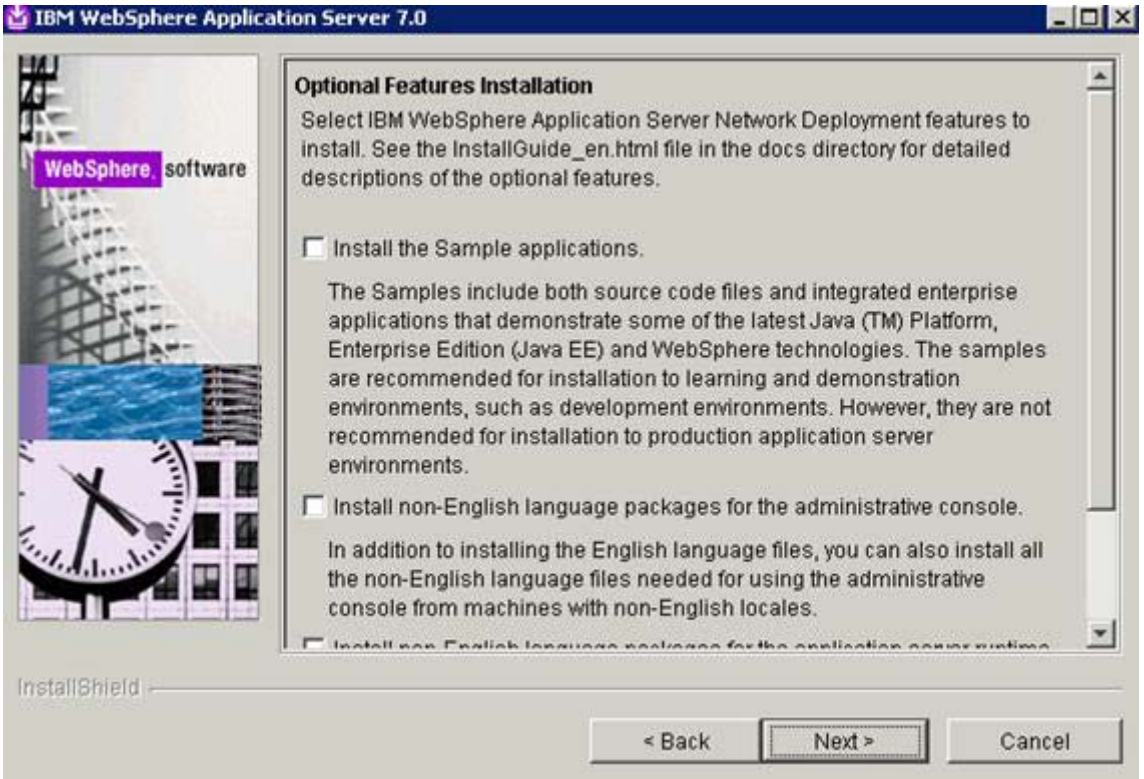


Figure 5. WebSphere Application Server Network Deployment: Optional Features Installation

__ 6. Select the installation directory and click **Next** to continue.

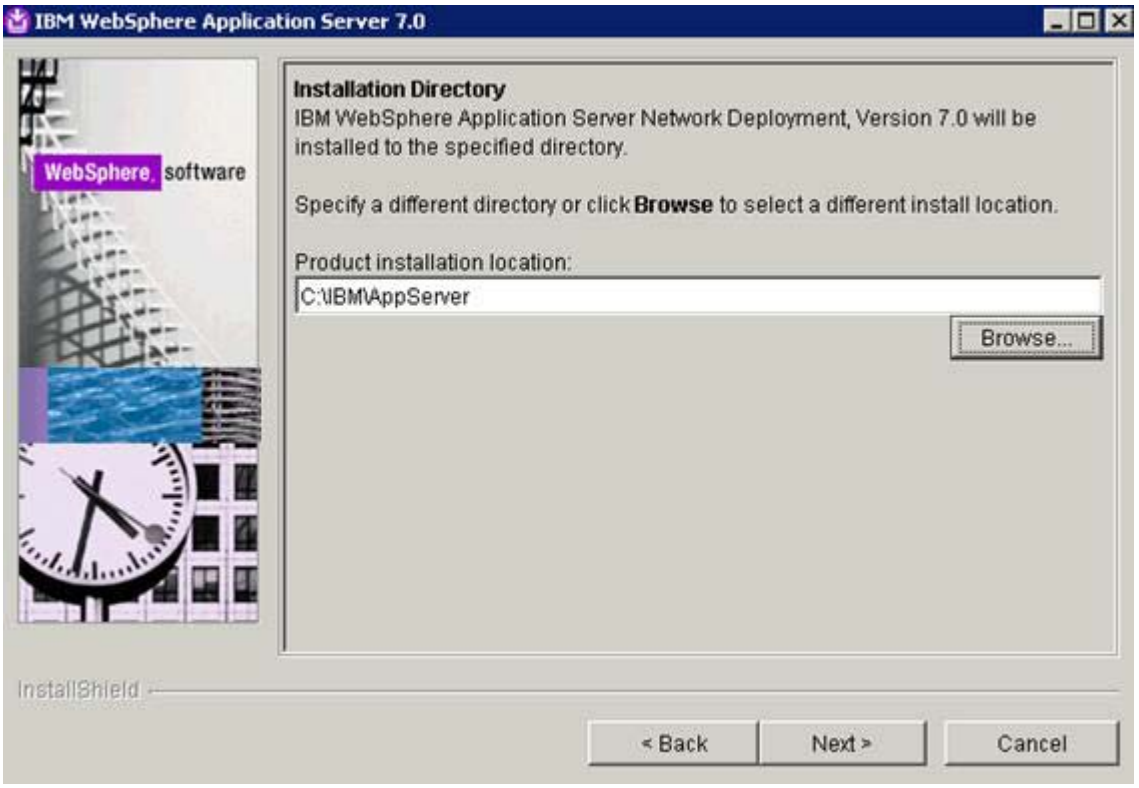


Figure 6. WebSphere Application Server Network Deployment: Installation Directory

__ 7. Select **Management** and click **Next** to continue.

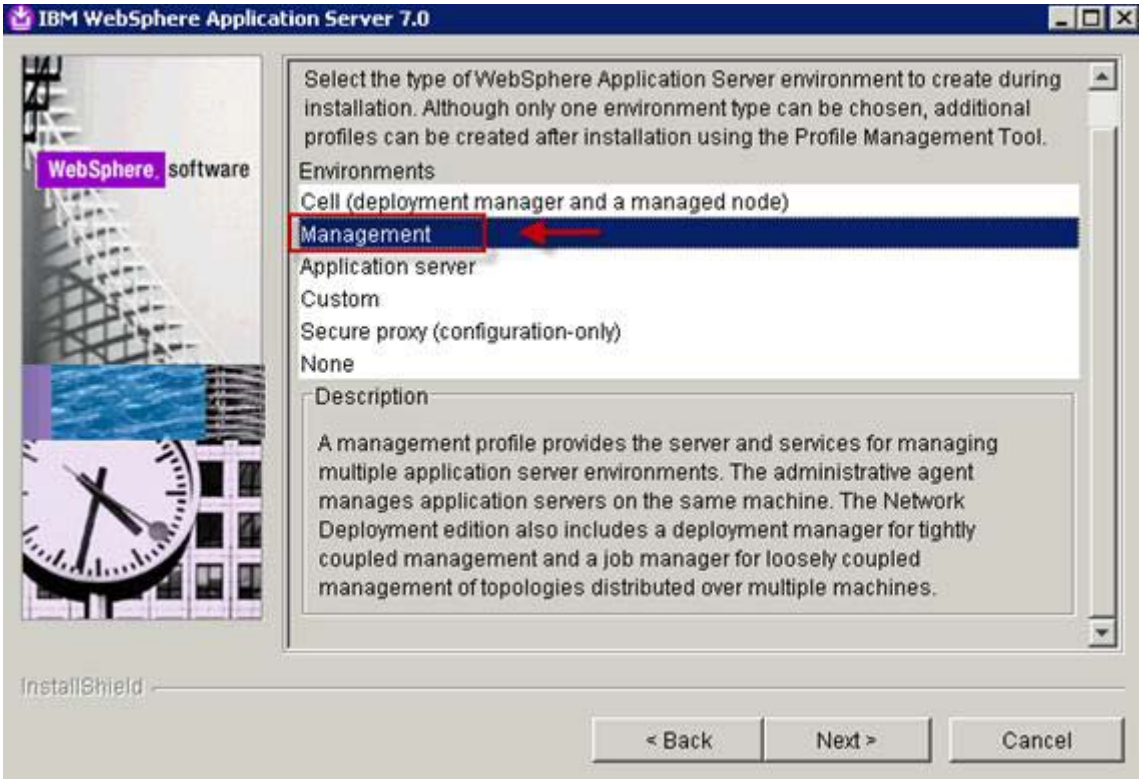


Figure 7. WebSphere Application Server Network Deployment: Environments

__ 8. Select **Deployment manager** and click **Next** to continue.

Figure 8. WebSphere Application Server Network Deployment: Server Type Selection

__ 9. Select **Enable administrative security** and enter the user name and password of the Admin user, and then click **Next** to continue.

Figure 9. WebSphere Application Server Network Deployment: Enable Administrative Security

__ 10. Click **Next** to continue.

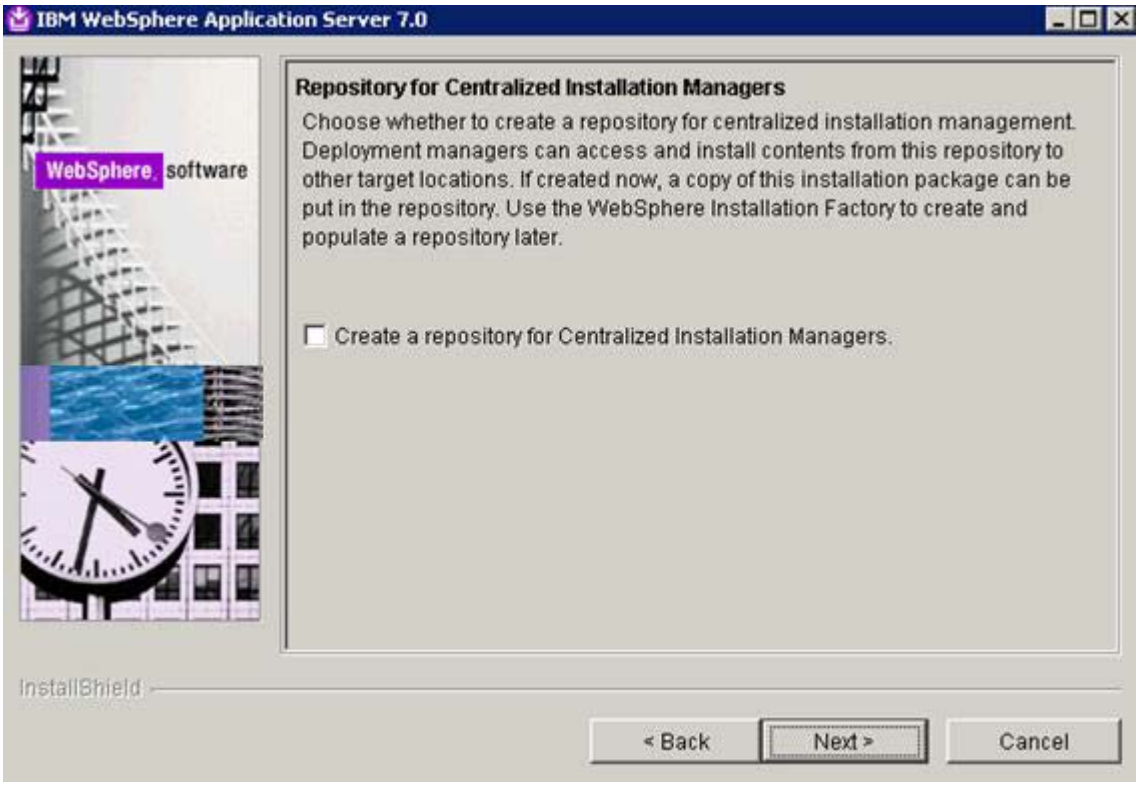


Figure 10. WebSphere Application Server Network Deployment: Repository for Centralized Installation Managers

__ 11. Click **Next** to continue after reviewing the installation summary screen.

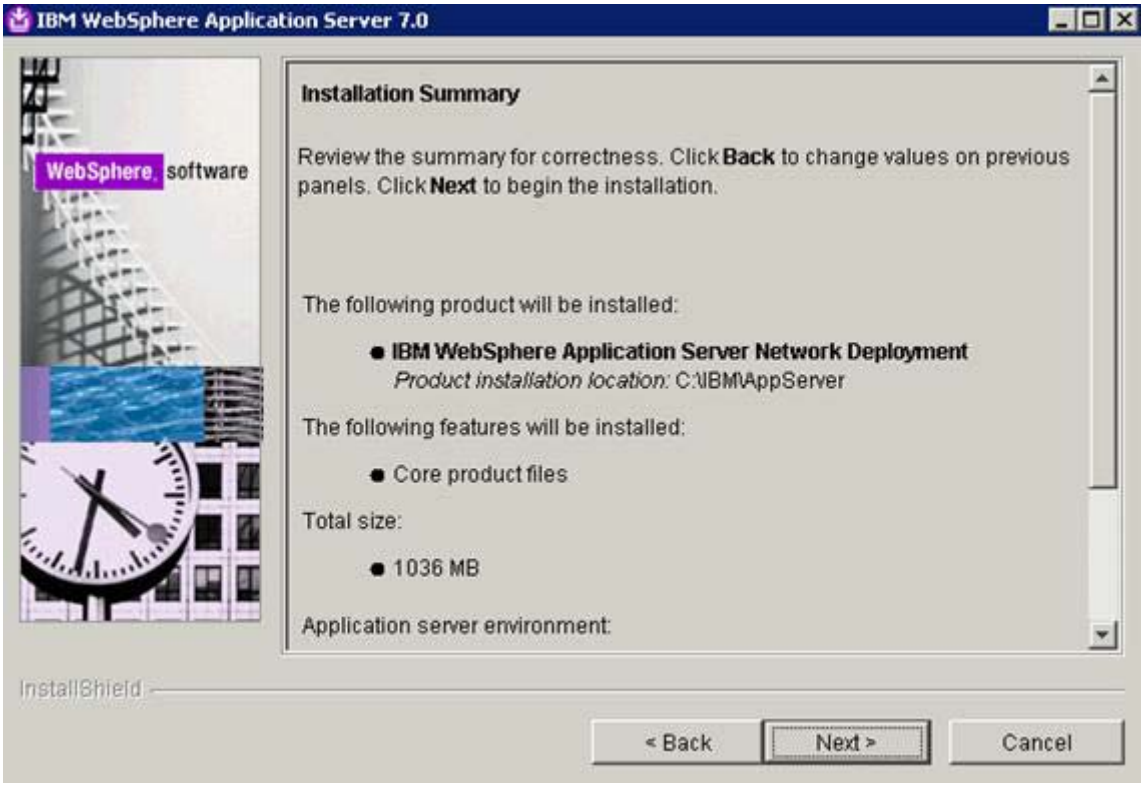


Figure 11. WebSphere Application Server Network Deployment: Installation Summary

The component installation starts.

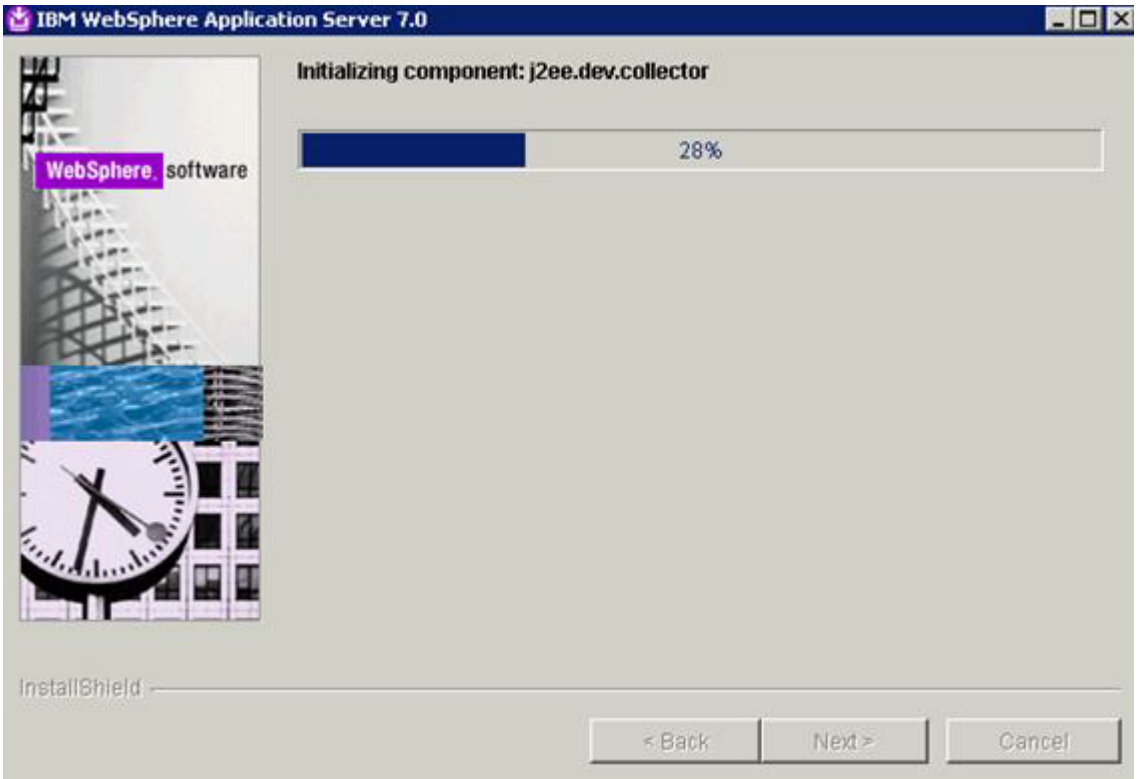


Figure 12. WebSphere Application Server Network Deployment: Installation in progress

__ 12. Click **Finish** to complete installation.

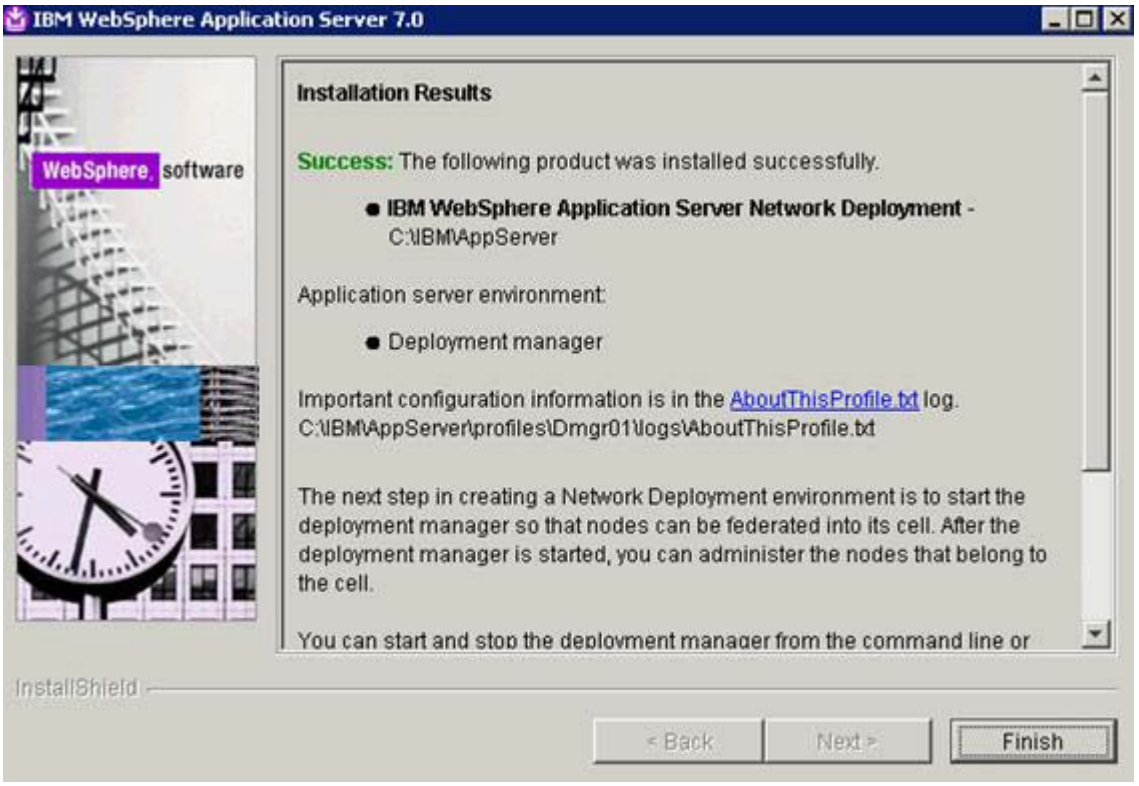


Figure 13. WebSphere Application Server Network Deployment: Installation results

__ 13. Click **Installation verification** to verify that the installation completed successfully.

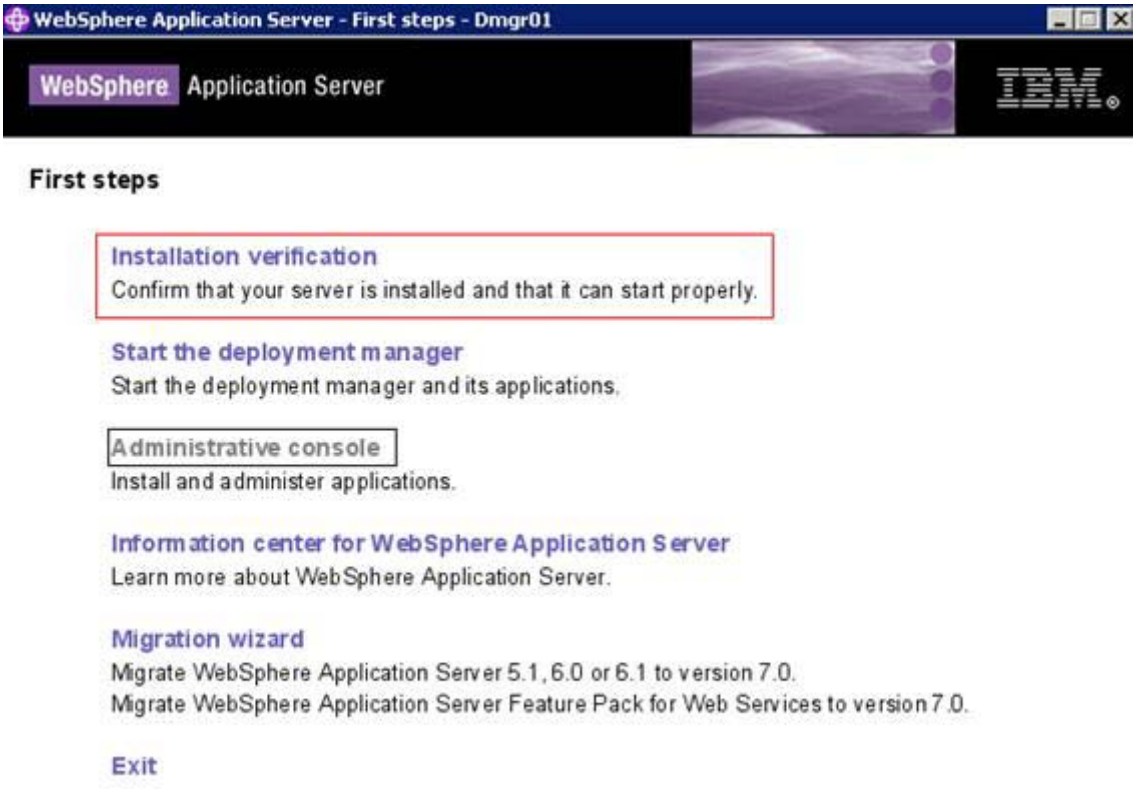


Figure 14. WebSphere Application Server 7.0: Verification

__ 14. A confirmation of successful installation is displayed.

Figure 15. WebSphere Application Server 7.0: Successful installation

Application Server

__ 1. Repeat the same steps as previously on `node1.example.com` and `node2.example.com`, choosing **Application Server** instead of **Management** in the panel. Click **Next** to continue.

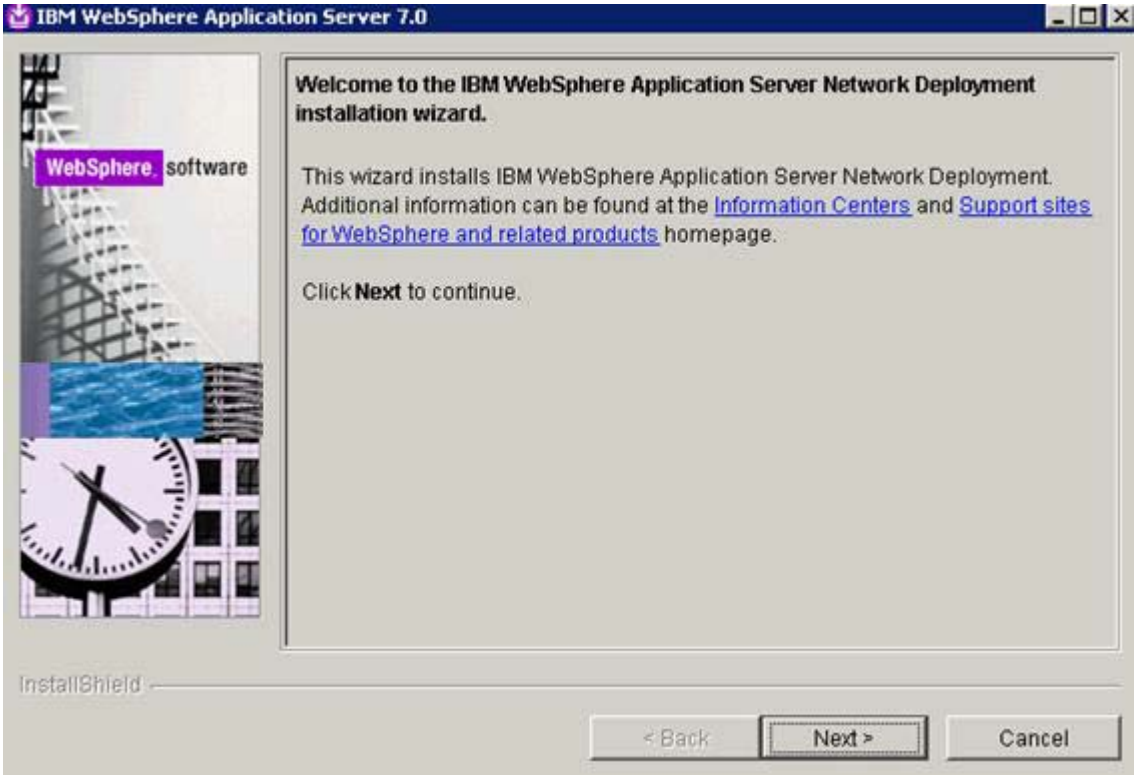


Figure 16. IBM WebSphere Application Server 7.0: Welcome

__ 2. Accept the IBM terms and click **Next** to continue.

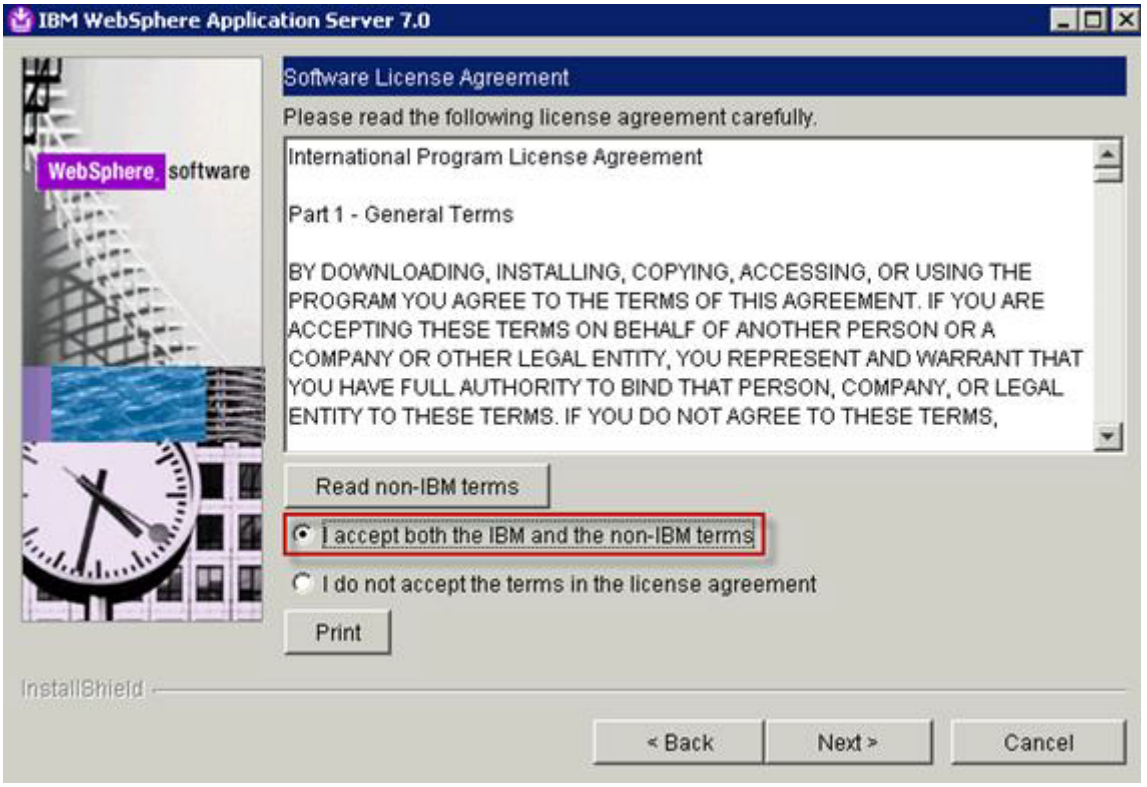


Figure 17. IBM WebSphere Application Server 7.0: Software License Agreement

__ 3. Click **Next** to continue when the prerequisite checks are passed.

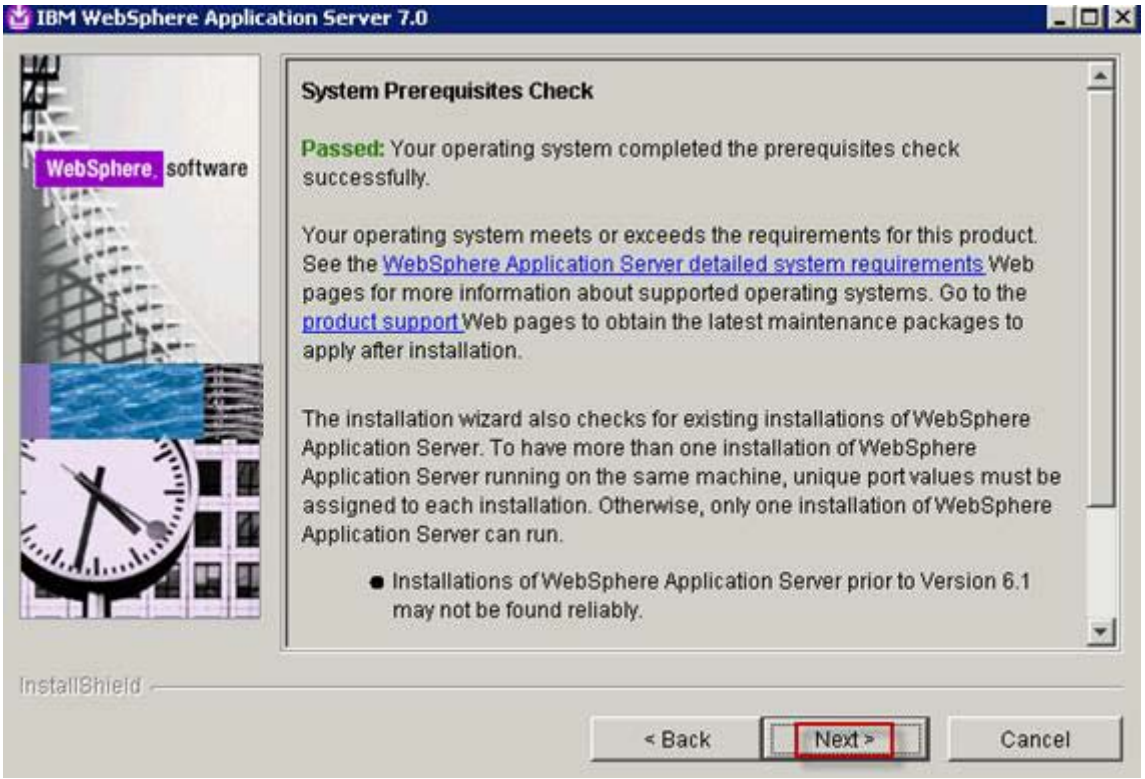


Figure 18. IBM WebSphere Application Server 7.0: System Prerequisites Check

__ 4. Click **Next** to continue.

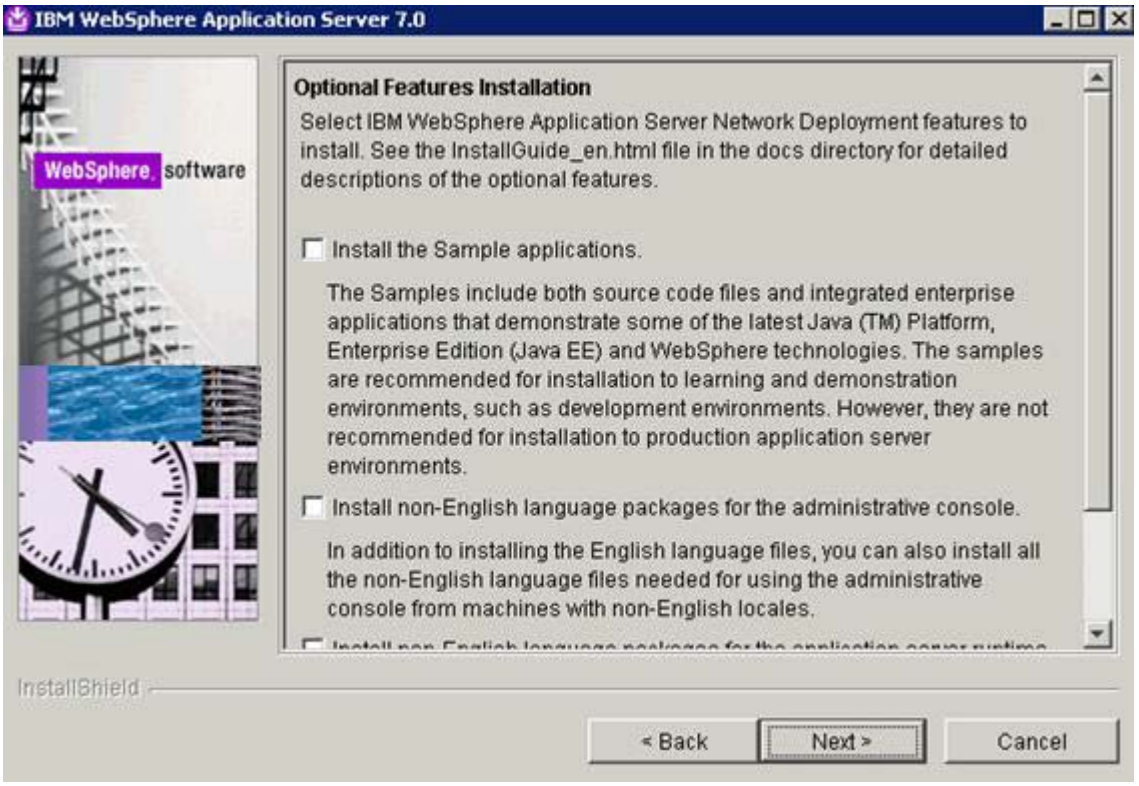


Figure 19. IBM WebSphere Application Server 7.0: Optional Features Installation

__ 5. Select the installation directory and click **Next** to continue.

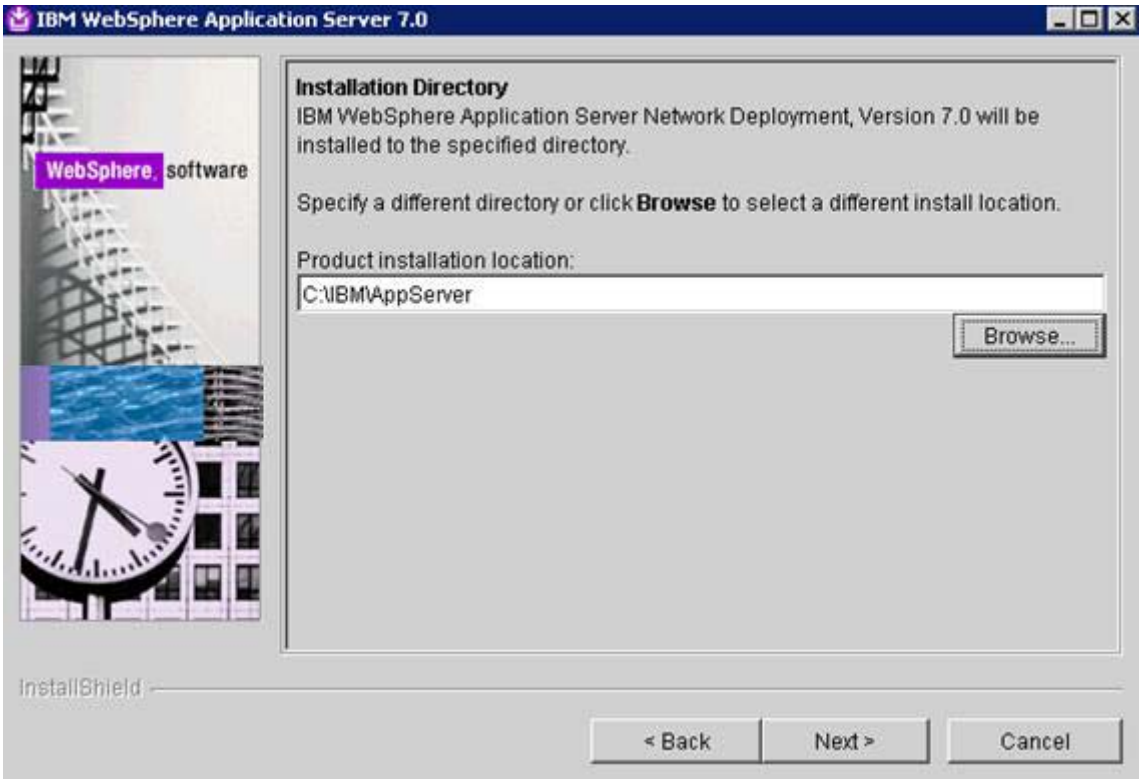


Figure 20. IBM WebSphere Application Server 7.0: Installation Directory

__ 6. Select **Application server** and click **Next** to continue.

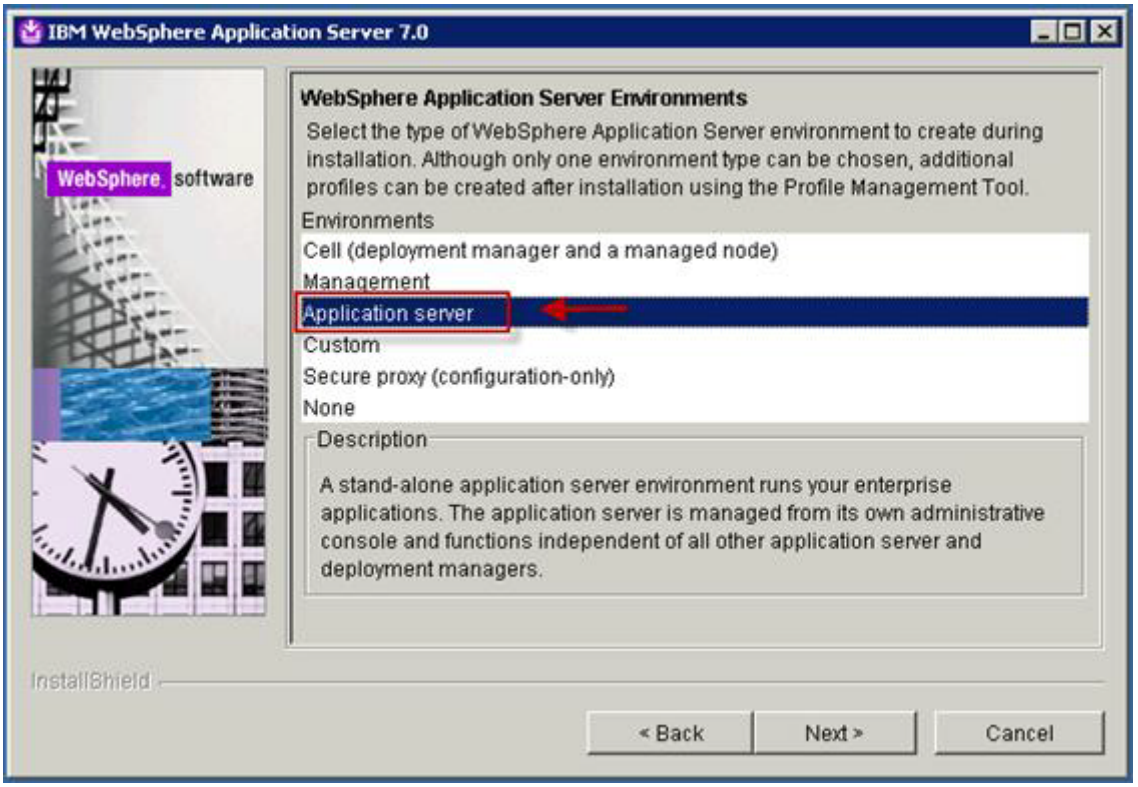


Figure 21. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments

__ 7. Select **Enable administrative security** and enter the user name and password of the Admin user, and then click **Next** to continue.

Figure 22. IBM WebSphere Application Server 7.0: Enable Administrative Security

__ 8. Click **Next** to continue after reviewing the installation summary screen.

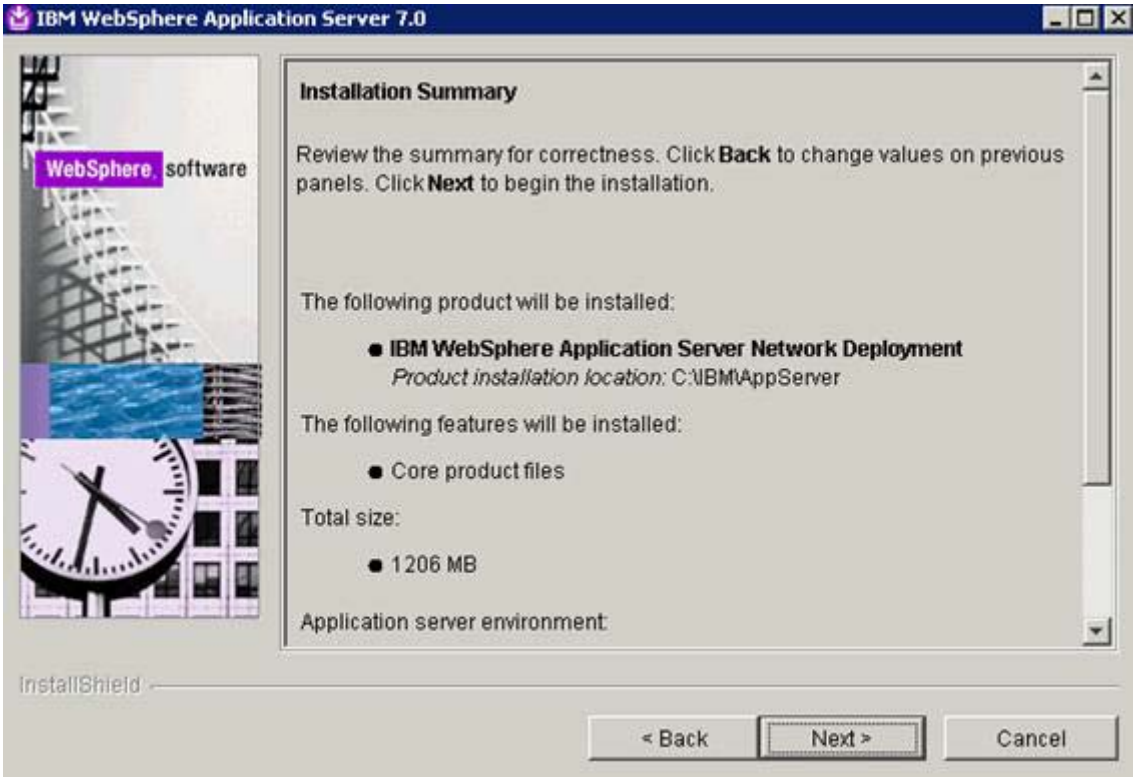


Figure 23. IBM WebSphere Application Server 7.0: Installation Summary

The component starts to install.

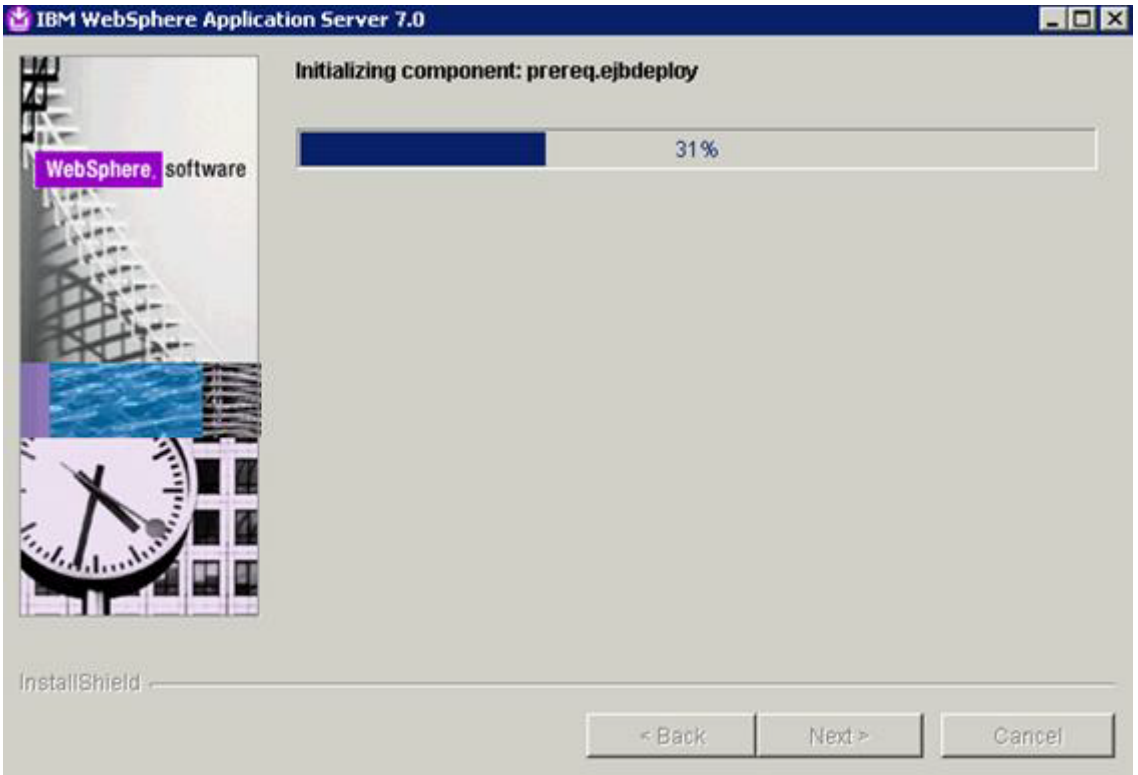


Figure 24. IBM WebSphere Application Server 7.0: Component installation in progress

__ 9. Click **Finish** to complete install.

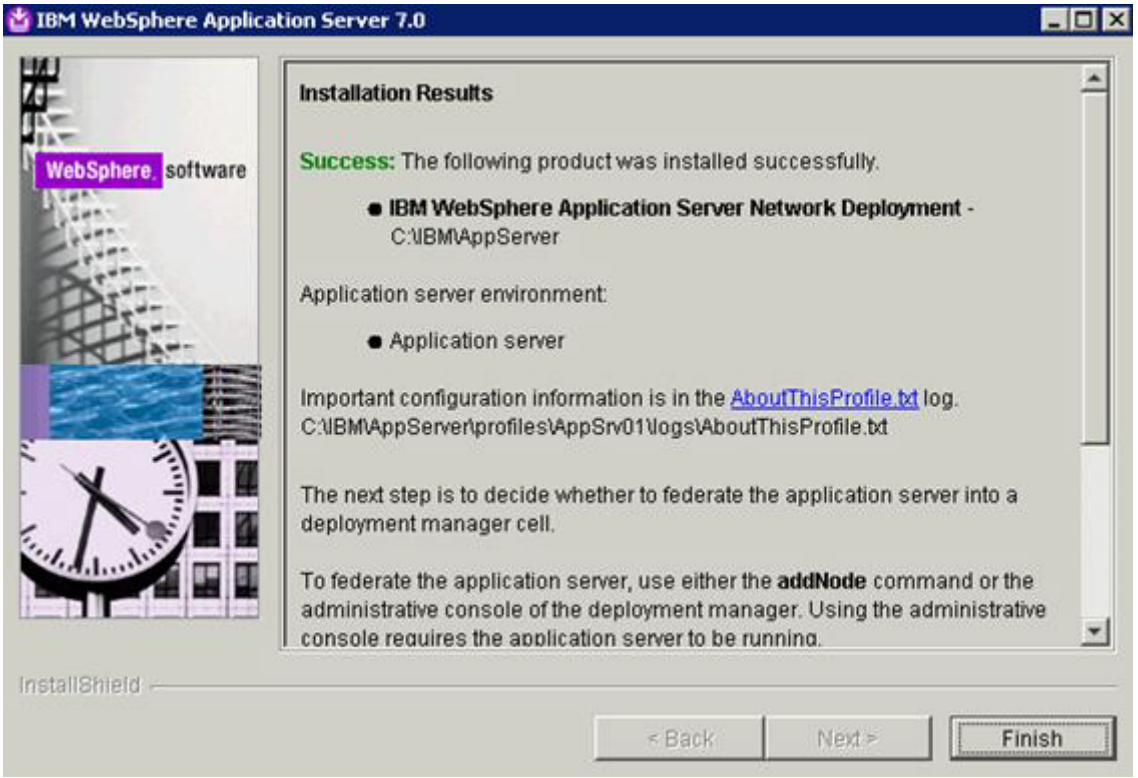


Figure 25. IBM WebSphere Application Server 7.0: Installation Results

__ 10. Click **Installation verification** to verify that the installation completed successfully.

Figure 26. WebSphere Application Server: First steps

A confirmation of successful installation is displayed.

Figure 27. WebSphere Application Server: First steps: Installation verification

Federating Application Server into Deployment Manager

On both node1 and node2, do the following steps:

__ 1. Start the Deployment Manager if it is not already started.

__ 2. On each of the nodes you want to add to the cell (and install IBM Connections on), do the following steps:

__ a. Open a command prompt (terminal on Linux) and change directory to <*AppServer/profiles/AppSrv01/bin*

__ b. Issue the command, addNode.bat(.sh) <*DeploymentManagerHostName*<*DM_SoapPort* -username <*WebSphere Application Server Admin User* -password <*WAS Admin Password*>.
The command appears similar to the following example:

addNode.bat dm.example.com 8879 -username wsadmin -password wsadmin

```
C:\IBM\AppServer\bin>addNode.bat dslvm337.mul.ie.ibm.com 8879 -user wasadmin -pa
ssword wasadmin
ADMU0116I: Tool information is being logged in file
           C:\IBM\AppServer\profiles\AppSrv01\logs\addNode.log
ADMU0128I: Starting tool with the AppSrv01 profile
CWPKI0308I: Adding signer alias "CN=dslvm337, OU=Root Certificat" to local
           keystore "ClientDefaultTrustStore" with the following SHA digest:
           CB:9A:3A:90:04:4D:8F:37:E9:CC:5C:55:FF:A6:77:B9:16:D2:7D:0A
CWPKI0308I: Adding signer alias "datapower" to local keystore
           "ClientDefaultTrustStore" with the following SHA digest:
           A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17
ADMU0001I: Begin federation of node dslvm338Node01 with Deployment Manager at
           dslvm337.mul.ie.ibm.com:8879.
ADMU0009I: Successfully connected to Deployment Manager Server:
           dslvm337.mul.ie.ibm.com:8879
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU2010I: Stopping all server processes for node dslvm338Node01
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: dslvm338Node01
ADMU0014I: Adding node dslvm338Node01 configuration to cell: dslvm337Cell01
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: dslvm338Node01
ADMU0020I: Reading configuration for Node Agent process: nodeagent
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id is:
           2764
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: nodeagent
ADMU0506I: Server name: server1
ADMU7703I: The Windows Service dslvm338Node01 associated with server1 is now
           being deregistered.


ADMU0300I: The node dslvm338Node01 was successfully added to the dslvm337Cell01
           cell.


ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone dslvm337Cell01
           configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the dslvm337Cell01 Deployment Manager
           with values from the old cell-level documents.


ADMU0306I: Note:
ADMU0304I: Because -includeapps was not specified, applications installed on
           the standalone node were not installed on the new cell.
ADMU0307I: You might want to:
ADMU0305I: Install applications onto the dslvm337Cell01 cell using wsadmin
           $AdminApp or the Administrative Console.


ADMU0003I: Node dslvm338Node01 has been successfully federated.

C:\IBM\AppServer\bin>_
```

Figure 28. Node 1


```
C:\IBM\AppServer\bin>addNode.bat dslvm337.mul.ie.ibm.com 8879 -user wasadmin -pa
ssword wasadmin
ADMU0116I: Tool information is being logged in file
           C:\IBM\AppServer\profiles\AppSrv01\logs\addNode.log
ADMU0128I: Starting tool with the AppSrv01 profile
CWPKI0308I: Adding signer alias "CN=dslvm337, OU=Root Certificat" to local
           keystore "ClientDefaultTrustStore" with the following SHA digest:
           CB:9A:3A:90:04:4D:8F:37:E9:CC:5C:55:FF:A6:77:B9:16:D2:7D:0A
CWPKI0308I: Adding signer alias "default" to local keystore
           "ClientDefaultTrustStore" with the following SHA digest:
           EC:67:61:08:45:2A:3A:DC:C7:B0:B4:F7:5B:F2:89:7C:50:83:12:4B
CWPKI0308I: Adding signer alias "datapower" to local keystore
           "ClientDefaultTrustStore" with the following SHA digest:
           A9:BA:A4:B5:BC:26:2F:5D:2A:80:93:CA:BA:F4:31:05:F2:54:14:17
ADMU0001I: Begin federation of node dslvm348Node01 with Deployment Manager at
           dslvm337.mul.ie.ibm.com:8879.
ADMU0009I: Successfully connected to Deployment Manager Server:
           dslvm337.mul.ie.ibm.com:8879
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: server1
ADMU2010I: Stopping all server processes for node dslvm348Node01
ADMU0024I: Deleting the old backup directory.
ADMU0015I: Backing up the original cell repository.
ADMU0012I: Creating Node Agent configuration for node: dslvm348Node01
ADMU0014I: Adding node dslvm348Node01 configuration to cell: dslvm337Cell01
ADMU0016I: Synchronizing configuration between node and cell.
ADMU0018I: Launching Node Agent process for node: dslvm348Node01
ADMU0020I: Reading configuration for Node Agent process: nodeagent
ADMU0022I: Node Agent launched. Waiting for initialization status.
ADMU0030I: Node Agent initialization completed successfully. Process id is: 124
ADMU0505I: Servers found in configuration:
ADMU0506I: Server name: nodeagent
ADMU0506I: Server name: server1
ADMU7703I: The Windows Service dslvm348Node01 associated with server1 is now
           being deregistered.


ADMU0300I: The node dslvm348Node01 was successfully added to the dslvm337Cell01
           cell.


ADMU0306I: Note:
ADMU0302I: Any cell-level documents from the standalone dslvm337Cell01
           configuration have not been migrated to the new cell.
ADMU0307I: You might want to:
ADMU0303I: Update the configuration on the dslvm337Cell01 Deployment Manager
           with values from the old cell-level documents.


ADMU0306I: Note:
ADMU0304I: Because -includeapps was not specified, applications installed on
           the standalone node were not installed on the new cell.
ADMU0307I: You might want to:
ADMU0305I: Install applications onto the dslvm337Cell01 cell using wsadmin
           $AdminApp or the Administrative Console.


ADMU0003I: Node dslvm348Node01 has been successfully federated.

C:\IBM\AppServer\bin>_
```

Figure 29. Node 2

Both nodes are added and shown in WebSphere Application Server console:

Figure 30. Integrated Solutions Console: Application servers

Installing HTTP Server and plug-ins v7.0.0.0

__ 1. On connections.example.com, extract the WebSphere Application Server Supplements file into a directory on your hard disk. Go into the IBM HTTP Server subdirectory and double-click `install.exe`. The following panel is displayed. Click **Next**.

Figure 31. IBM HTTP Server 7.0: Welcome

__ 2. Accept both the IBM and non-IBM terms and click **Next**.

Figure 32. IBM HTTP Server 7.0: Software License Agreement

__ 3. If the prerequisites check is successful, click **Next**.

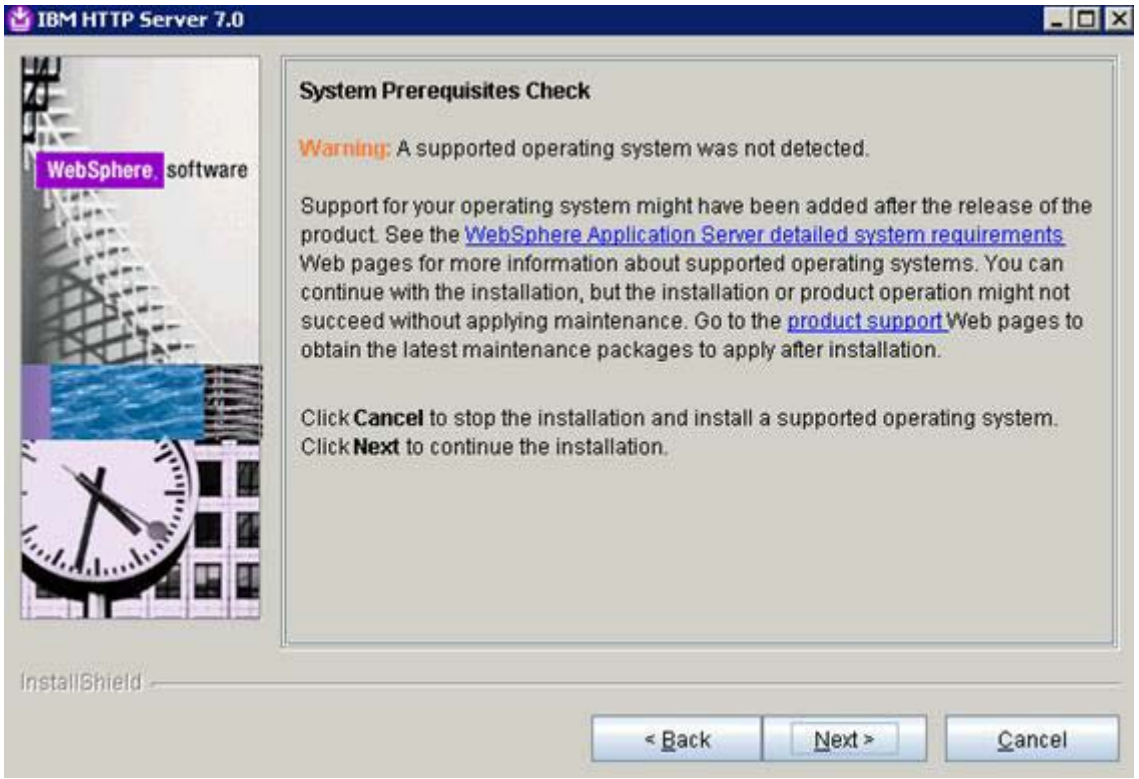


Figure 33. IBM HTTP Server 7.0: System Prerequisites Check

__ 4. Select an installation directory, preferably not in `c:\Program Files`, and click **Next**.

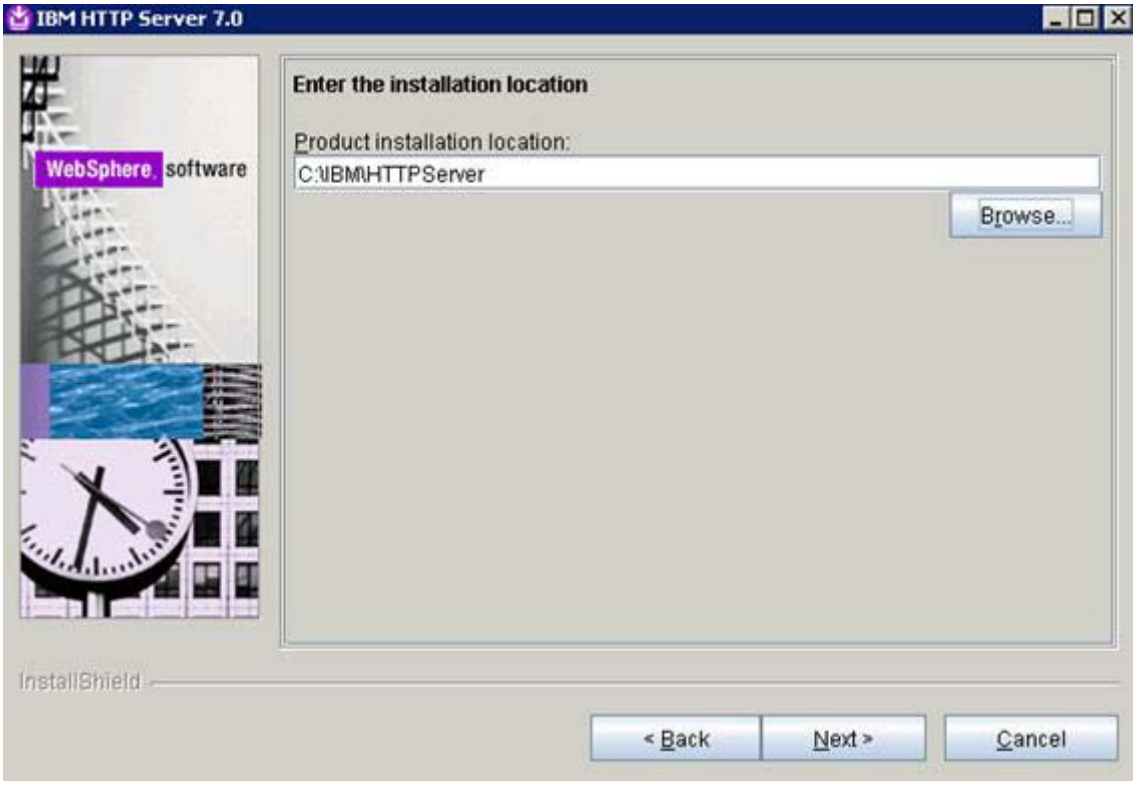


Figure 34. IBM HTTP Server 7.0: Enter the installation location

__ 5. Leave the default values, and click **Next**.

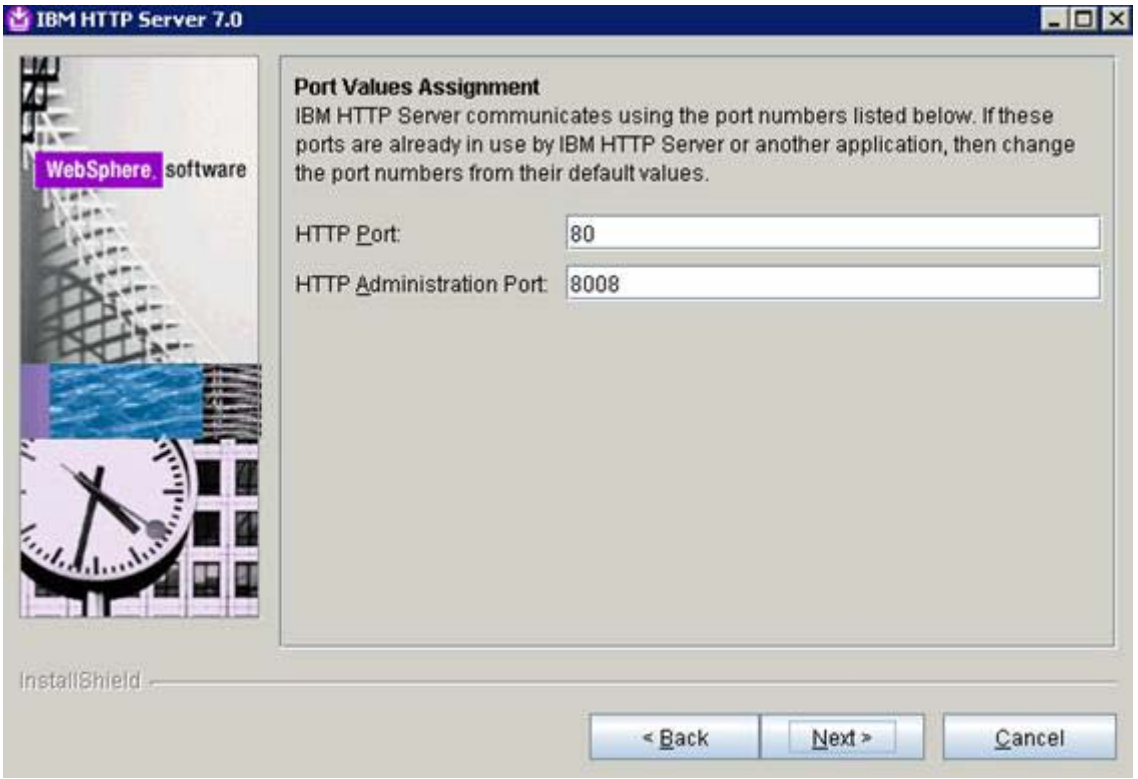


Figure 35. IBM HTTP Server 7.0: Port Values Assignment

__ 6. Select the two check boxes at the top, select **Log on as a specified user account**, and select a user name and a password for that account. Click **Next**.

Figure 36. IBM HTTP Server 7.0: Windows Service Definition

__ 7. Check "Create a user ID for IBM HTTP Server administration server authentication", and select a user name and a password. Click **Next**.

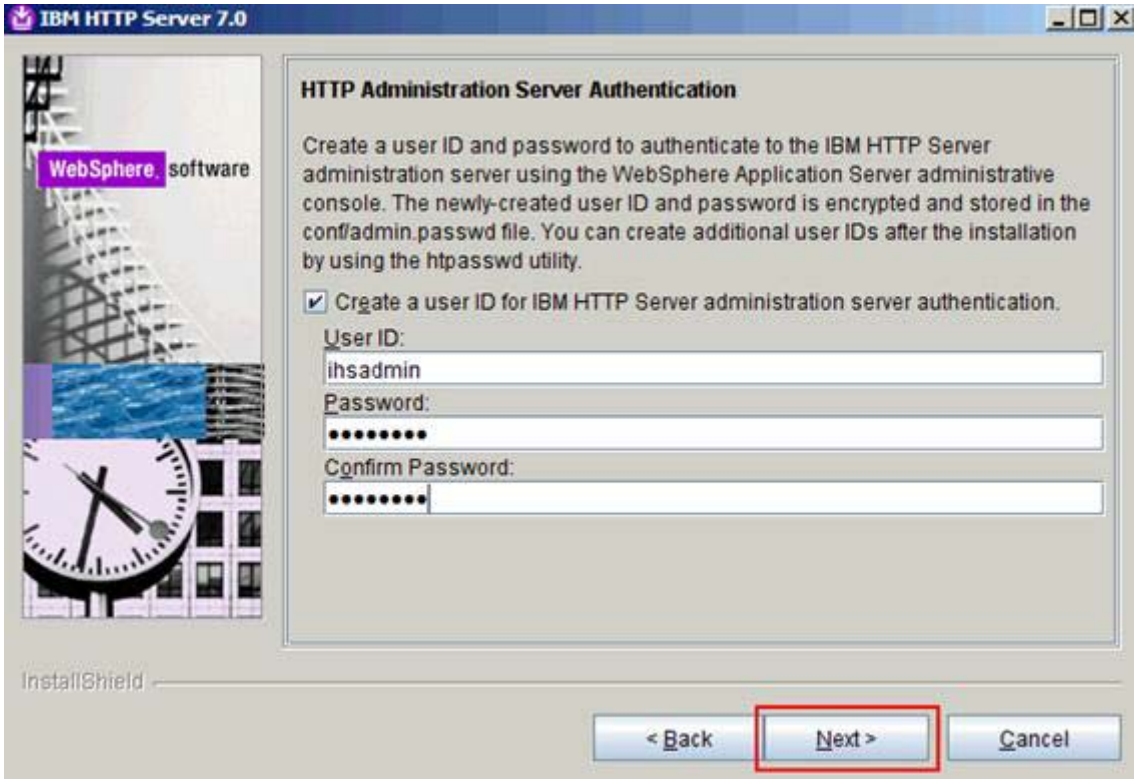


Figure 37. IBM HTTP Server 7.0: HTTP Administration Server Authentication

__ 8. Select "Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server Web server definition". For the following two that should already be completed, leave the defaults and click **Next**.

Figure 38. IBM HTTP Server 7.0: IBM HTTP Server Plug-in for IBM WebSphere Application Server

__ 9. Review the installation summary, and click **Next**.

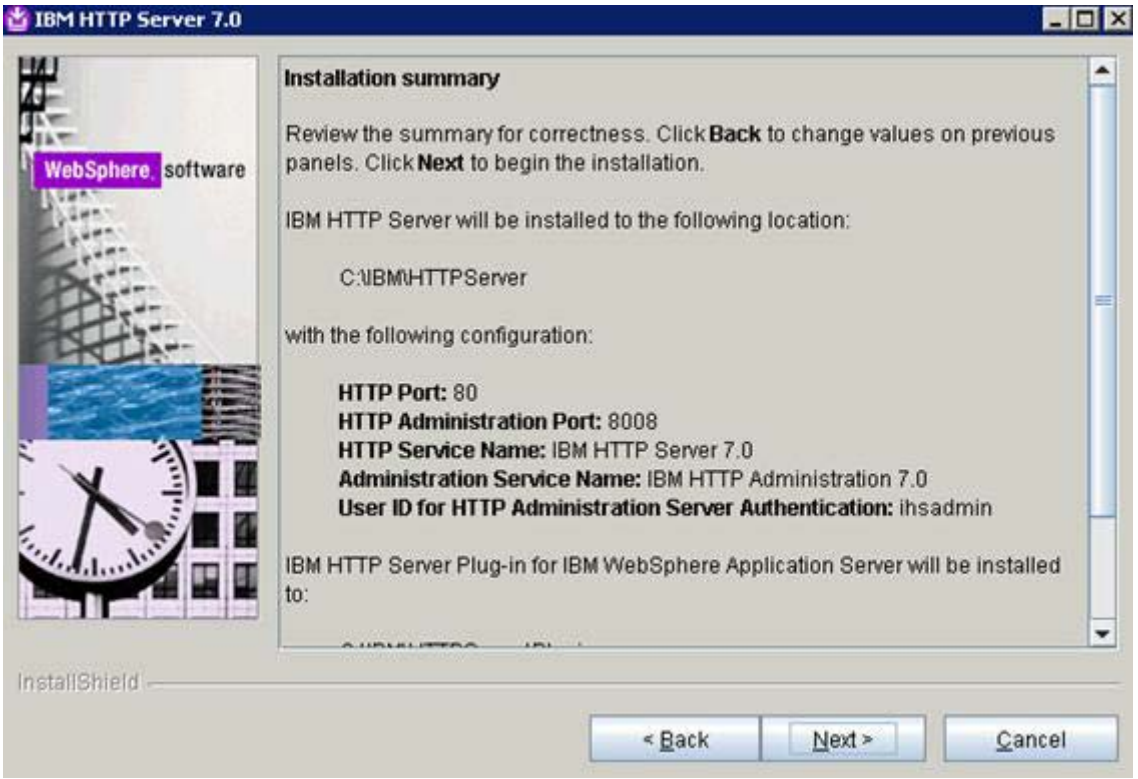


Figure 39. IBM HTTP Server 7.0: Installation summary

__ 10. Click **Finish** to quit the installer and continue installing the fix packs levels in next section.

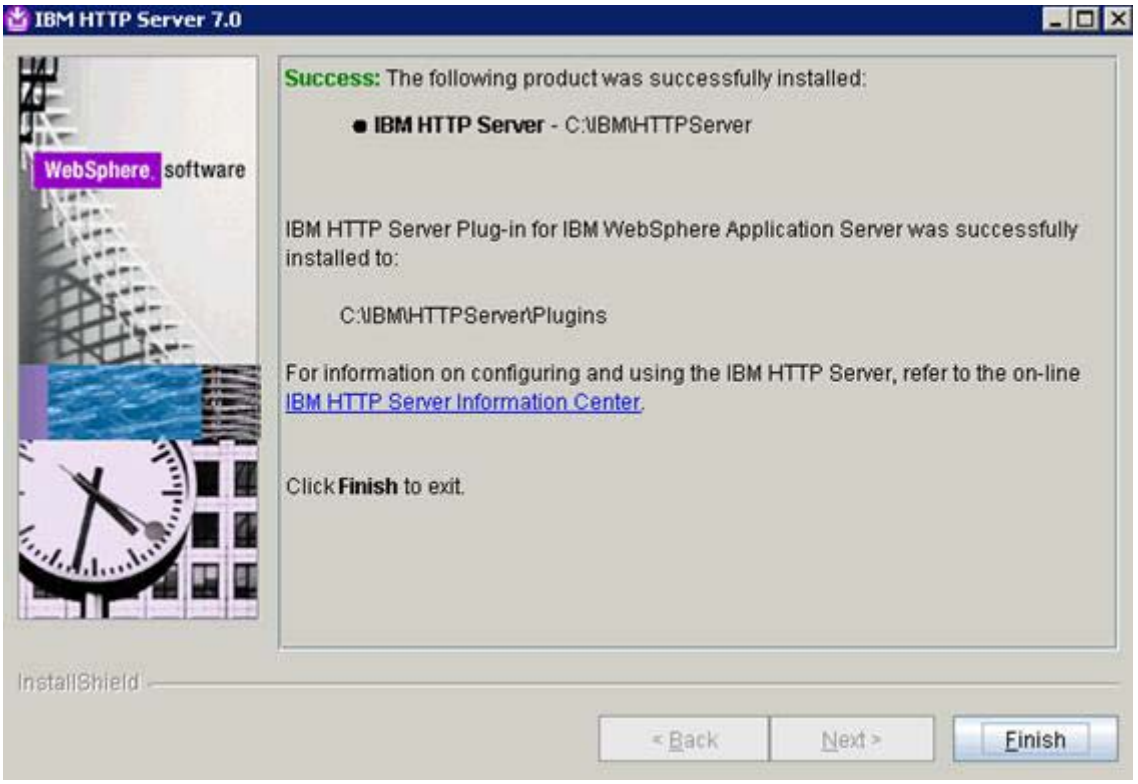


Figure 40. IBM HTTP Server 7.0: Installation Wizard for the Update Installer

Install WebSphere Update Installer and Upgrading to Fix Pack Level xx

Apply the fix pack on dm.example.com, node1.example.com, and node2.example.com

Note

You must repeat this procedure on all three servers.

__ 1. In the directory where you extracted the WebSphere Application Server Supplements, go to the `UpdateInstaller` directory and click `Install.exe`. The following panel is displayed. Click **Next**.

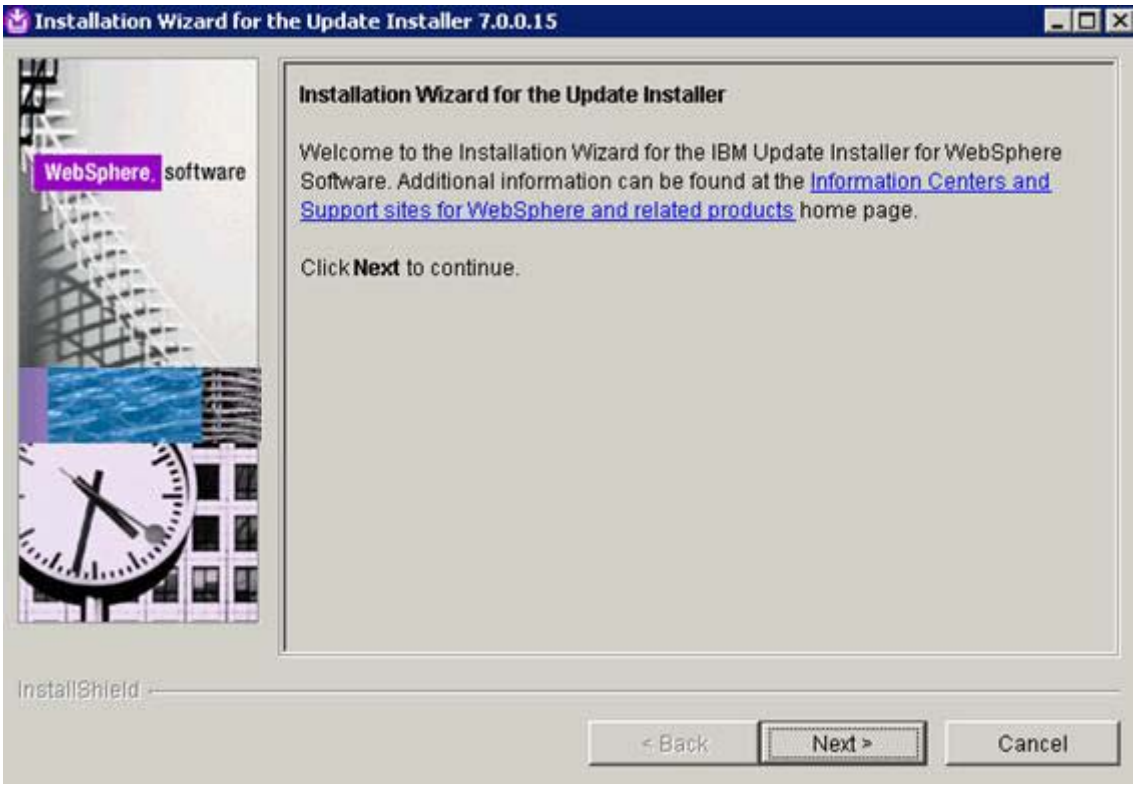


Figure 41. Installation Wizard for the Update Installer

__ 2. Accept both the IBM and non-IBM terms and click **Next**.

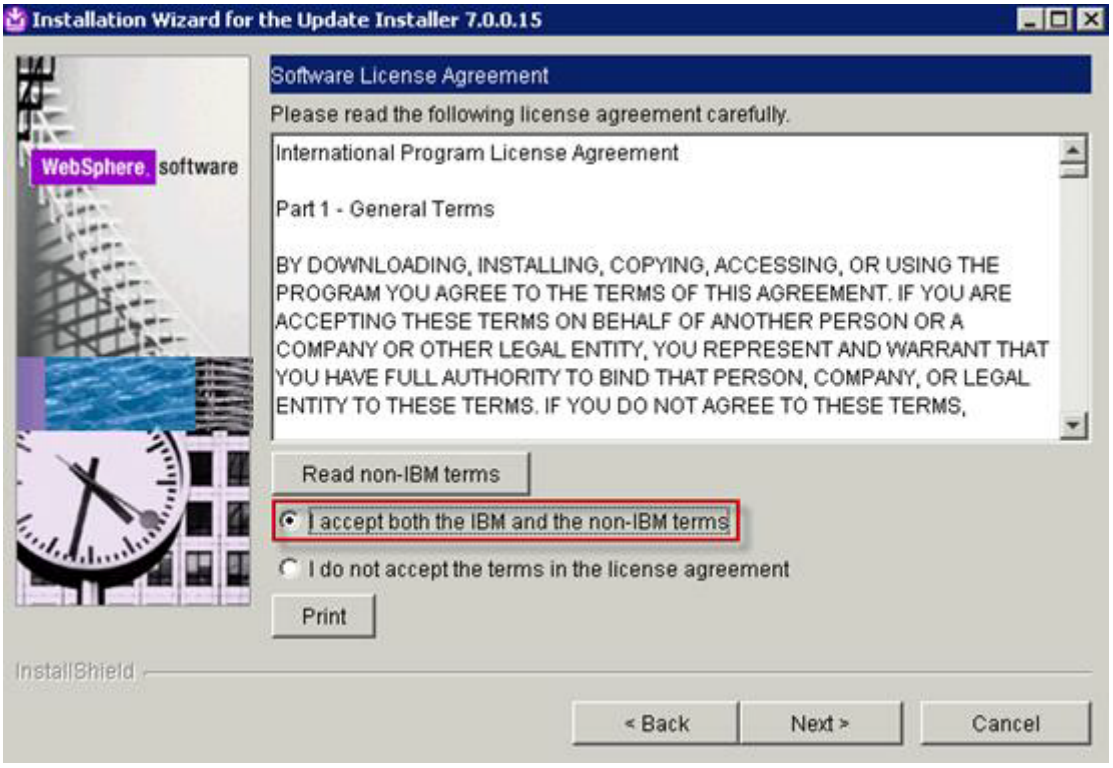


Figure 42. Installation Wizard for the Update Installer: License Agreement

__ 3. If the prerequisites check is successful, click **Next**.

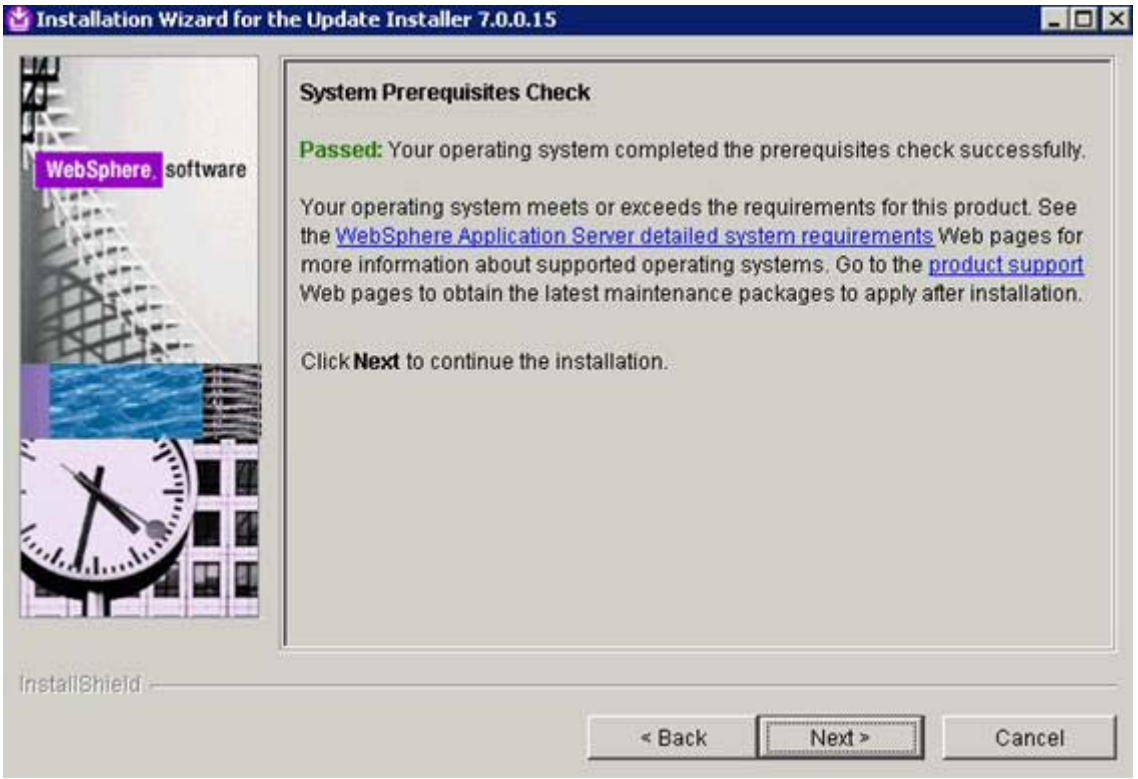


Figure 43. Installation Wizard for the Update Installer: System Prerequisites Check

__ 4. Select an installation directory, preferably not in `c:\Program Files`, and click **Next**.

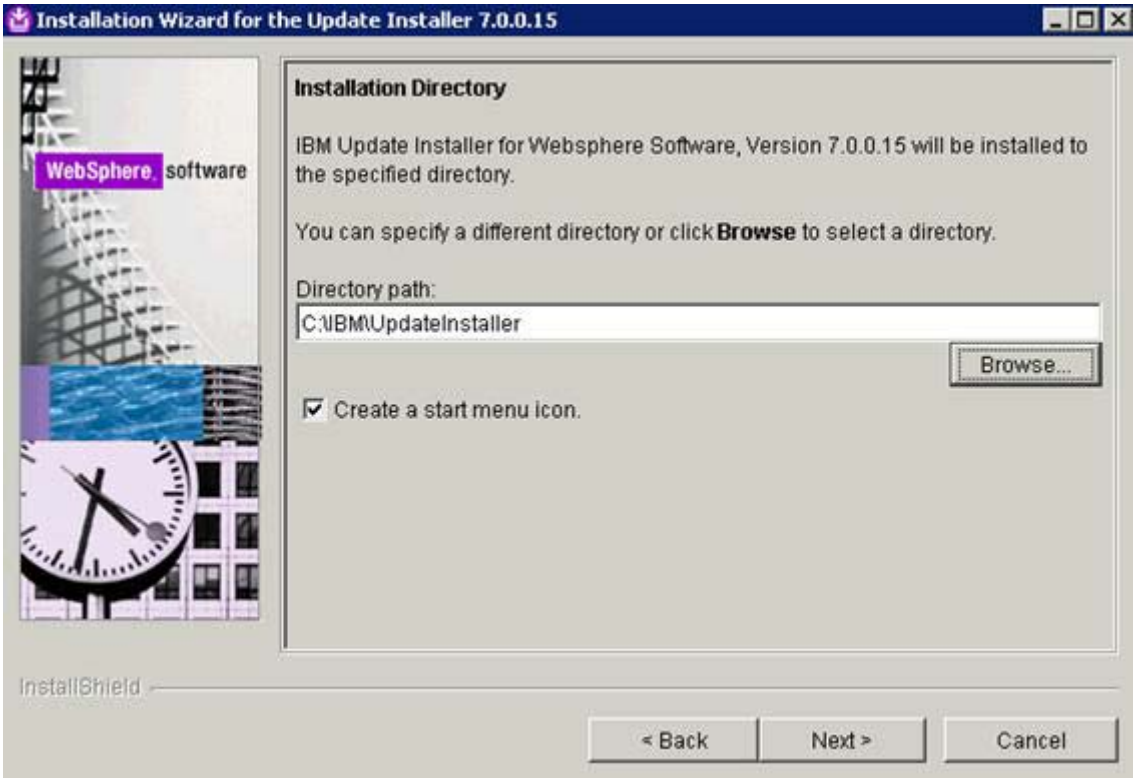


Figure 44. Installation Wizard for the Update Installer: Installation Directory

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

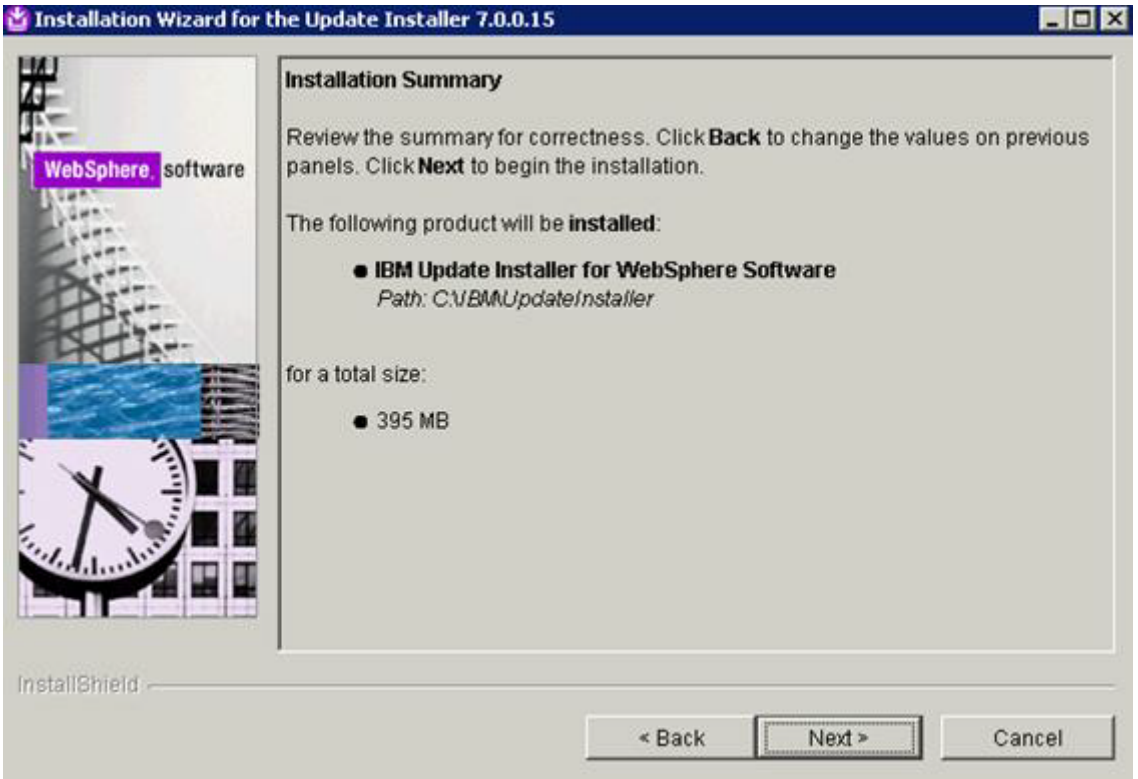


Figure 45. Installation Wizard for the Update Installer: Installation Summary

__ 6. Select Launch IBM Update installer for WebSphere Software on exit, and click **Finish** to exit the installer. The IBM Update Installer for WebSphere Software 7.0.0.15 wizard is displayed.

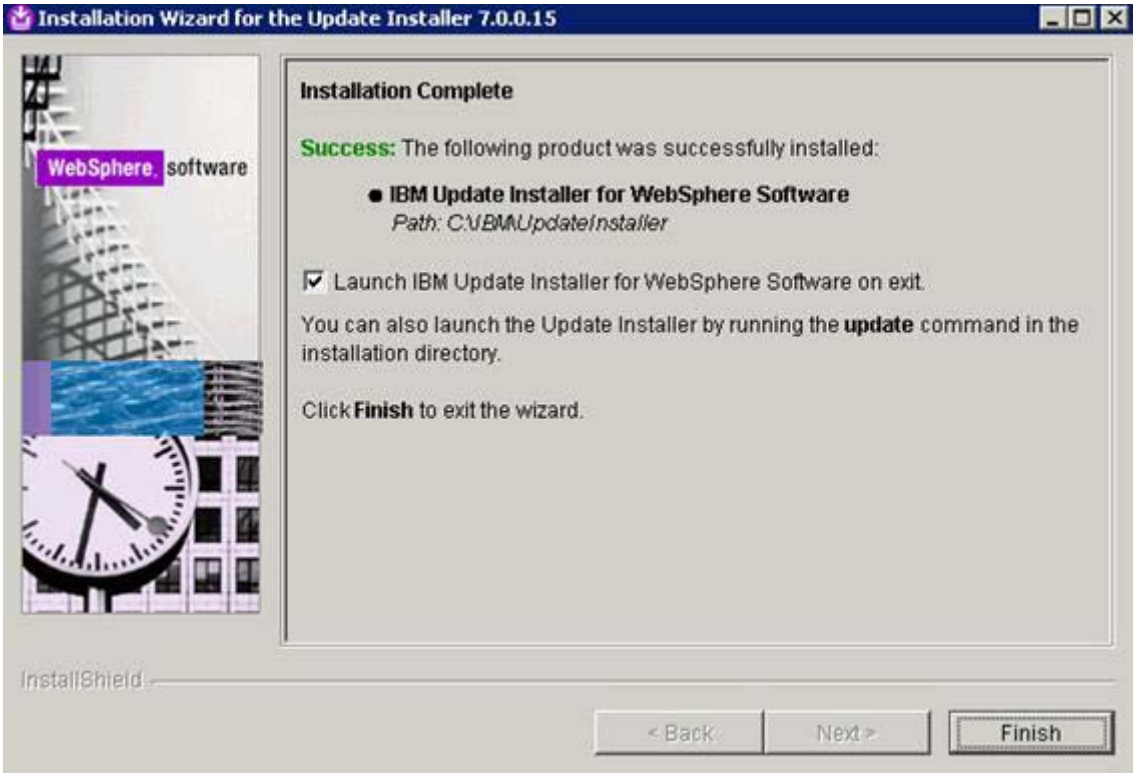


Figure 46. Installation Wizard for the Update Installer: Installation Complete

Upgrading to correct fix pack level

__ 1. In the welcome screen of the IBM Update Installer for WebSphere Software wizard, click Next.

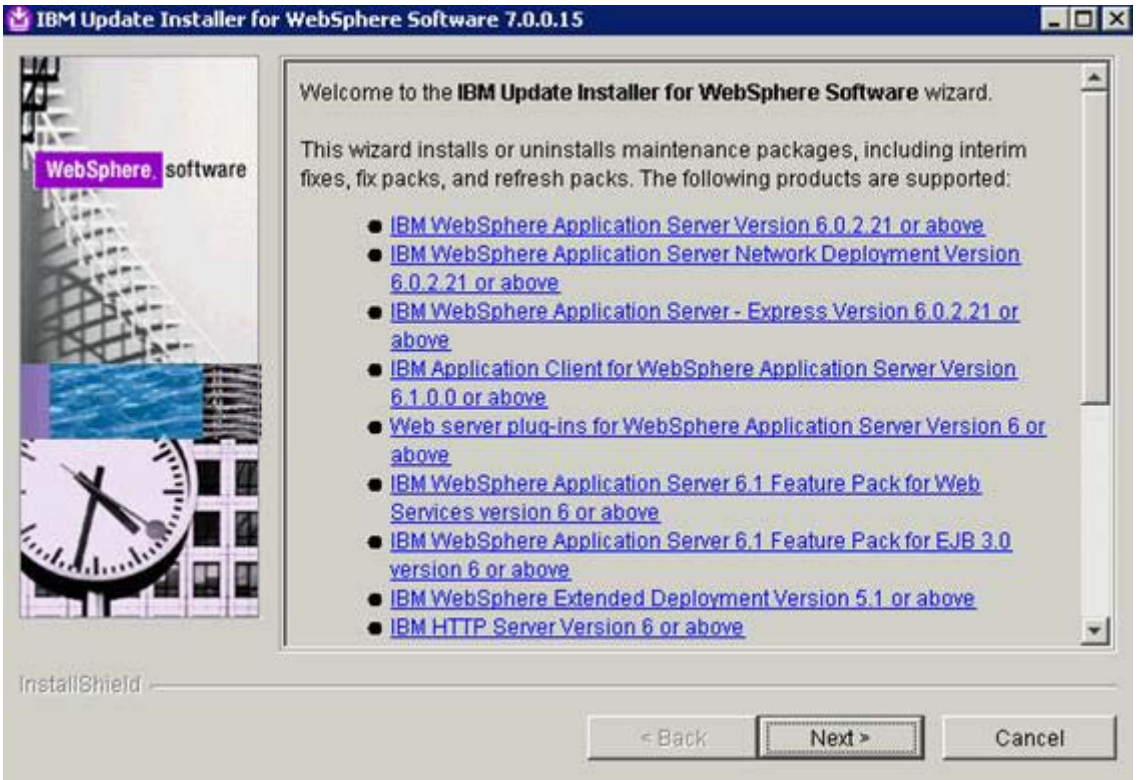


Figure 47. IBM Update Installer for WebSphere Software wizard: Welcome

__ 2. The location of the AppServer should already be completed. Click **Next**.

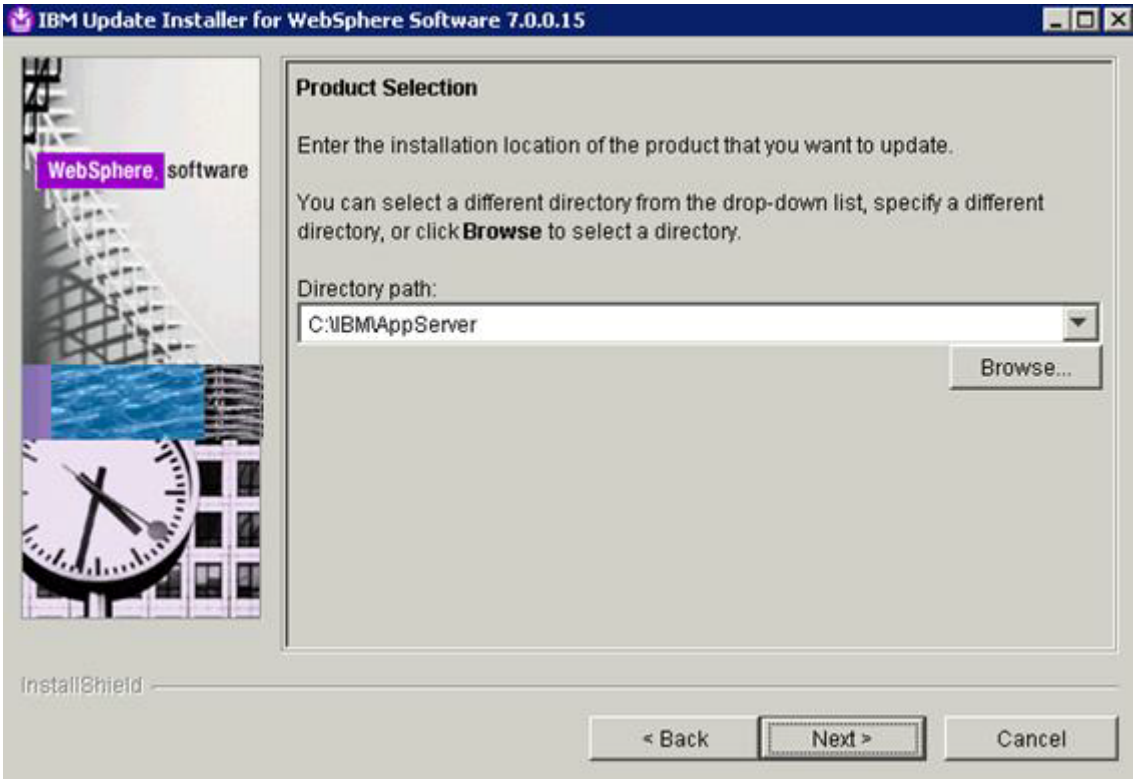


Figure 48. IBM Update Installer for WebSphere Software wizard: Product Selection

__ 3. Select "Install maintenance package" and click **Next**.

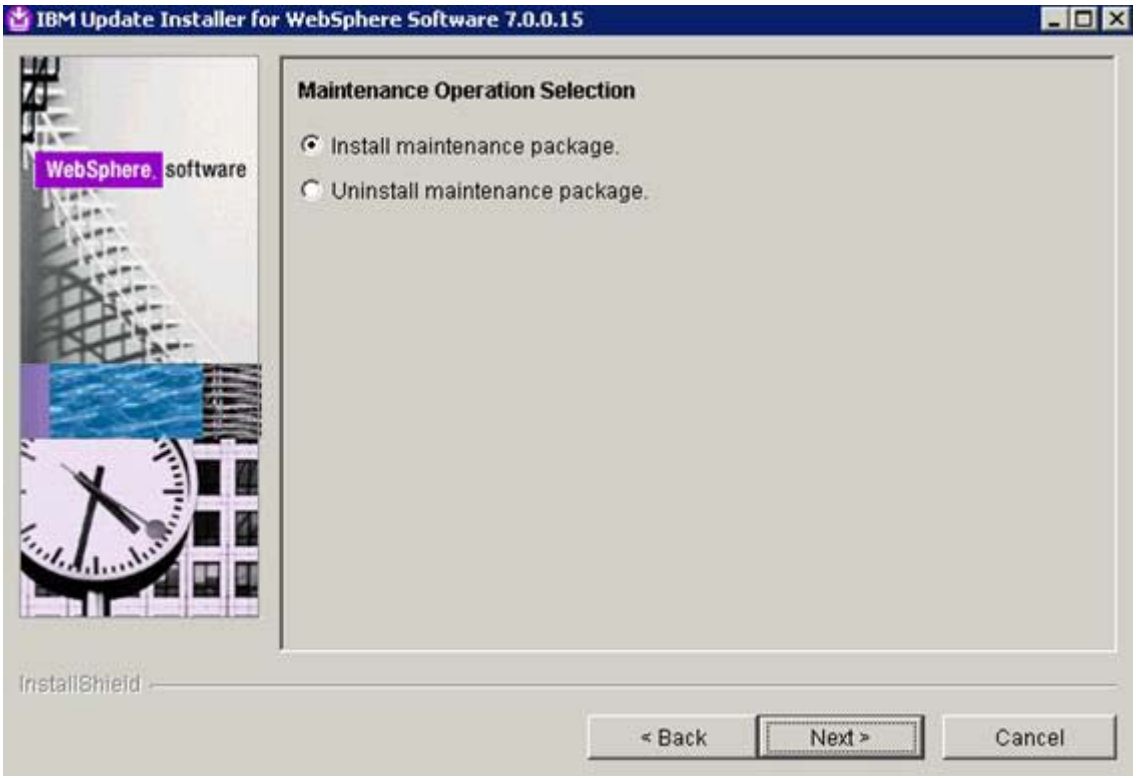


Figure 49. IBM Update Installer for WebSphere Software wizard: Maintenance Operation Selection

__ 4. Select the directory where you copied all the fix packs. Click **Next**.

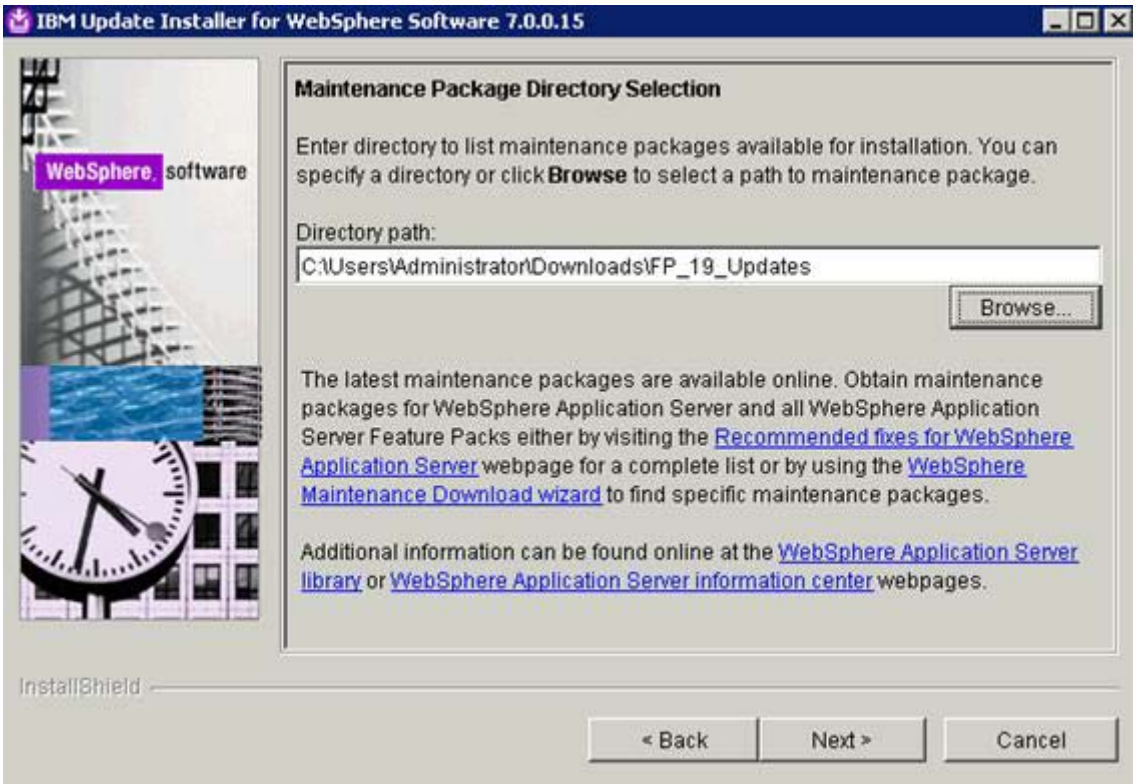


Figure 50. IBM Update Installer for WebSphere Software wizard: Maintenance Package Directory Selection

__ 5. Check the applicable boxes and click **Next**.

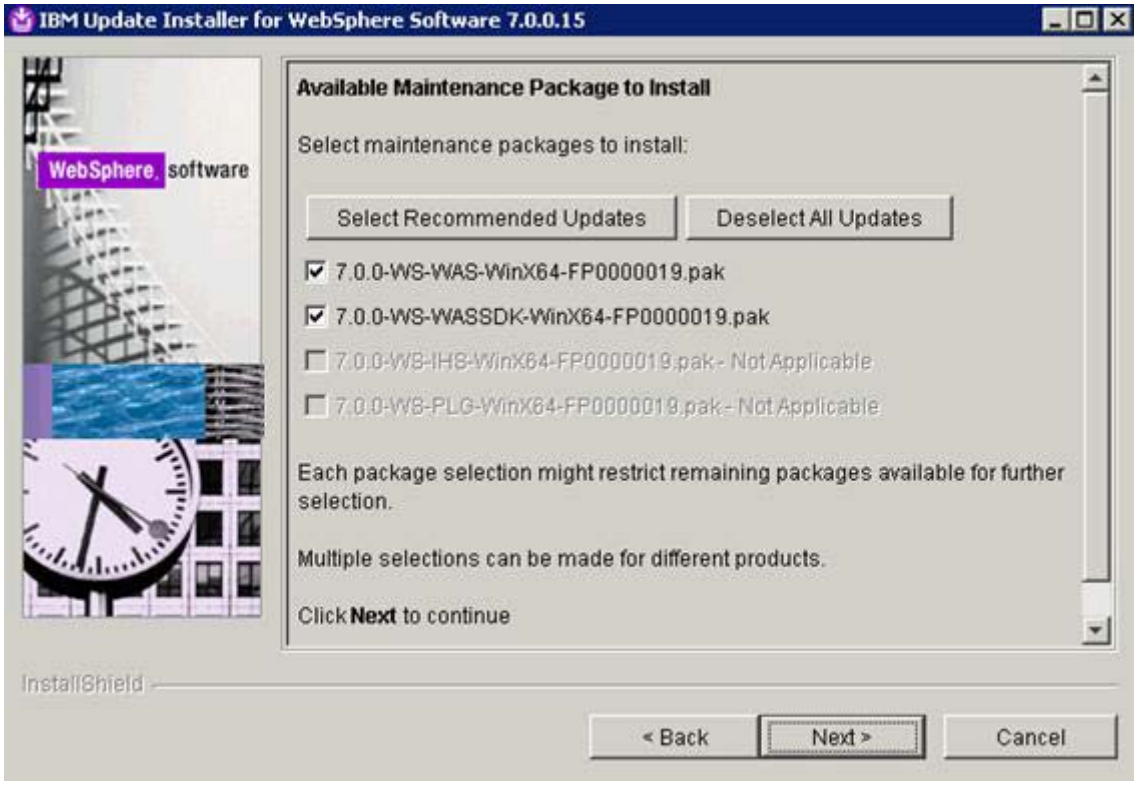


Figure 51. IBM Update Installer for WebSphere Software wizard: Available Maintenance Package to Install

__ 6. Review the installation summary and click **Next**.

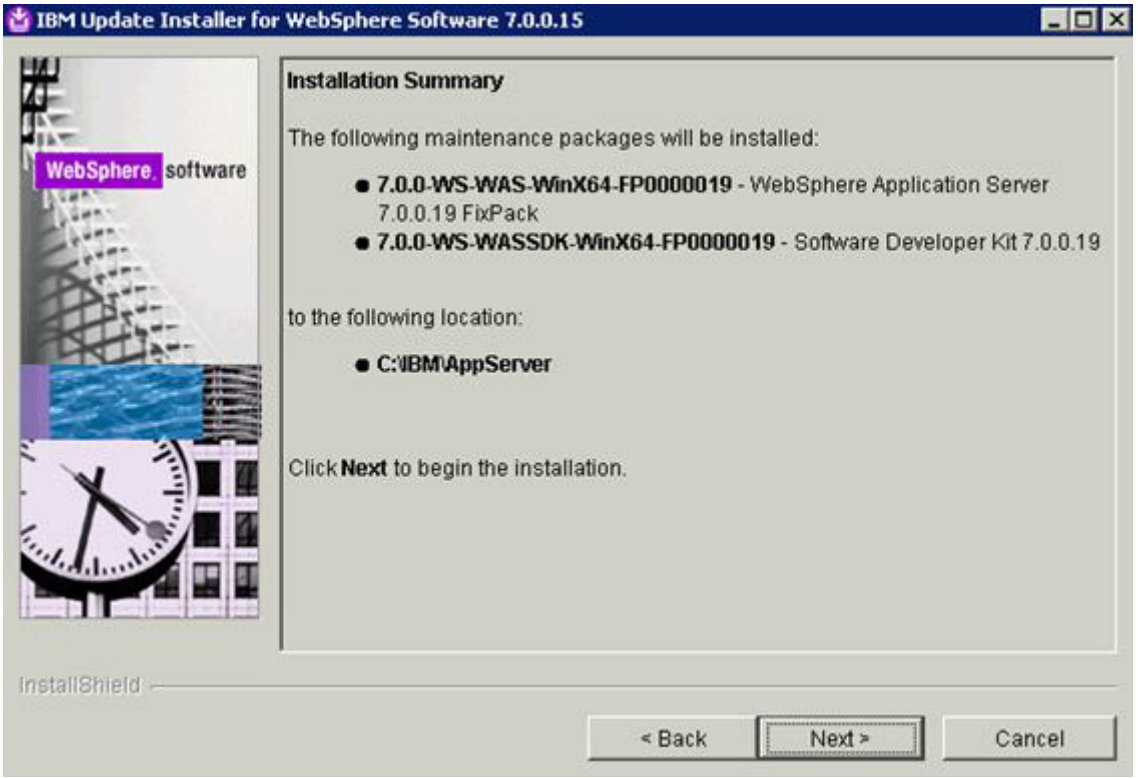


Figure 52. IBM Update Installer for WebSphere Software wizard: Installation Summary

The installation of fix pack updates begins.

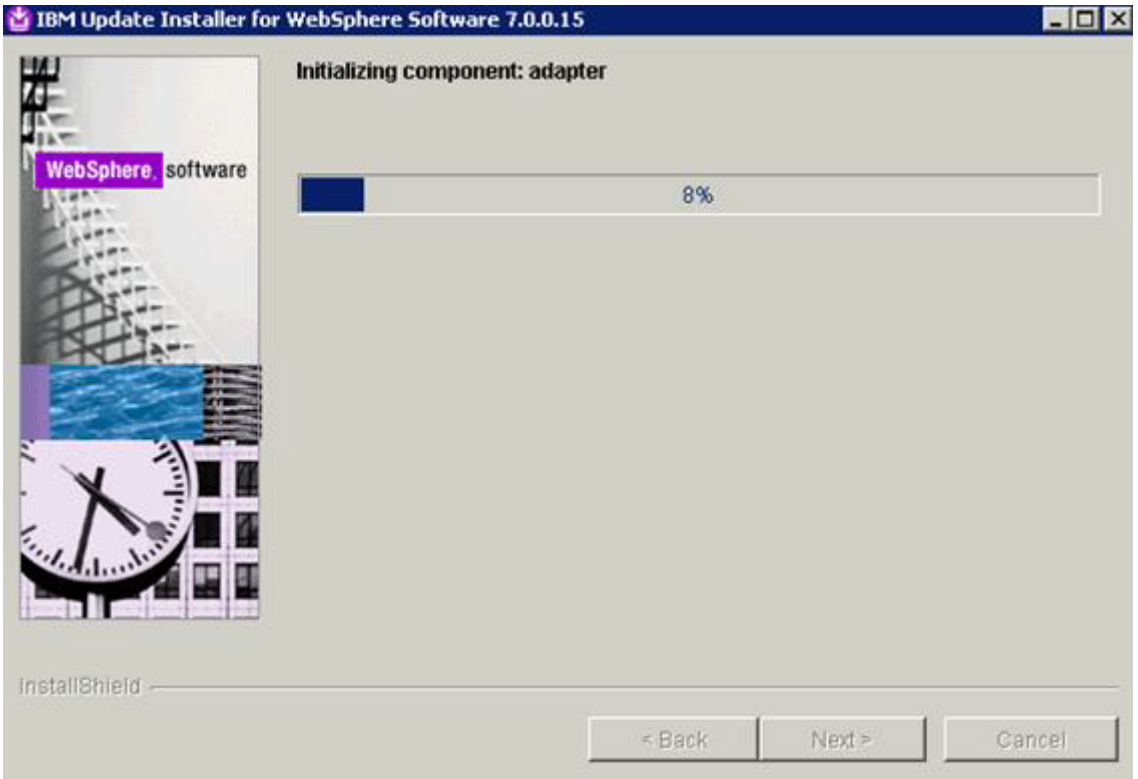


Figure 53. IBM Update Installer for WebSphere Software wizard: Component installation in progress

__ 7. When installation completes, click **Finish** to quit the installer.

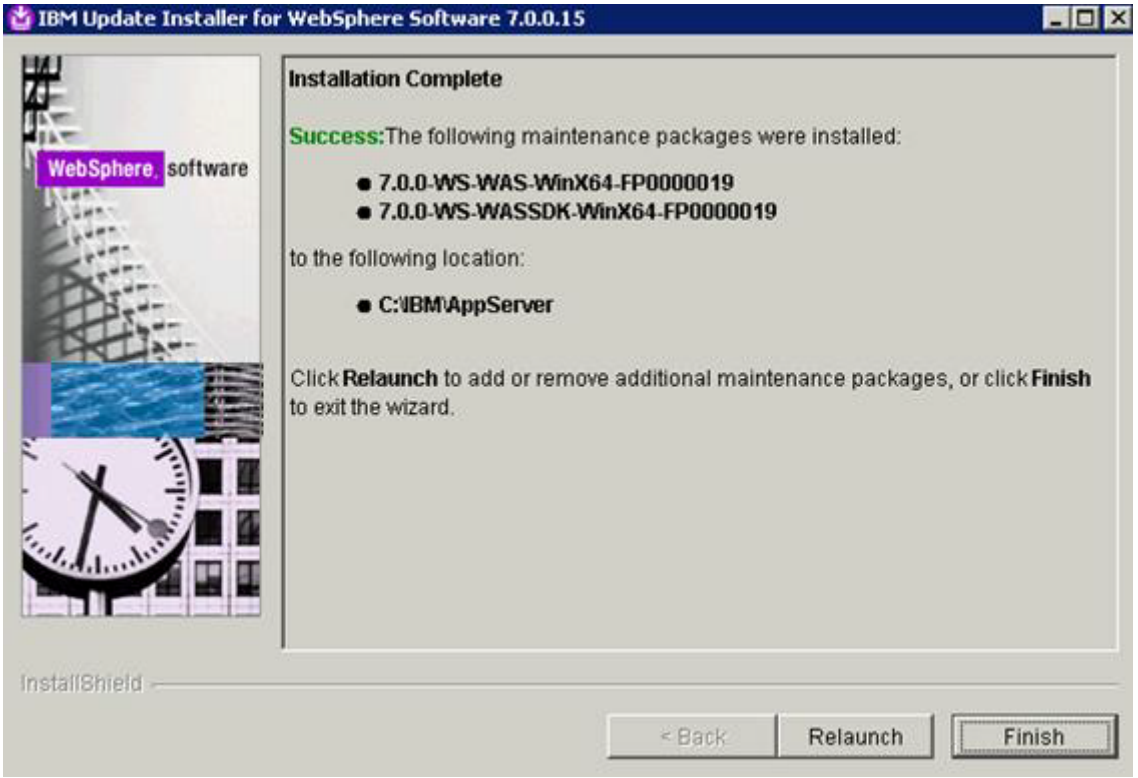


Figure 54. IBM Update Installer for WebSphere Software wizard: Installation Complete

Installing MS SQL Server 2008 SP1

__ 1. Run the MS SQL Server `iso` software from where it was downloaded, and click the `install.exe` file to begin the SQL Server Installation Center as shown in the following figure. Click **Installation** to continue.

Figure 55. SQL Server Installation Center

__ 2. Click **OK** to continue.

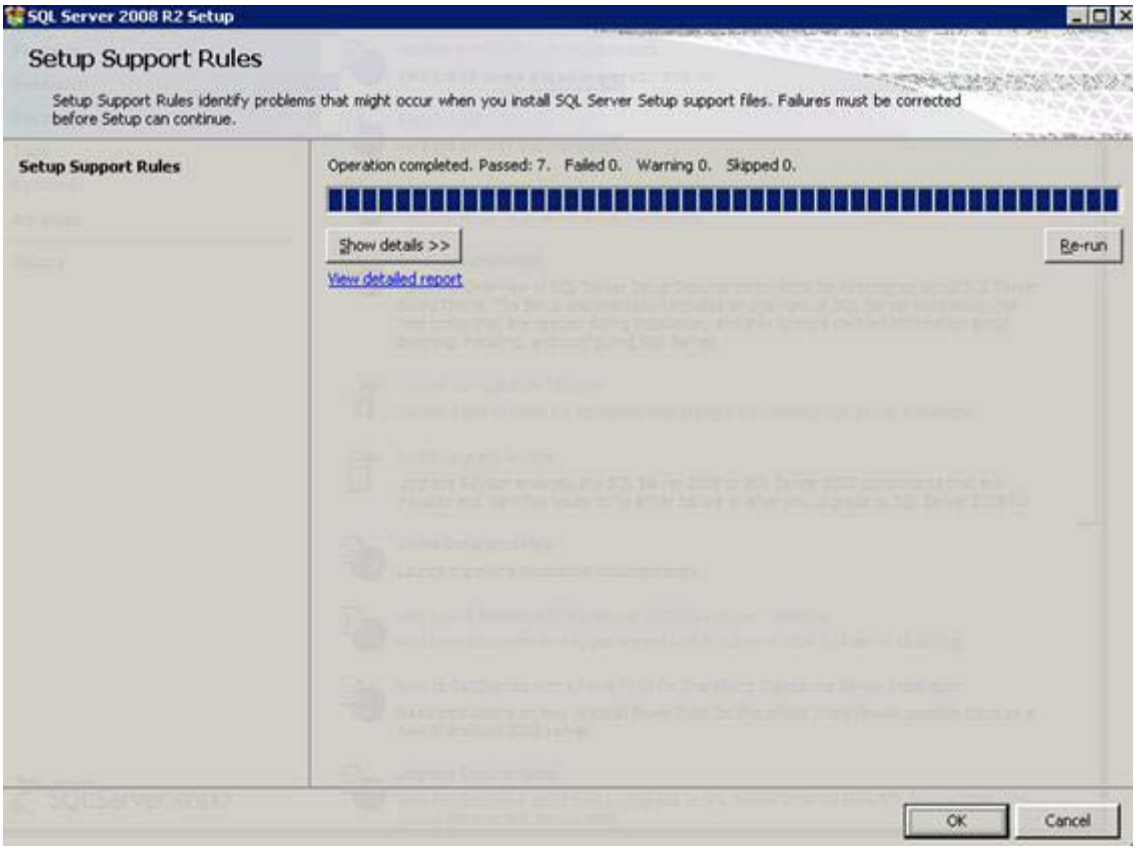


Figure 56. SQL Server Installation Center: Setup Support Rules

__ 3. Click **Install** to continue.

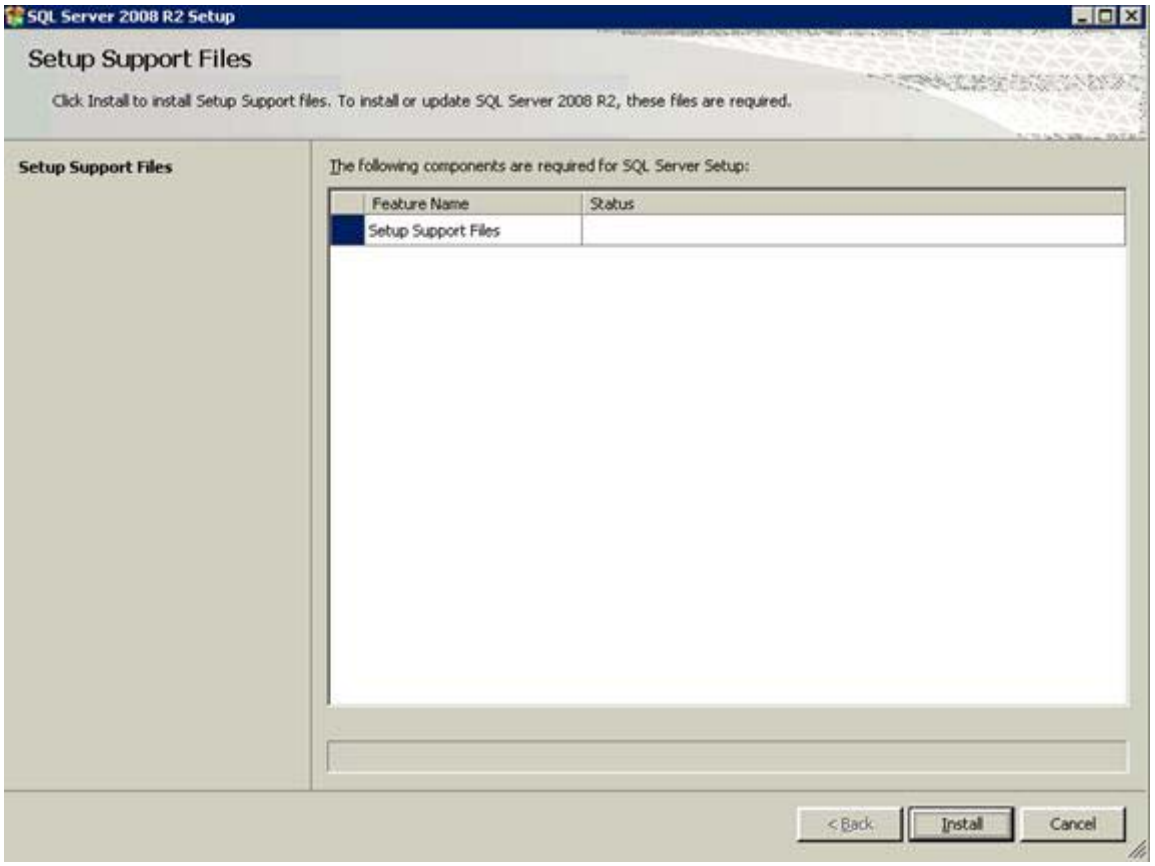


Figure 57. SQL Server Installation Center: Setup Support Files

__ 4. Click **Next** to continue.

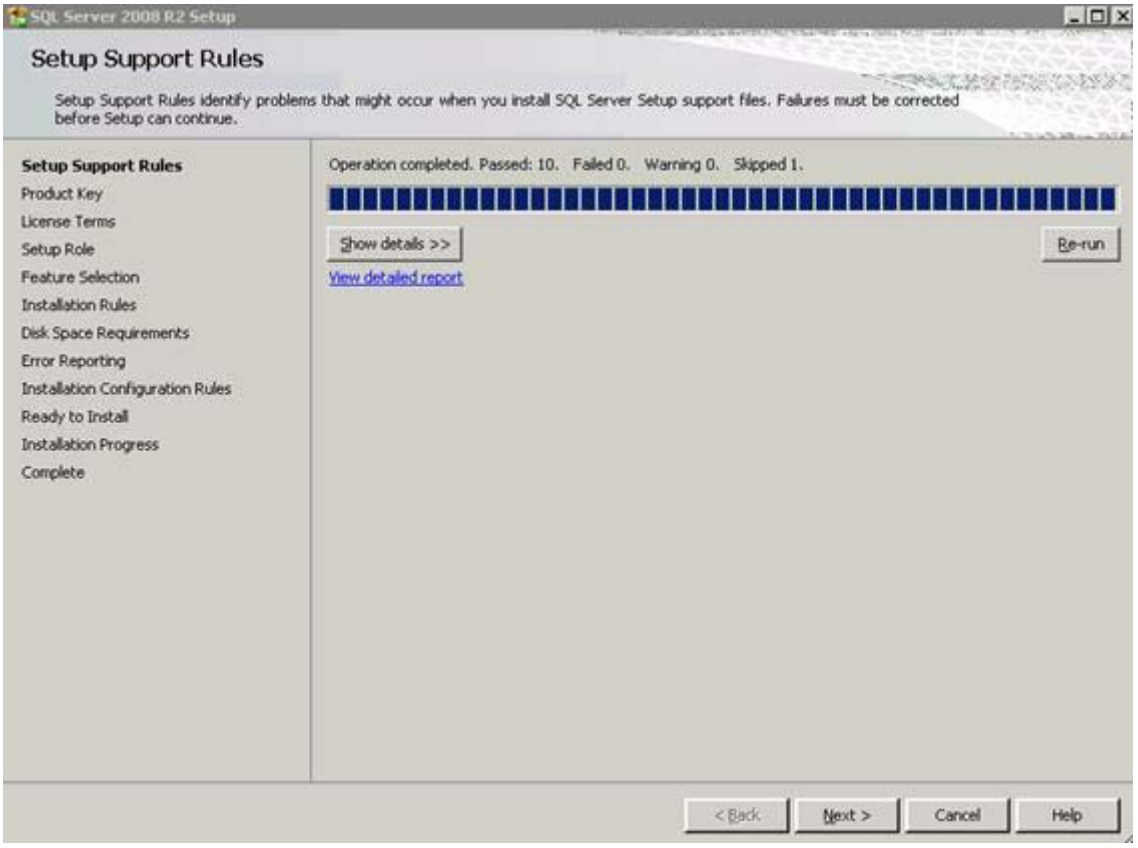


Figure 58. SQL Server Installation Center: Setup Support Rules

__ 5. Enter the product key for the software and click **Next** to continue.

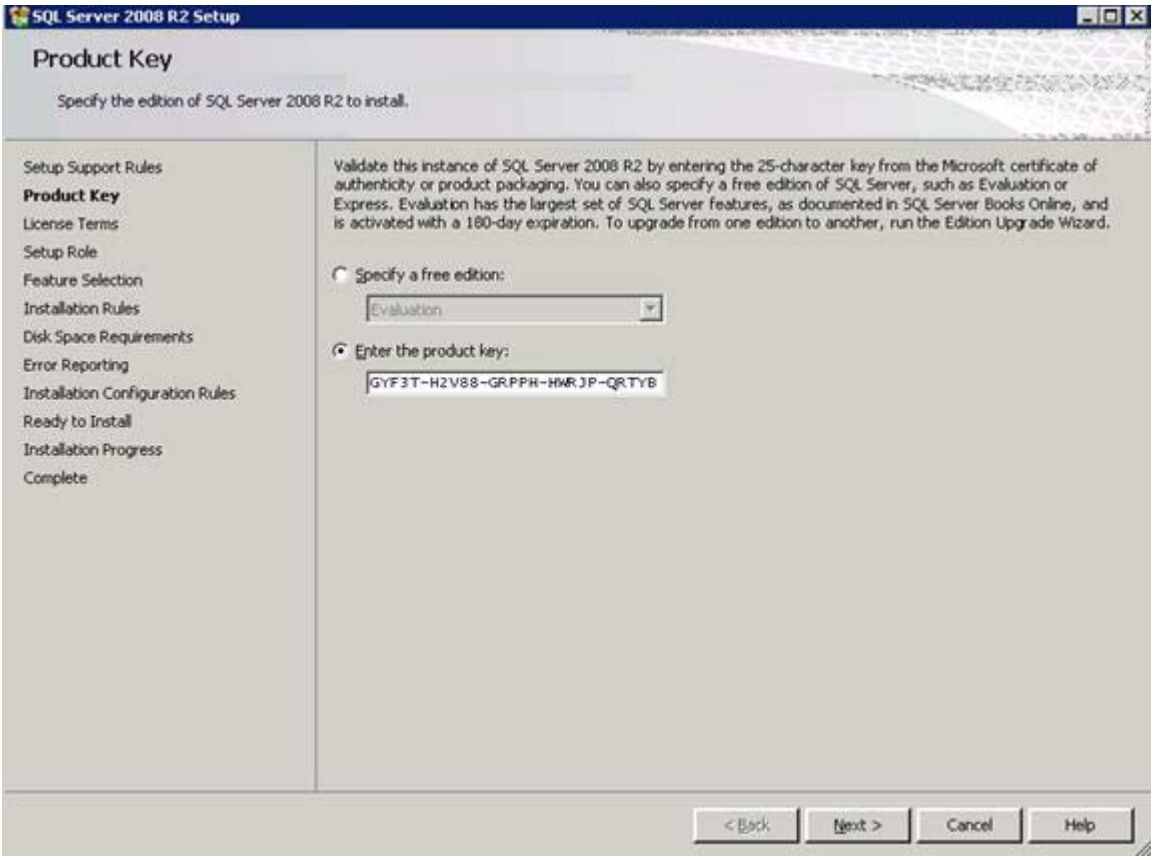


Figure 59. SQL Server Installation Center: Product Key

__ 6. Select the check box to accept the license terms and then click **Next** to continue.

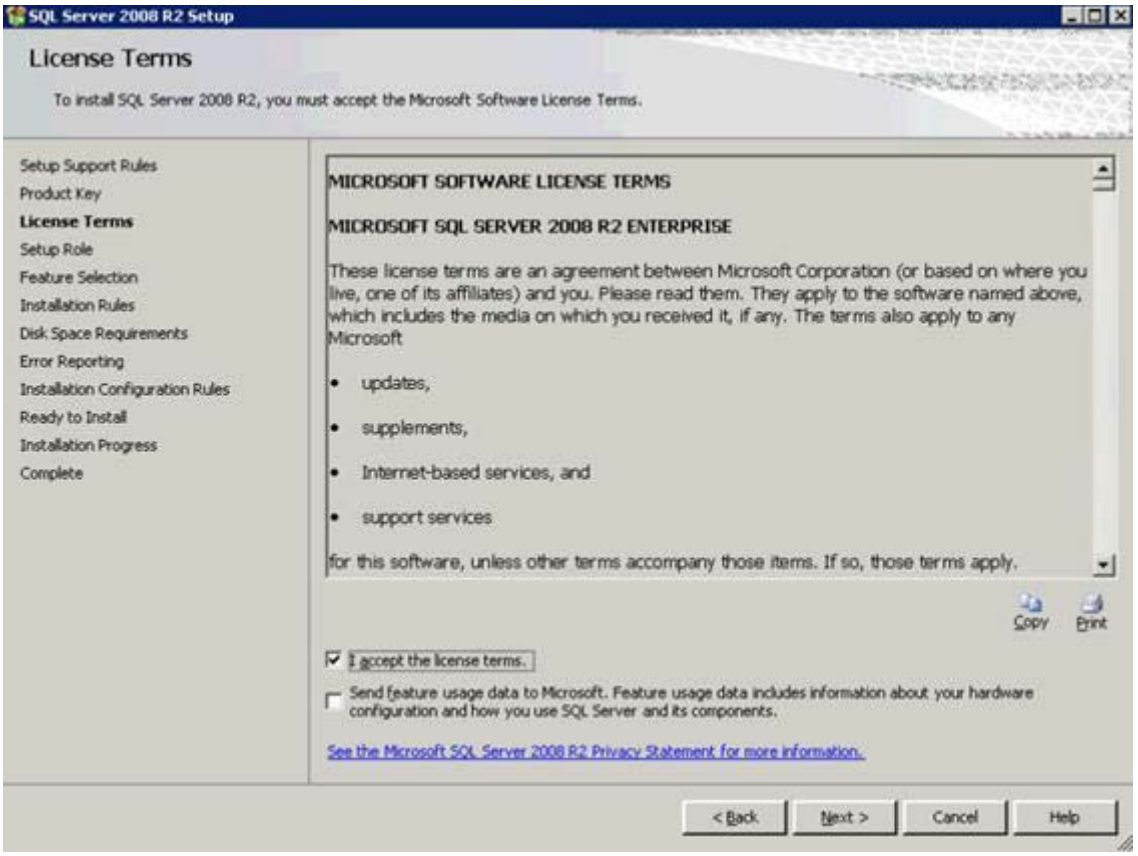


Figure 60. SQL Server Installation Center: License Terms

__ 7. Select **SQL Server Feature Installation** and click **Next** to continue.

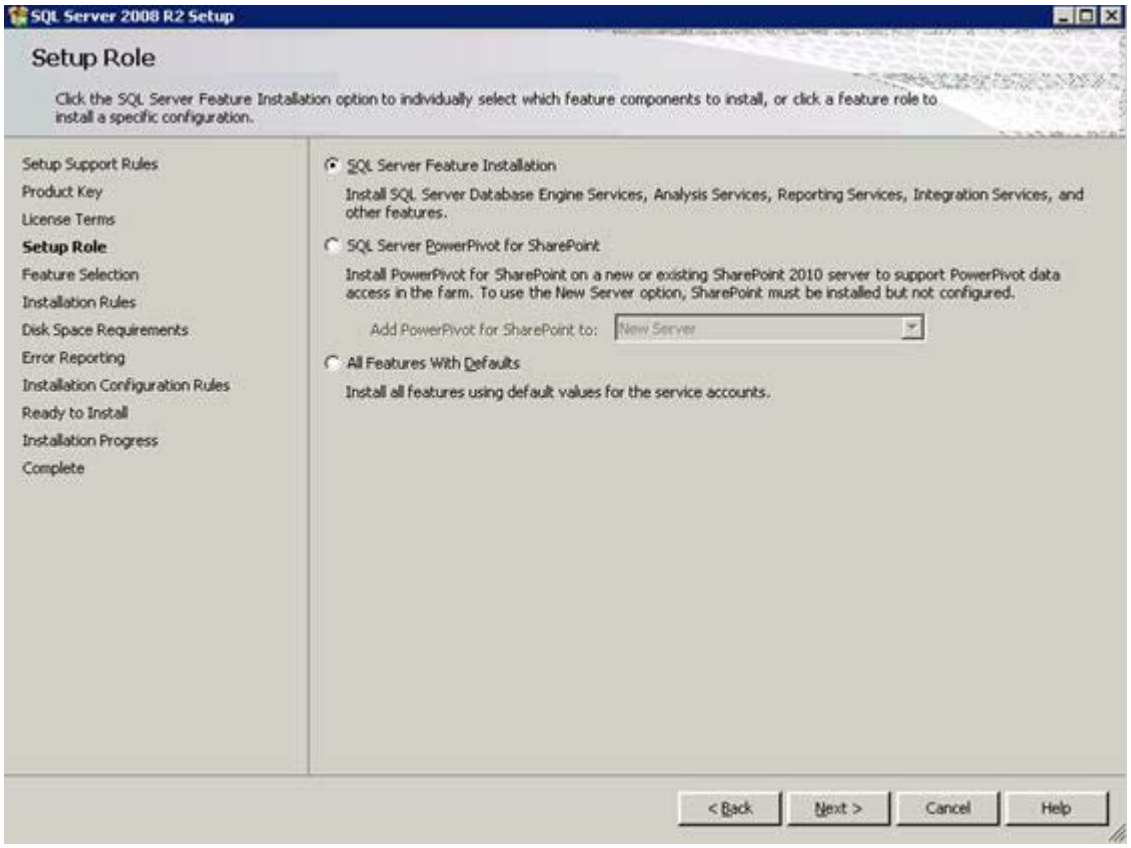


Figure 61. SQL Server Installation Center: Setup Role

__ 8. Select the features as shown in the following screen and select the Shared features directory. Then, click **Next** to continue.

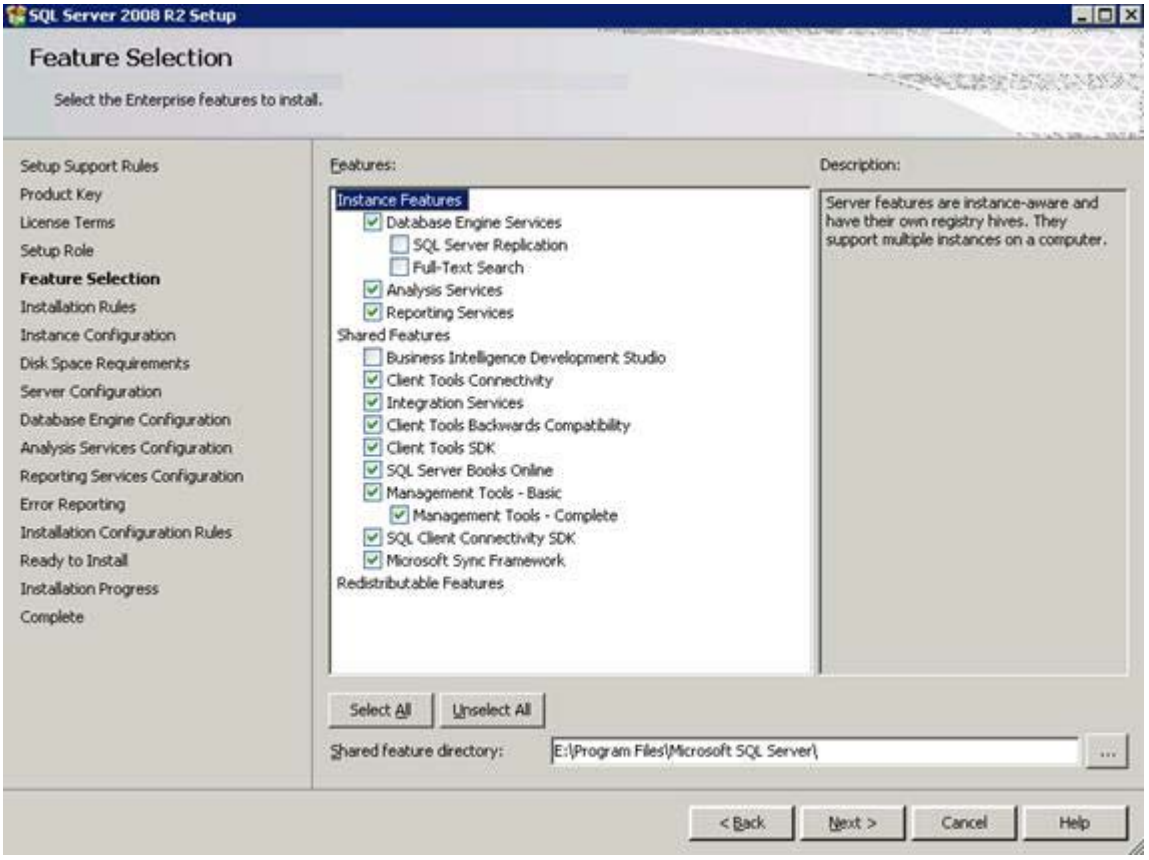


Figure 62. SQL Server Installation Center: Feature Selection

__ 9. The setup starts to run. Click **Next** to continue when it is finished.

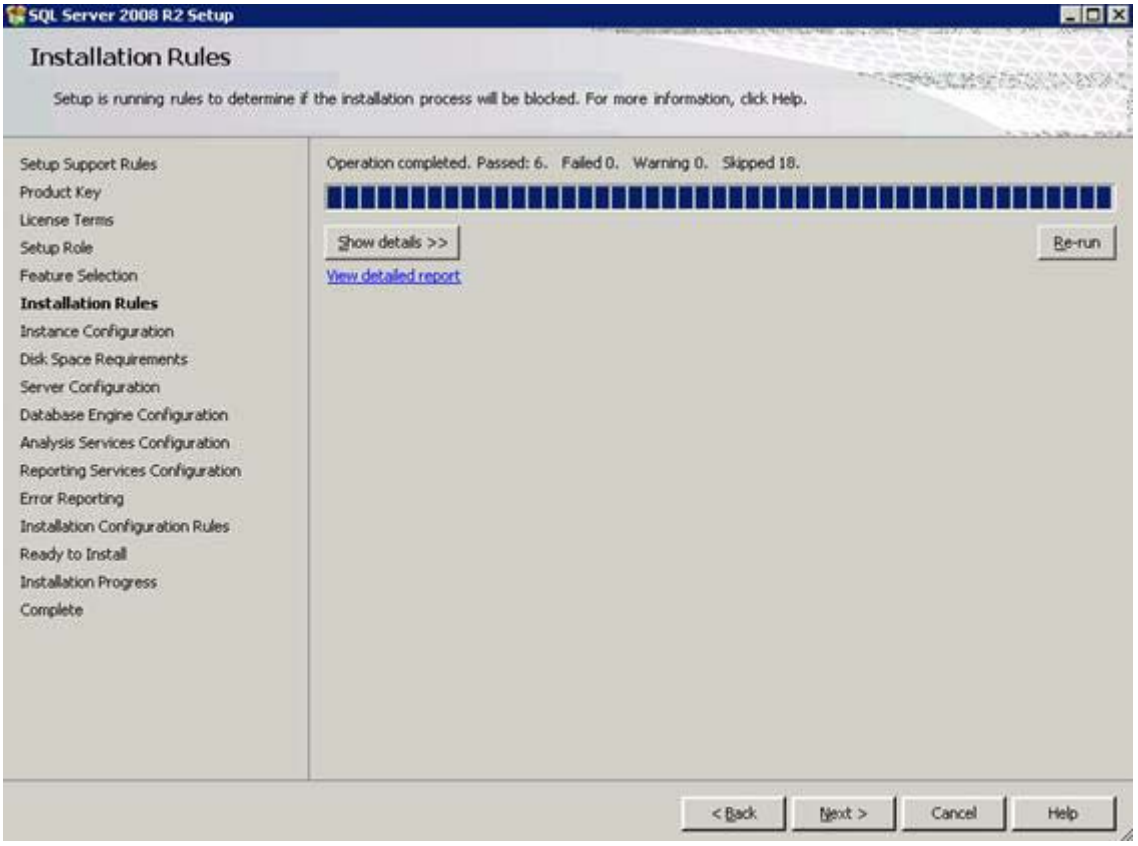


Figure 63. SQL Server Installation Center: Installation Rules

__ 10. Select **Named instance** and enter the name, instance ID (OPNACT is the first database instance: Activities), and the Instance root directory. Then, click **Next** to continue.

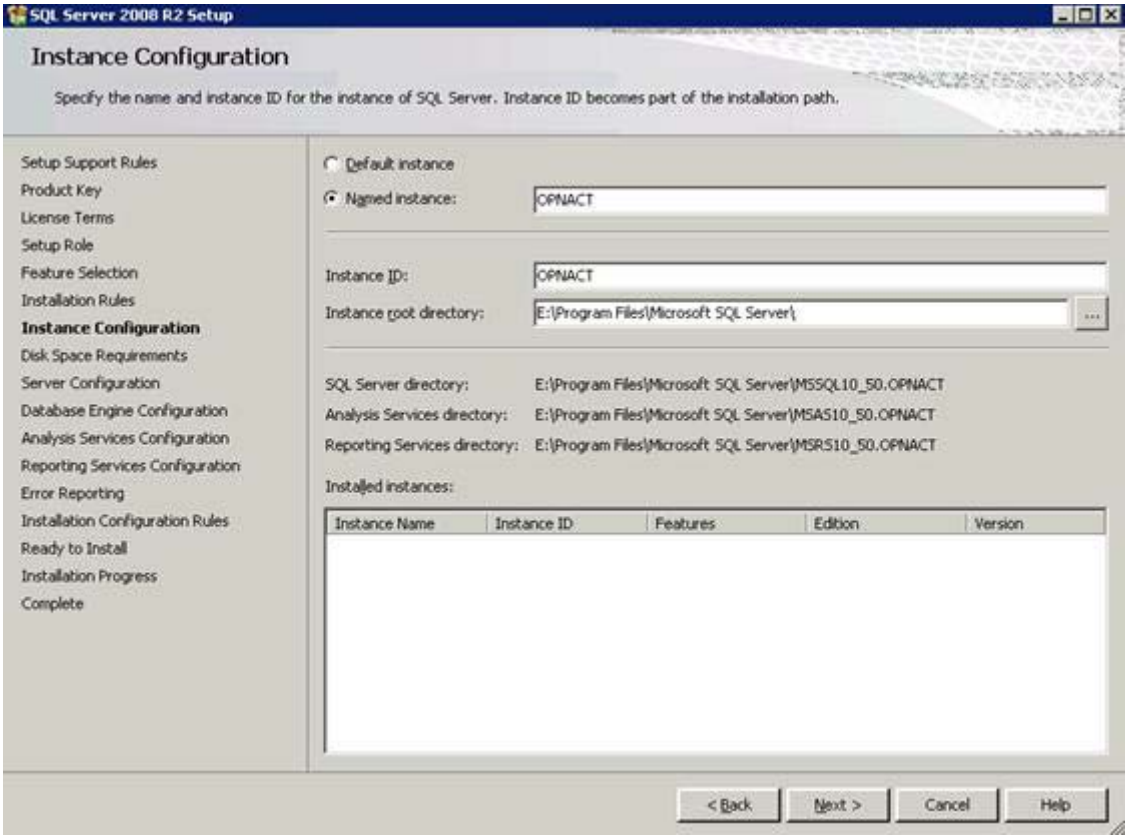


Figure 64. SQL Server Installation Center: Instance Configuration

__ 11. Review the disk space requirements that are needed for the installation. Then, click **Next** to continue.

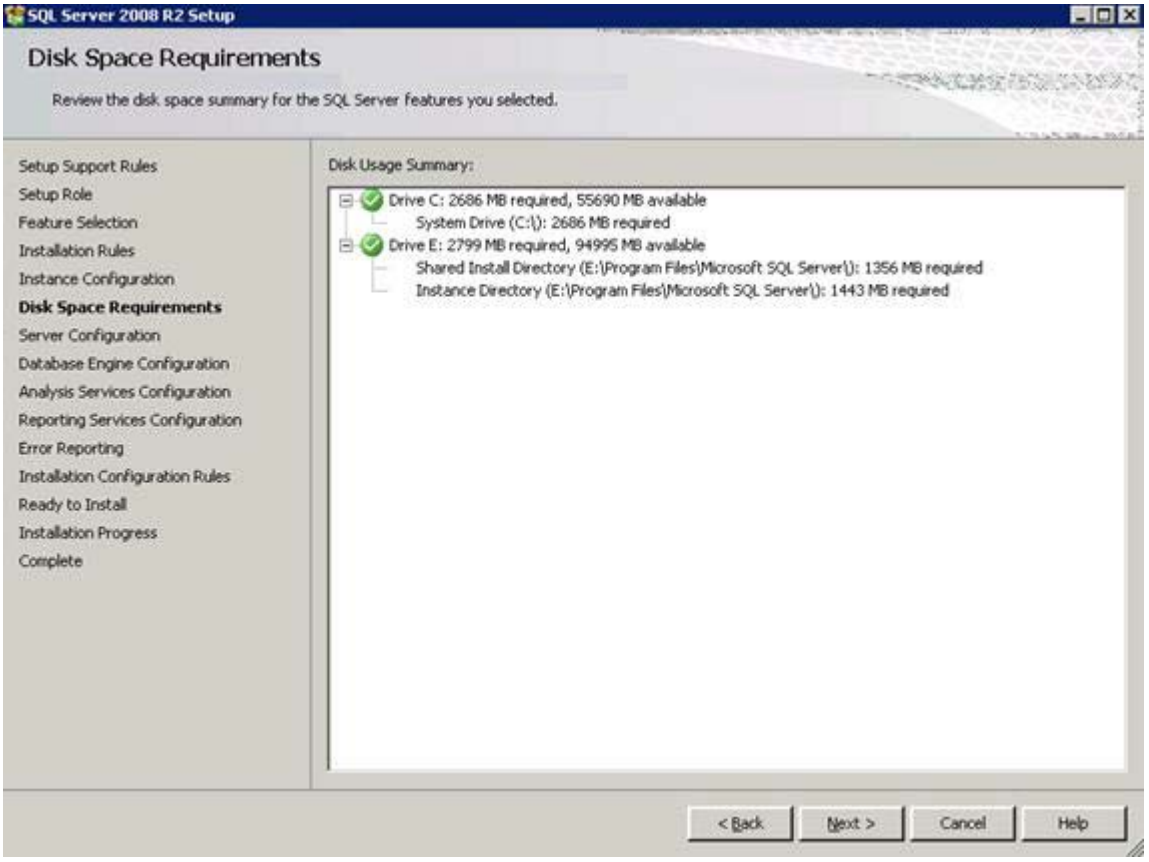


Figure 65. SQL Server Installation Center: Disk Space Requirements

__ 12. Change the Service Account Name to `NT AUTHORITY\SYSTEM` except for the service SQL Server Browser. See the following two screen captures for example.

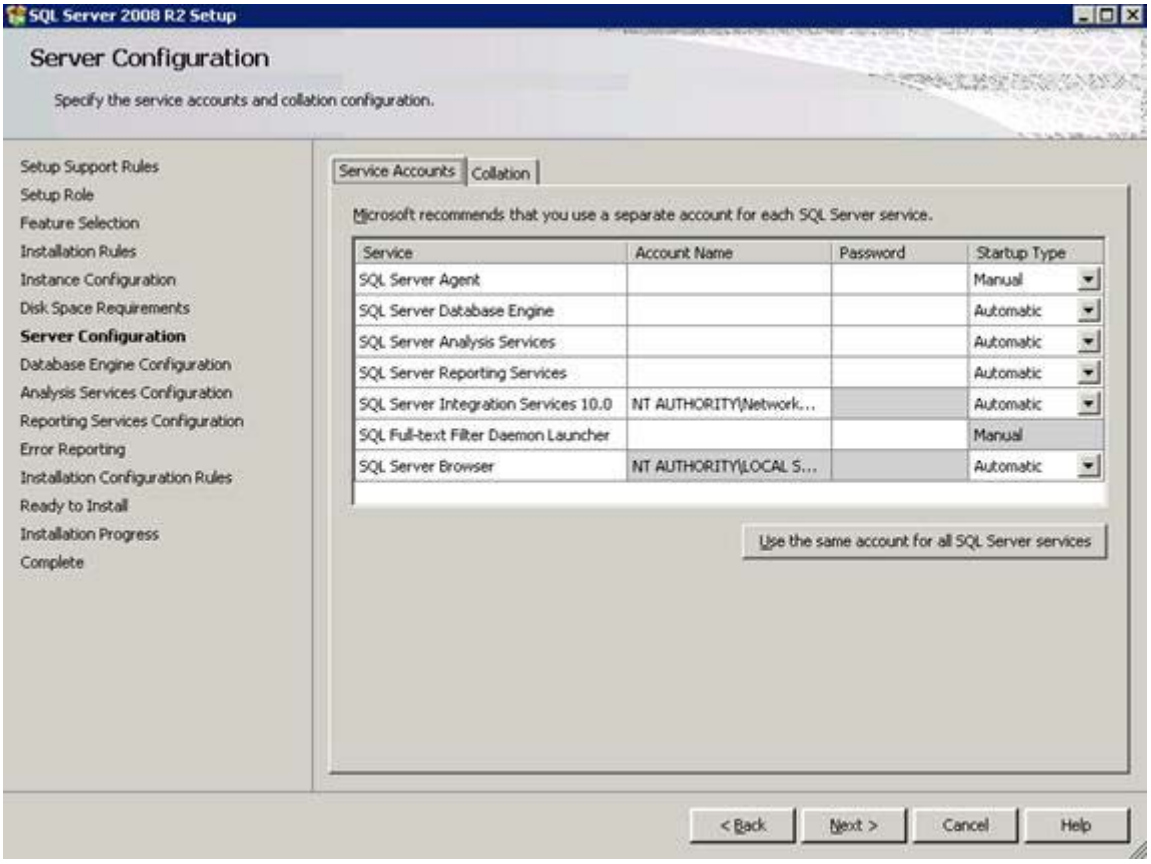


Figure 66. SQL Server Installation Center: Server Configuration (1 of 2)

__ 13. When you changed the Service Account Name, click **Next** to continue.

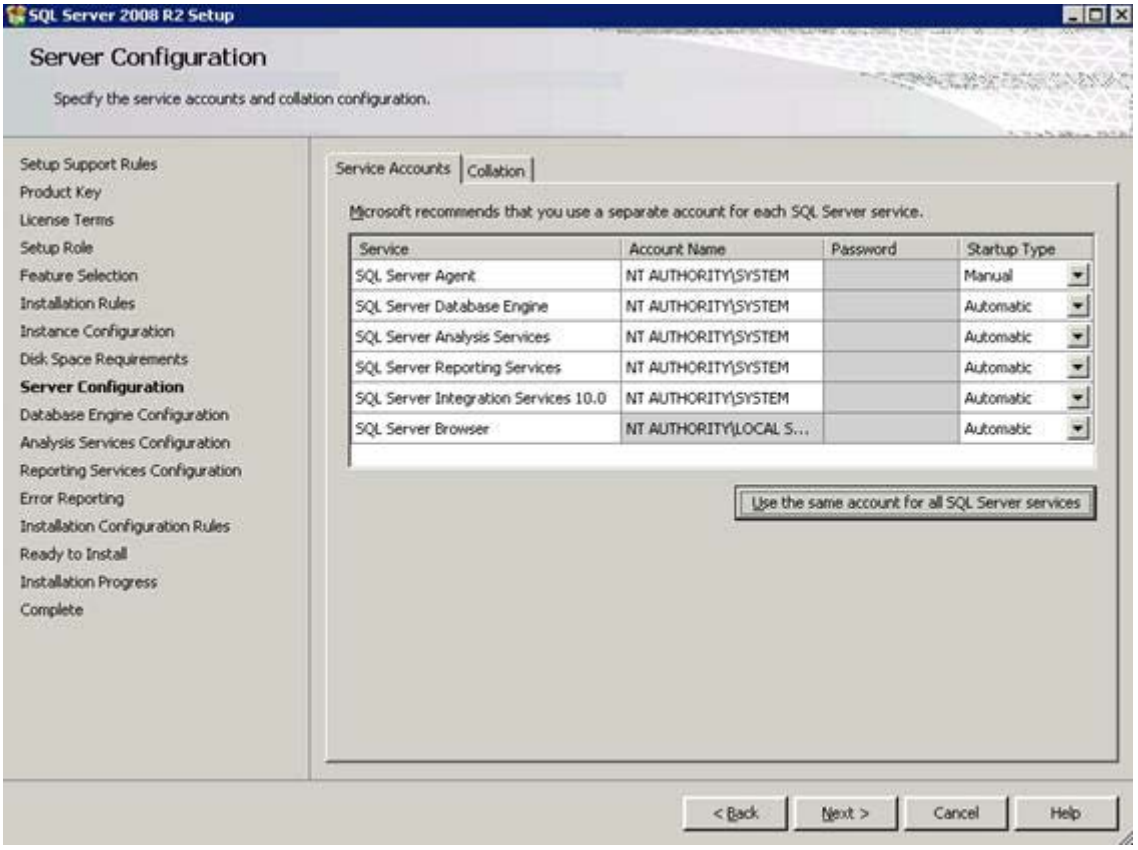


Figure 67. SQL Server Installation Center: Server Configuration (2 of 2)

__ 14. Click the **Collation** tab and click **Customize**. Then, make changes as shown in the following screen and click **OK**.

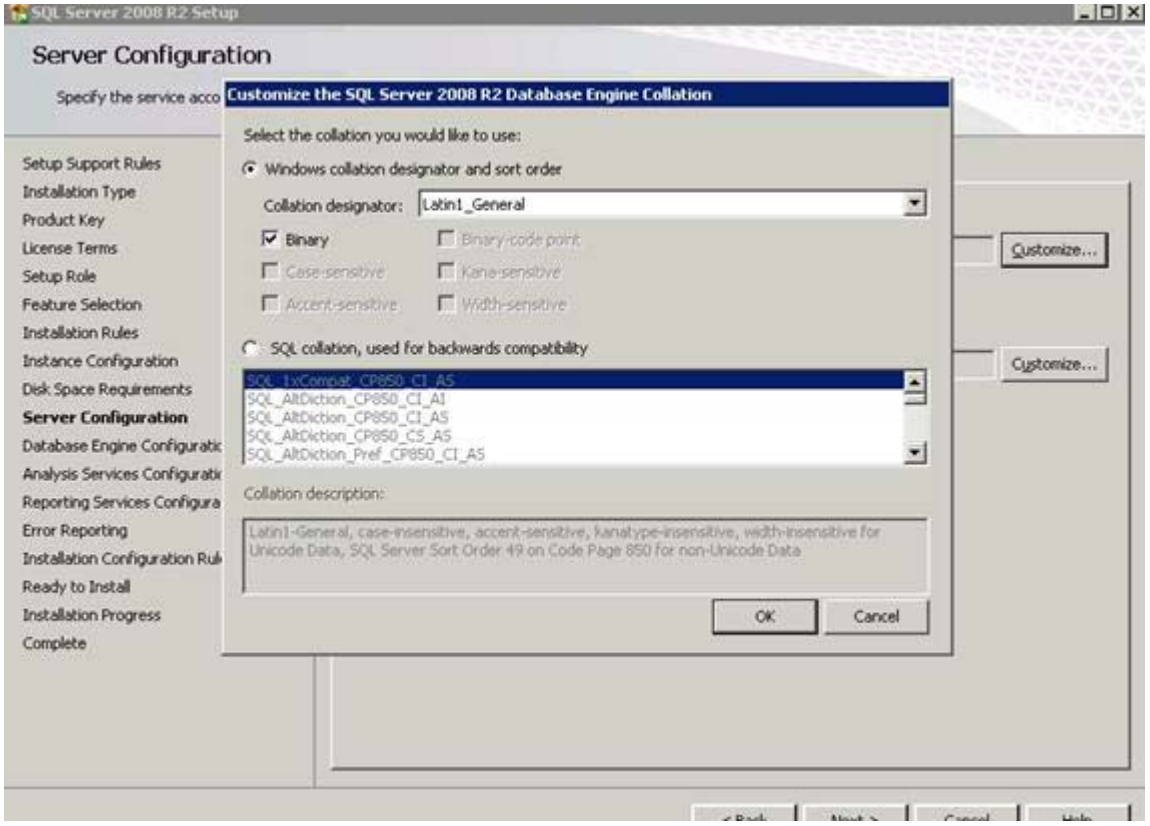


Figure 68. SQL Server Installation Center: Server Configuration: Customize the SQL Server 2008 R2 Database Engine Collation

__ 15. When you applied the changes to the Database Engine and Analysis Services, click **Next** to continue.

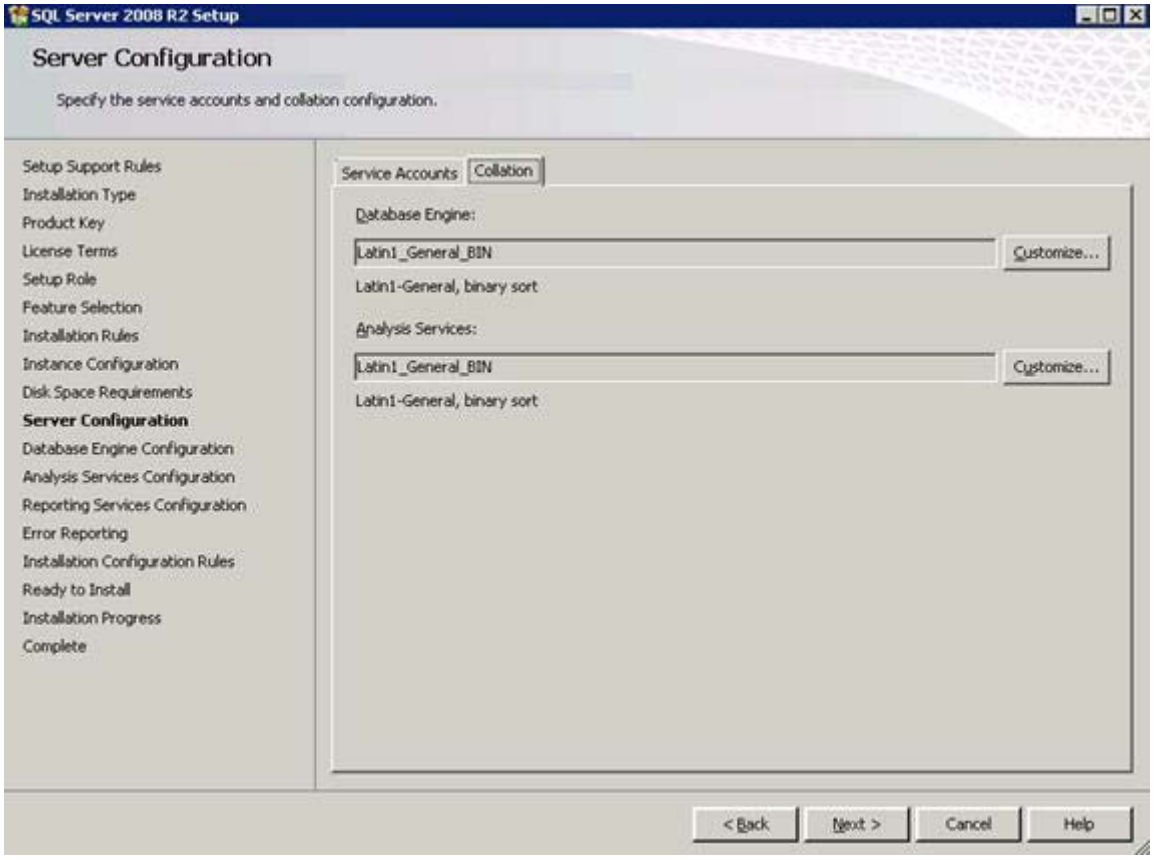


Figure 69. SQL Server Installation Center: Server Configuration: Collation

__ 16. Select **Mixed Mode**, and enter a password. Click **Add Current User** and add the computer administrator as shown in the following figure. Then, click **Next** to continue.

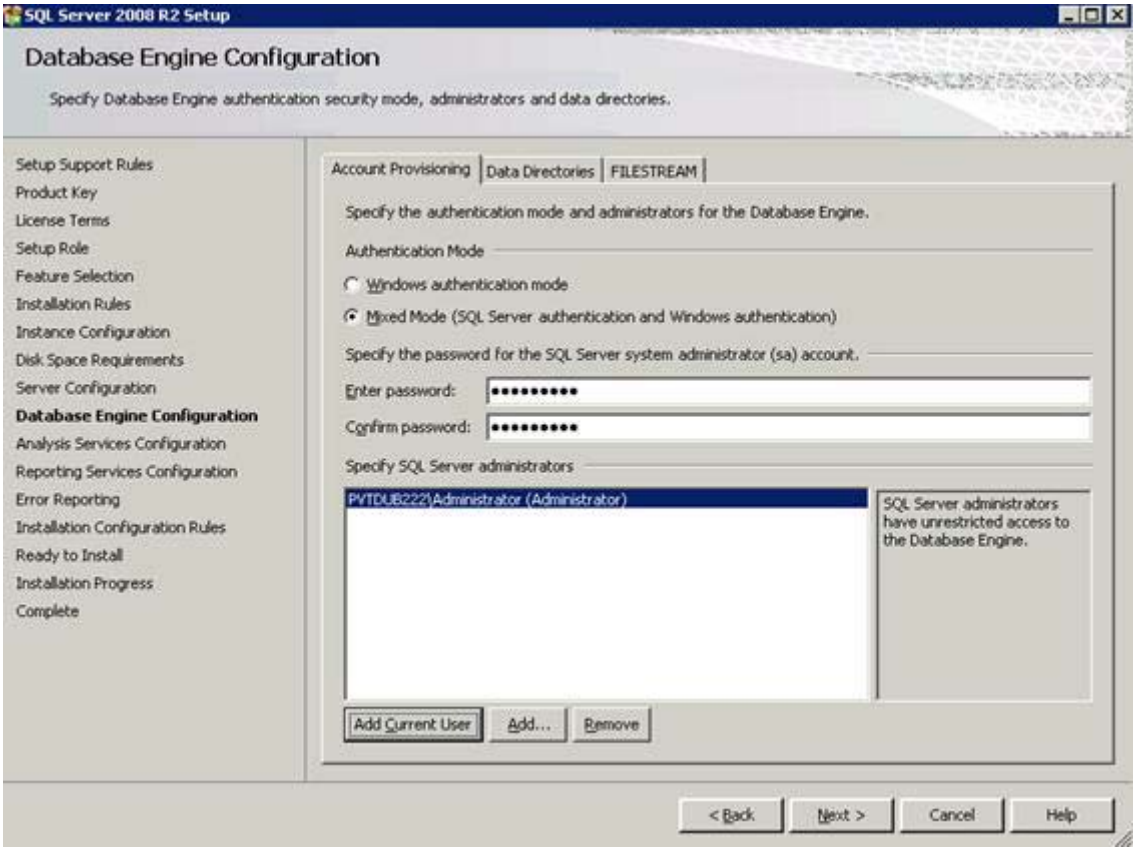


Figure 70. SQL Server Installation Center: Database Engine Configuration

__ 17. Click **Add Current User** and add the computer administrator as shown in the following figure. Then, click **Next** to continue.

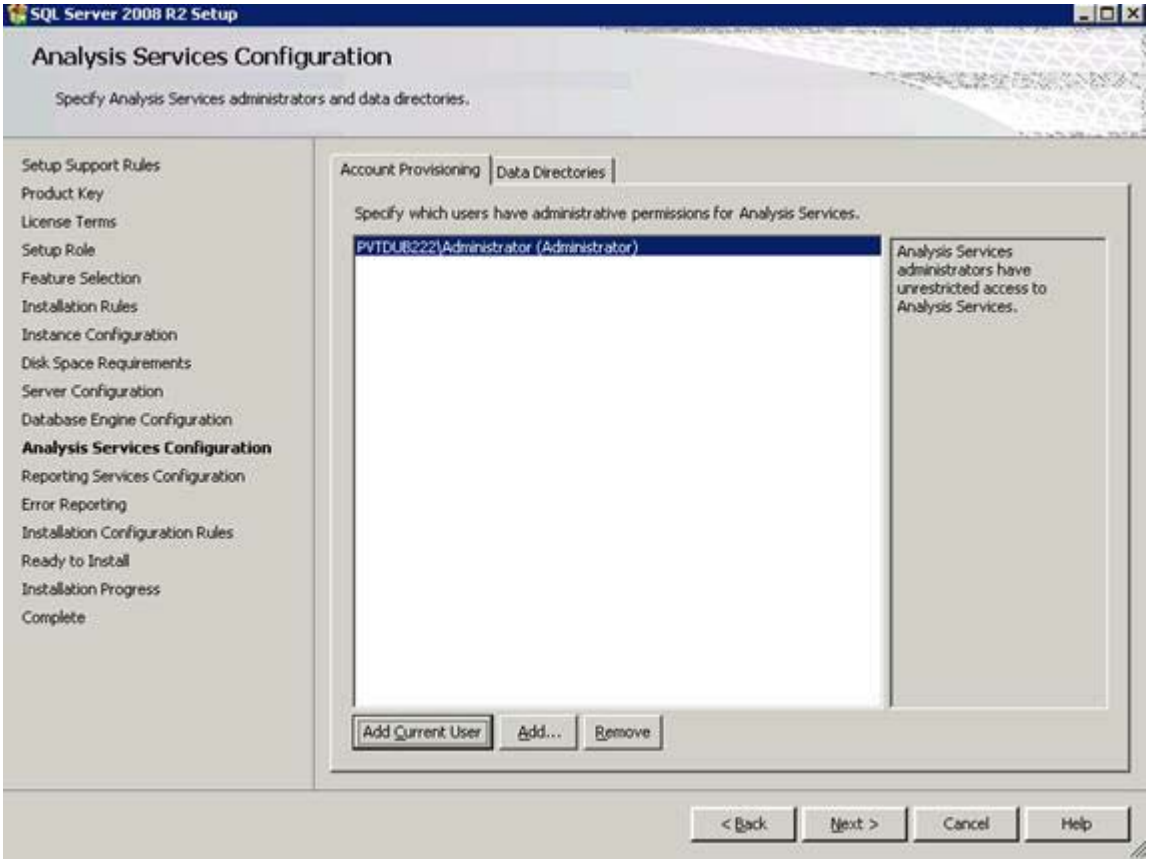


Figure 71. SQL Server Installation Center: Analysis Services Configuration

__ 18. Select **Install the native mode default configuration**, and click **Next** to continue.

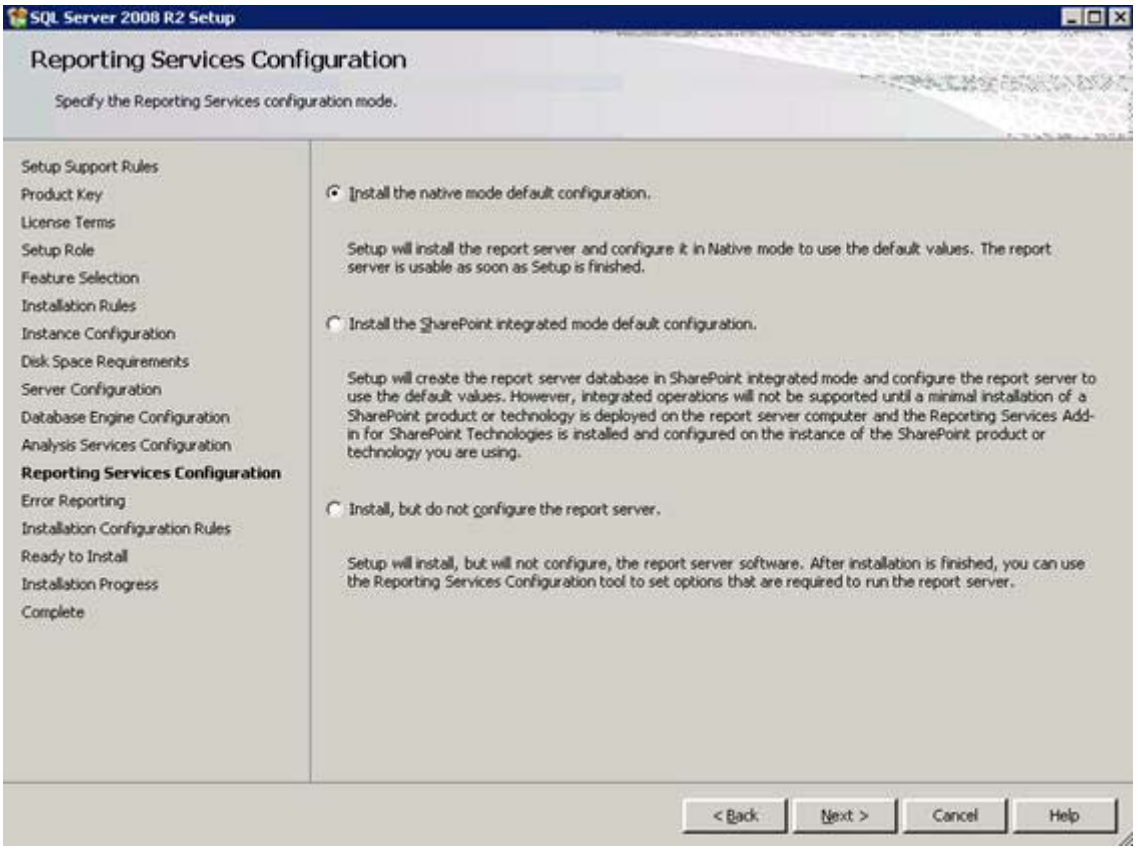


Figure 72. SQL Server Installation Center: Reporting Services Configuration

__ 19. Accept the default and click **Next** to continue.

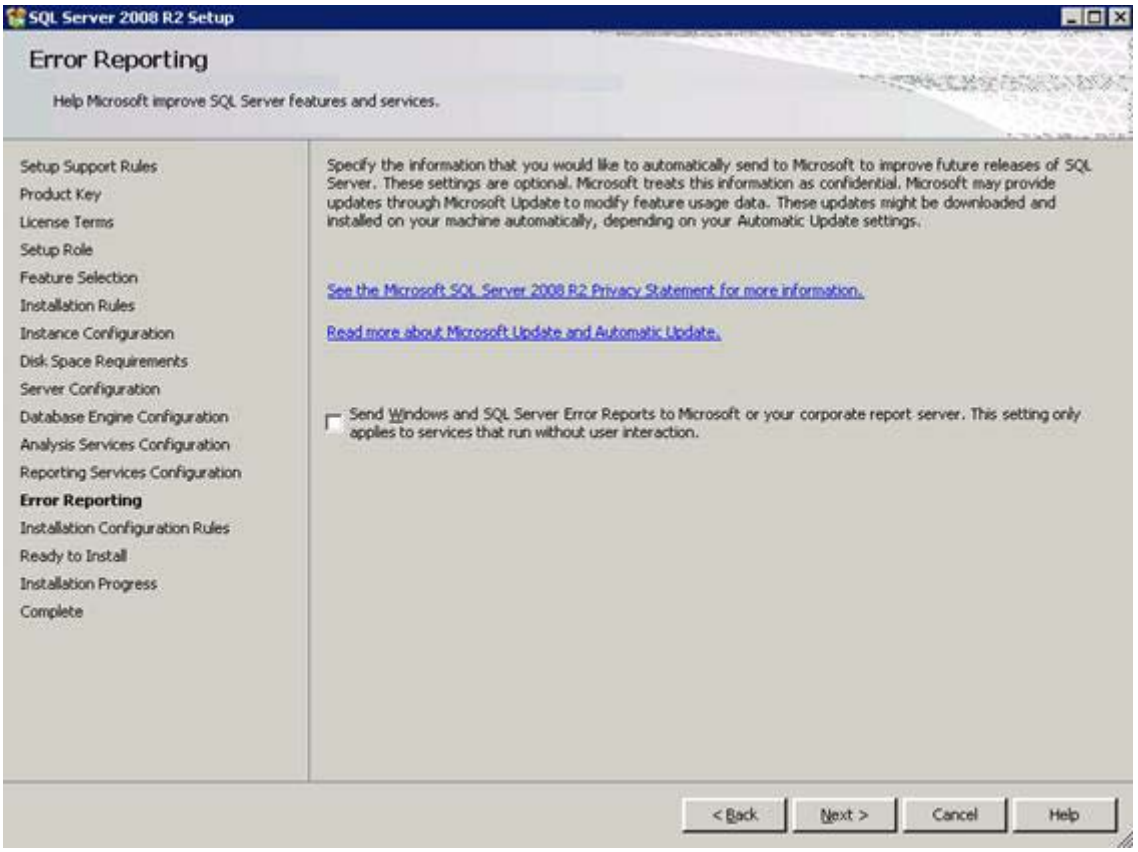


Figure 73. SQL Server Installation Center: Error Reporting

__ 20. When the setup completes, click **Next** to continue.

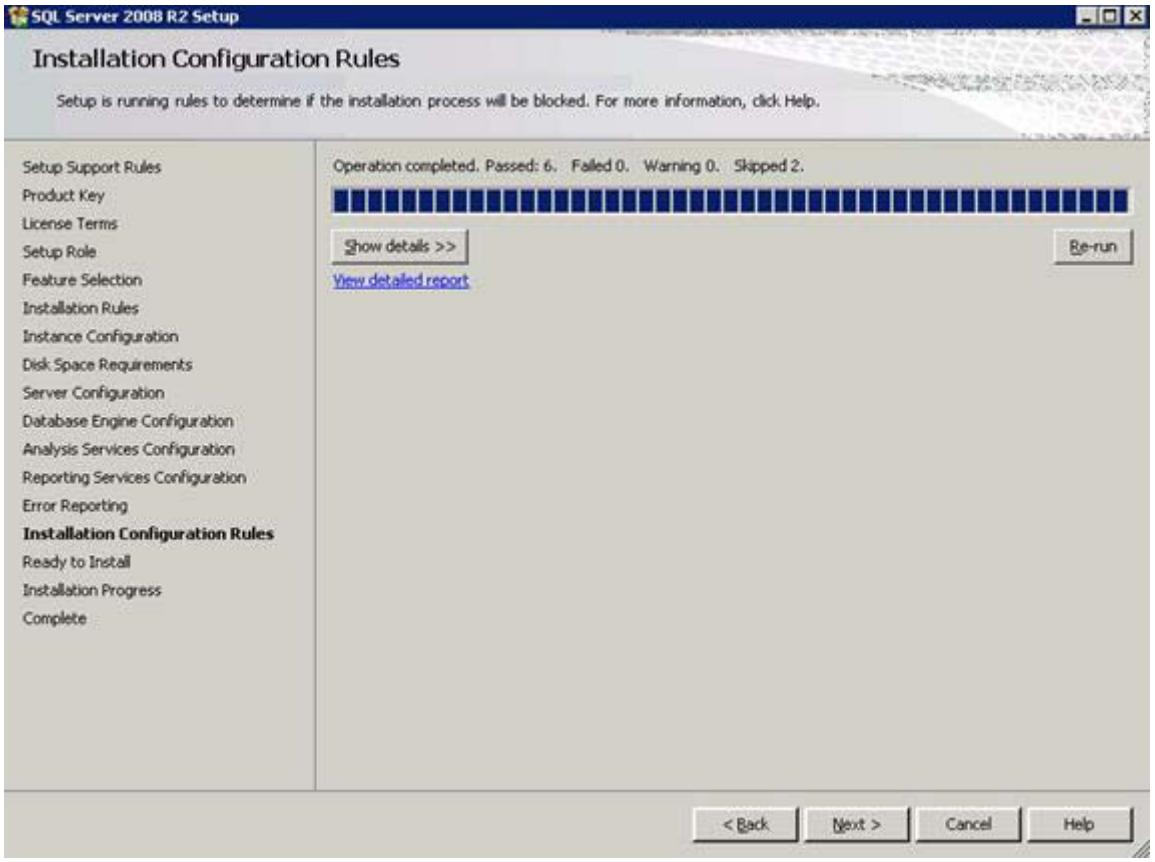


Figure 74. SQL Server Installation Center: Installation Configuration Rules

__ 21. Review the summary, and then click **Install** to start and complete the installation of the MS SQL Server.

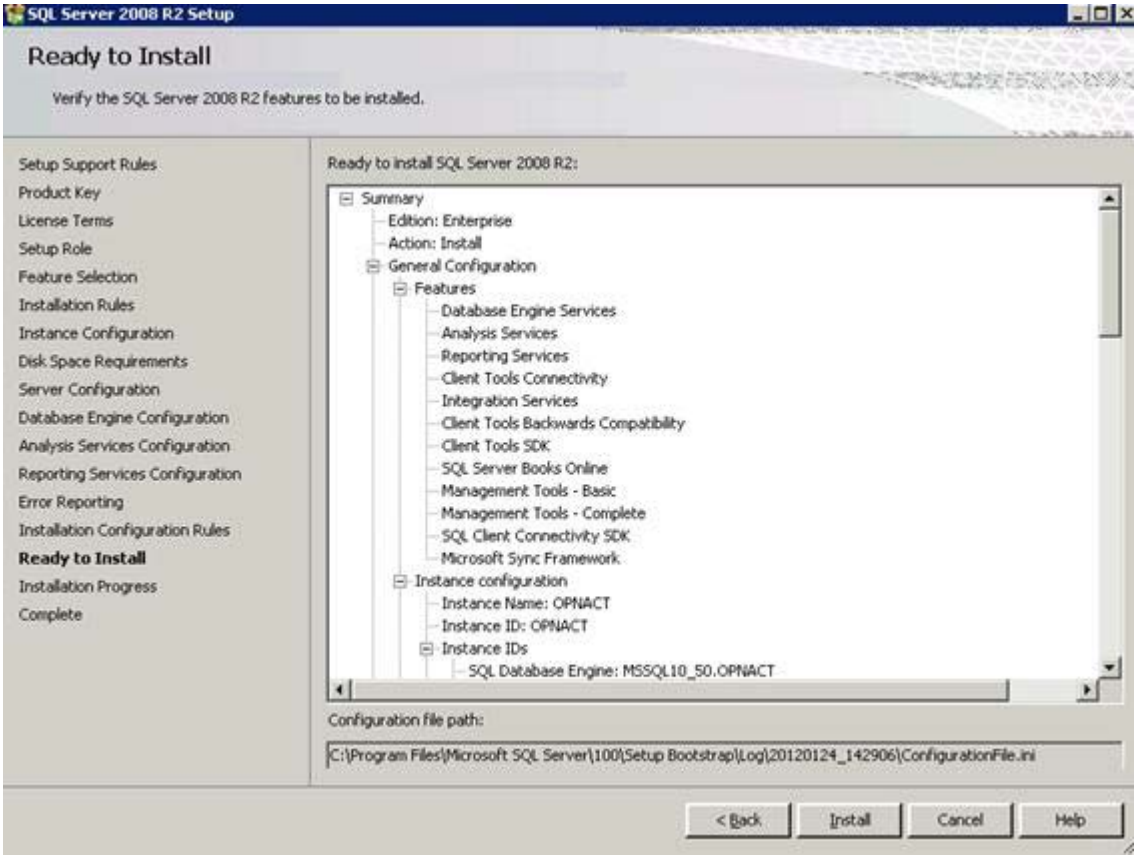


Figure 75. SQL Server Installation Center: Ready to Install

Installing Tivoli Directory Integrator v9.7 fix pack 5

__ 1. In the Tivoli Directory Integrator welcome screen, click **Install IBM Tivoli Directory Integrator**.

Figure 76. Tivoli Directory Integrator: Welcome

__ 2. Click **Tivoli Directory Integrator 7.1 Installer**.

Figure 77. Tivoli Directory Integrator: Starting the product installation

__ 3. The IBM Tivoli Directory Integrator v.7.1 installation wizard opens. Click **OK** to continue.

Figure 78. IBM Tivoli Directory Integrator v.7.1 installation wizard

__ 4. In the introduction screen, click **Next**.

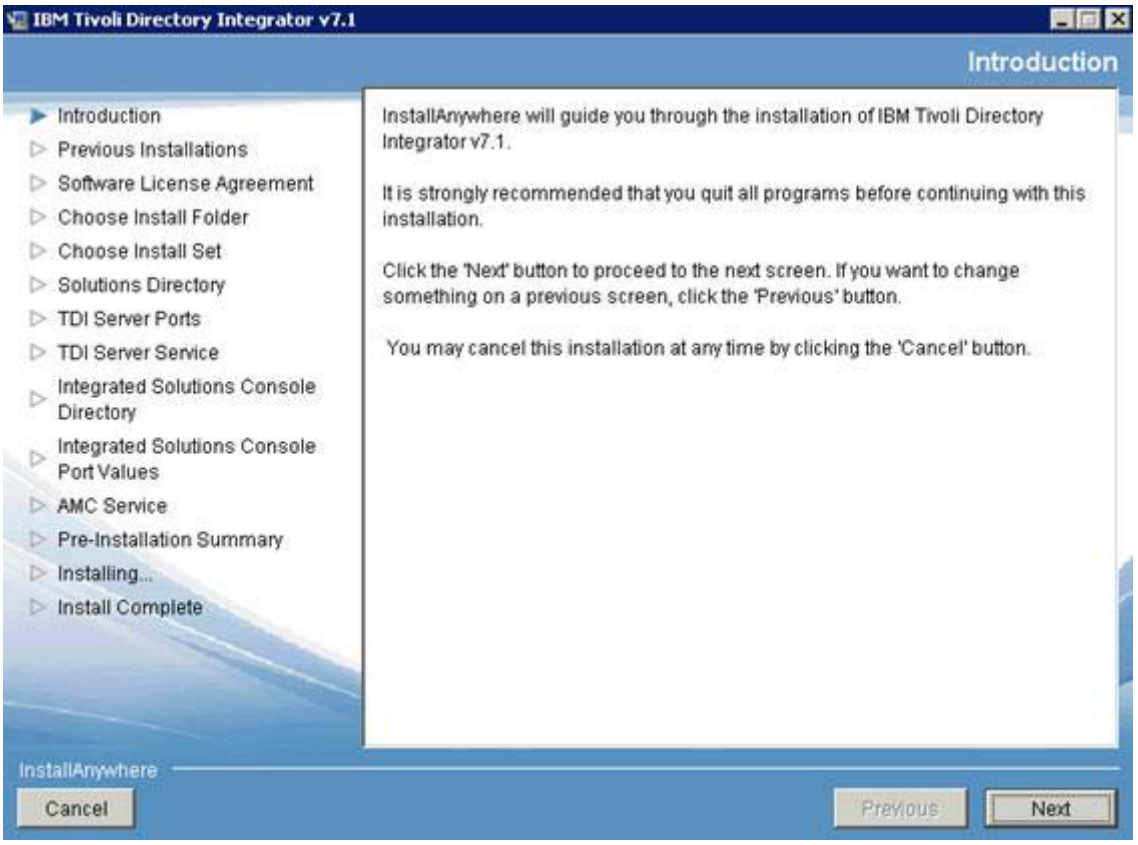


Figure 79. IBM Tivoli Directory Integrator v.7.1: Introduction

__ 5. Click **Next** to search for previous installations.

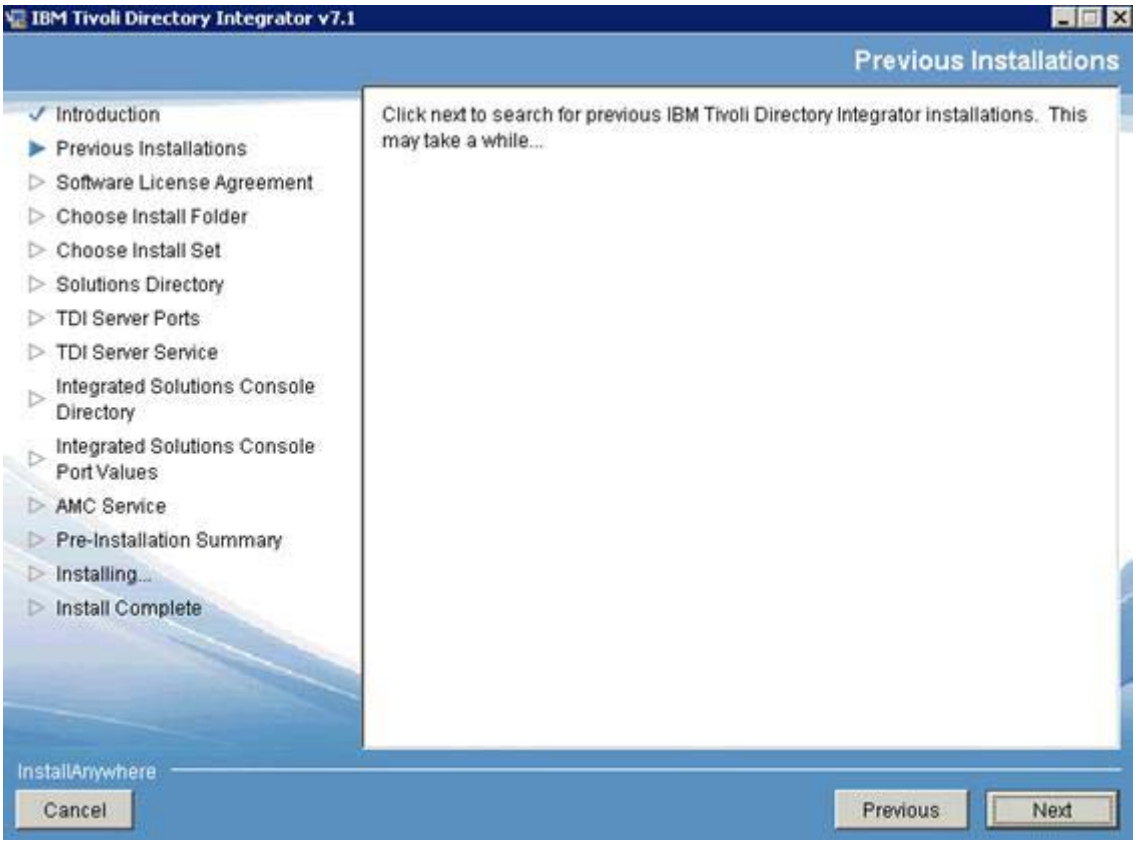


Figure 80. IBM Tivoli Directory Integrator v.7.1: Previous installations

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

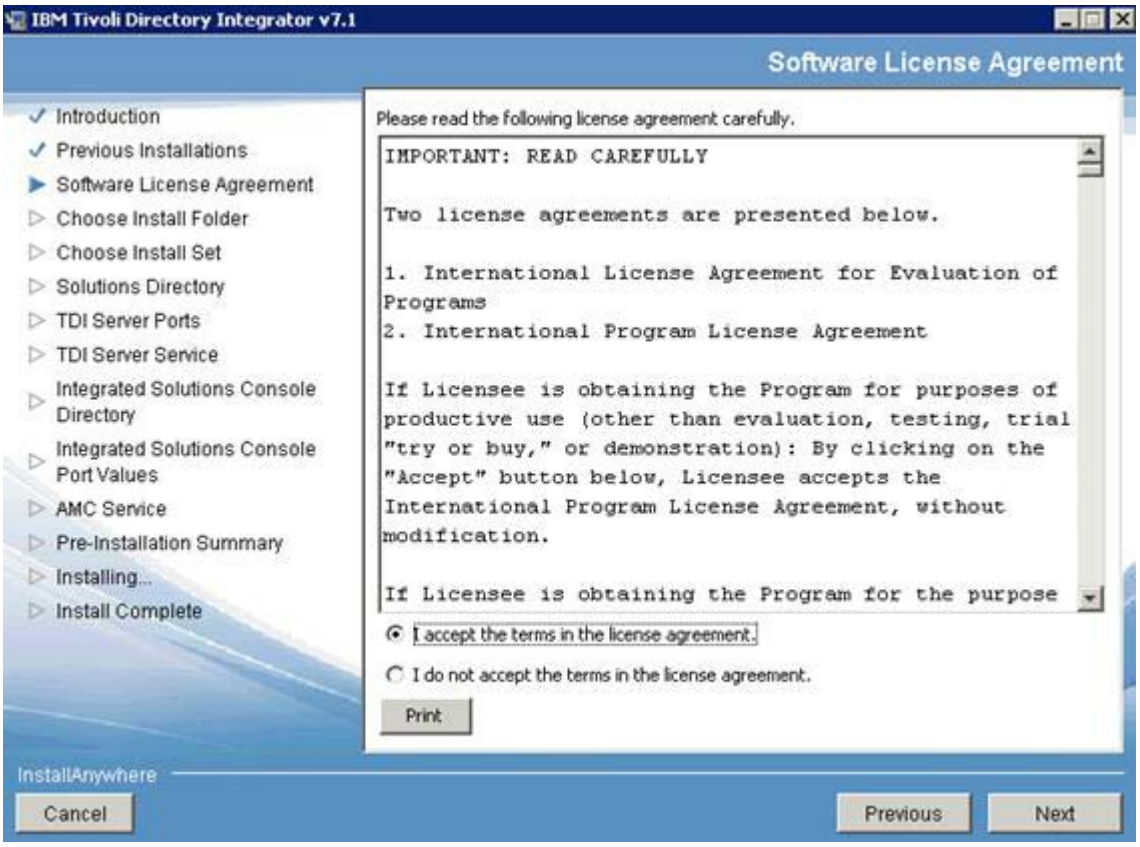


Figure 81. IBM Tivoli Directory Integrator v.7.1: Software License Agreement

__ 7. Select where you want to save install the product and click **Next**.

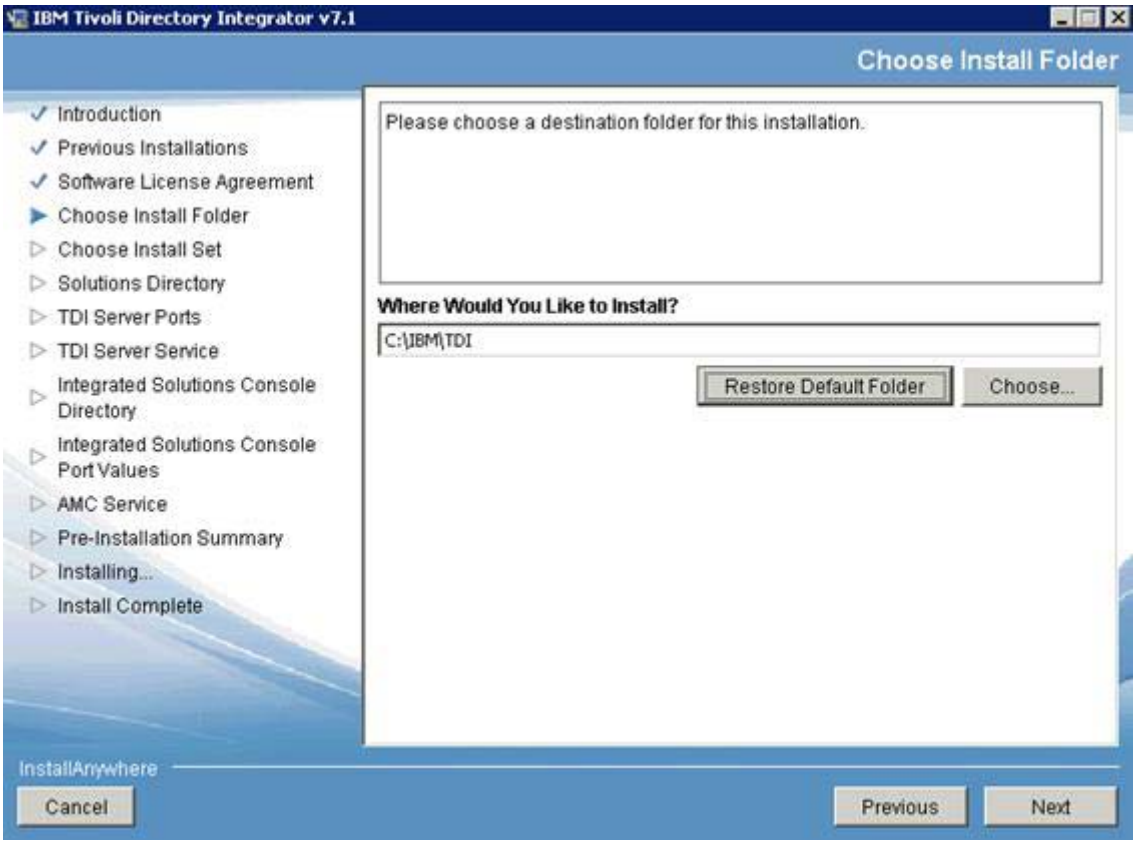


Figure 82. IBM Tivoli Directory Integrator v.7.1: Choose Install Folder

__ 8. Select **Typical** as installation method and click **Next**.

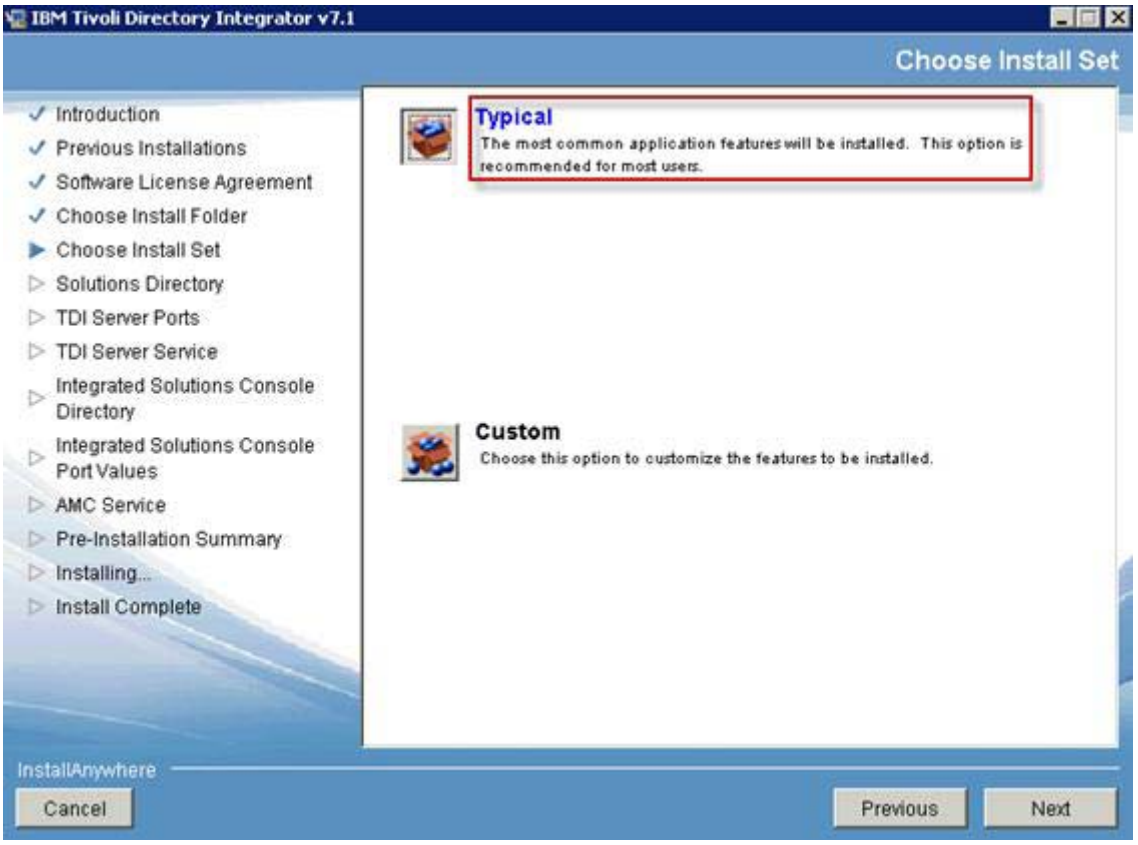


Figure 83. IBM Tivoli Directory Integrator v.7.1: Choose Install Set

__ 9. Do not specify a solutions directory and click **Next**.

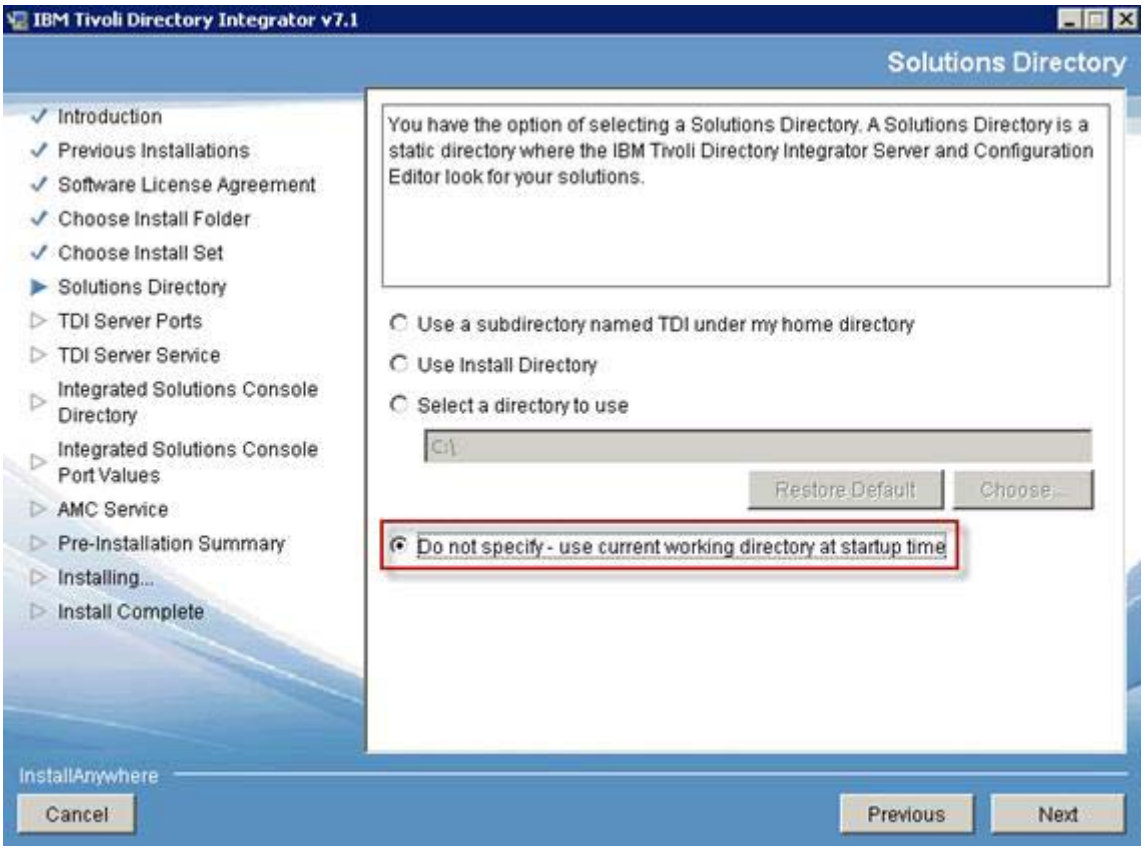


Figure 84. IBM Tivoli Directory Integrator v.7.1: Solutions Directory

__ 10. Enter the port values and click **Next**.

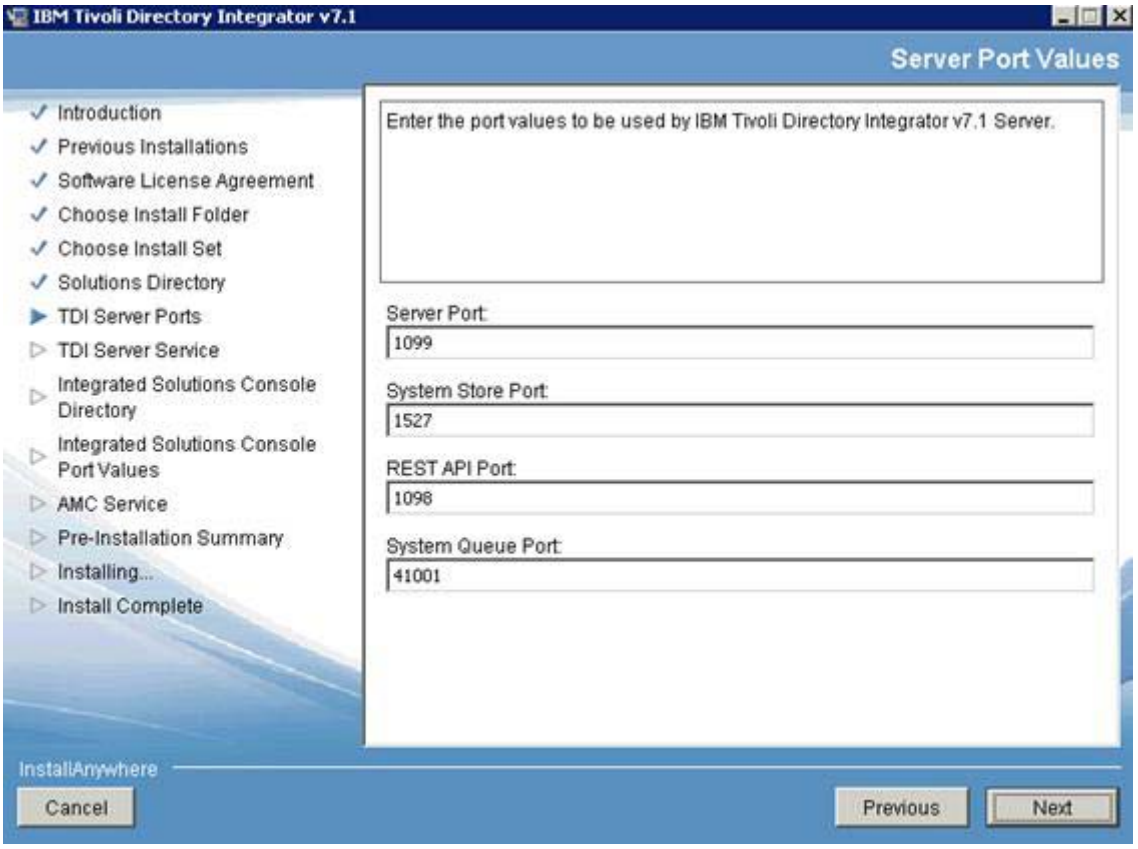


Figure 85. IBM Tivoli Directory Integrator v.7.1: Server Port Values

__ 11. Leave the “Register as a system service” option as default and click **Next**.

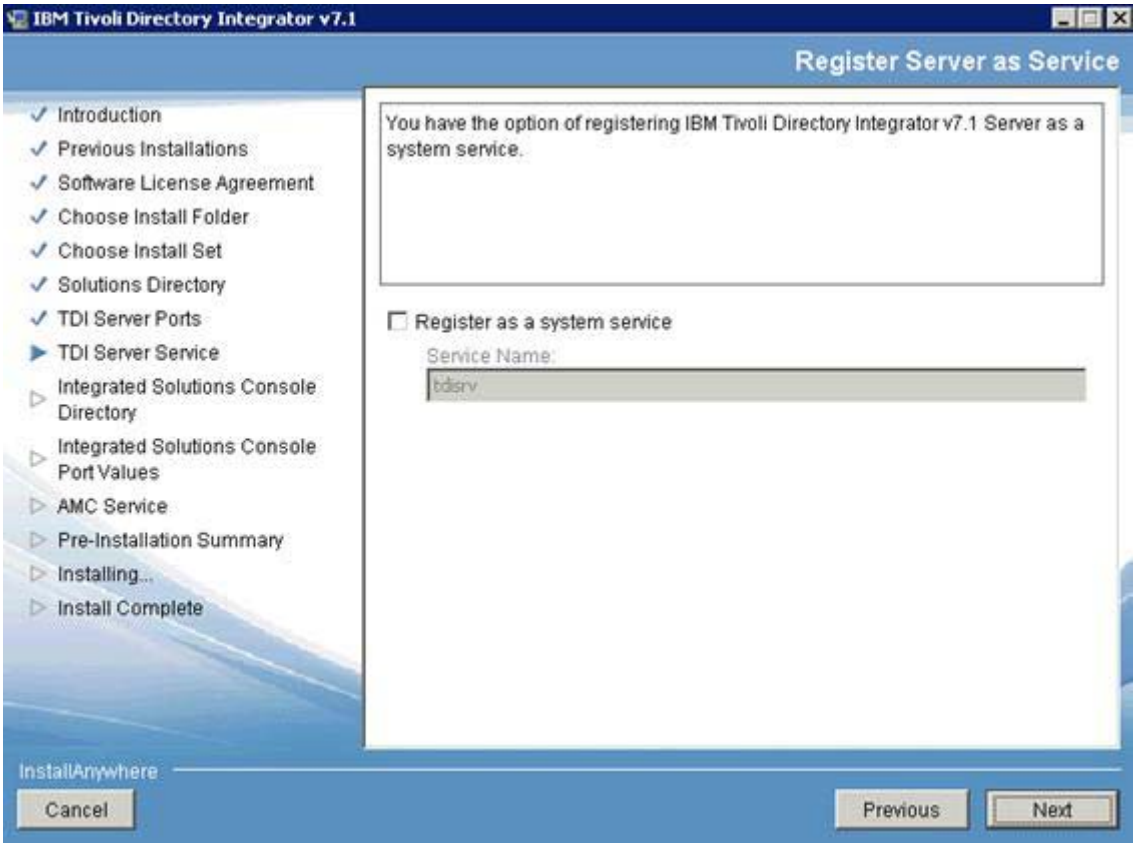


Figure 86. IBM Tivoli Directory Integrator v.7.1: Register Server as a Service

__ 12. Enter the port values to use in the Integrated Solutions Console and click **Next**.

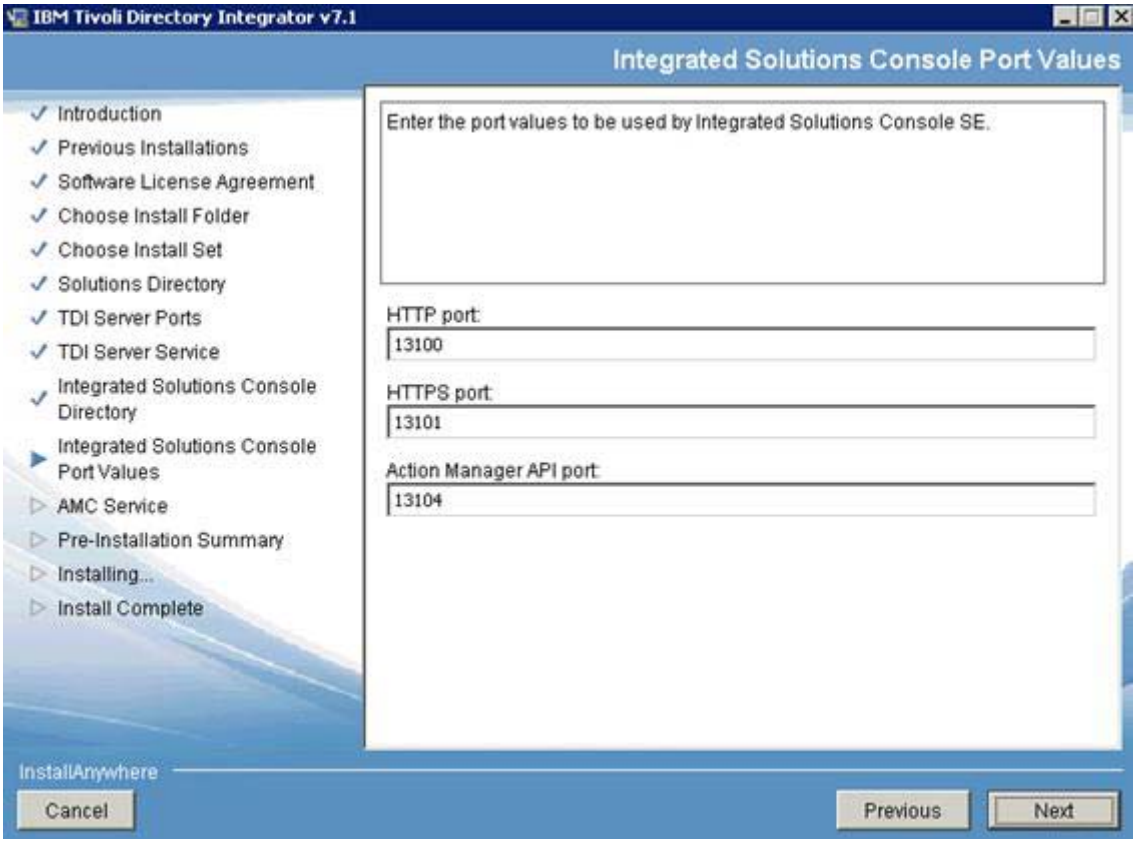


Figure 87. IBM Tivoli Directory Integrator v.7.1: Integrated Solutions Console Port Values

__ 13. Leave the “Register as a system service” option as default and click **Next**.

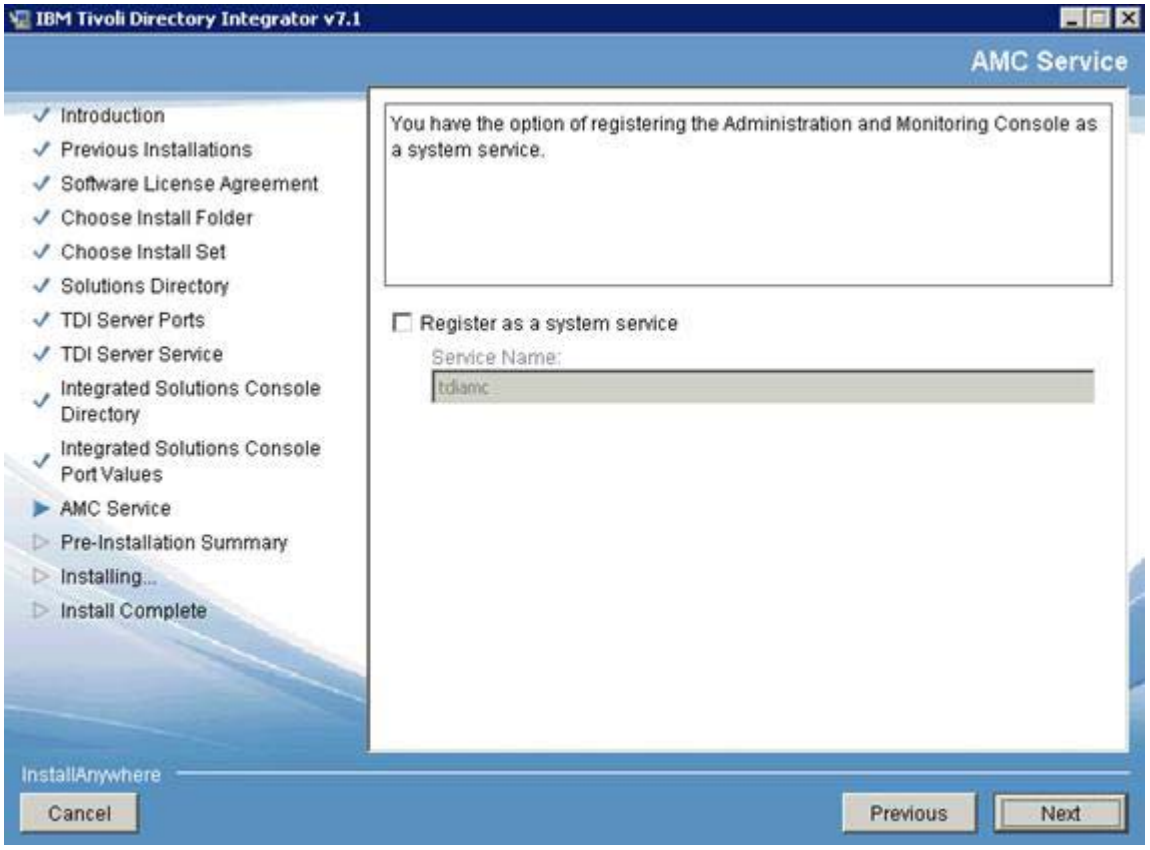


Figure 88. IBM Tivoli Directory Integrator v.7.1: AMC Service

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

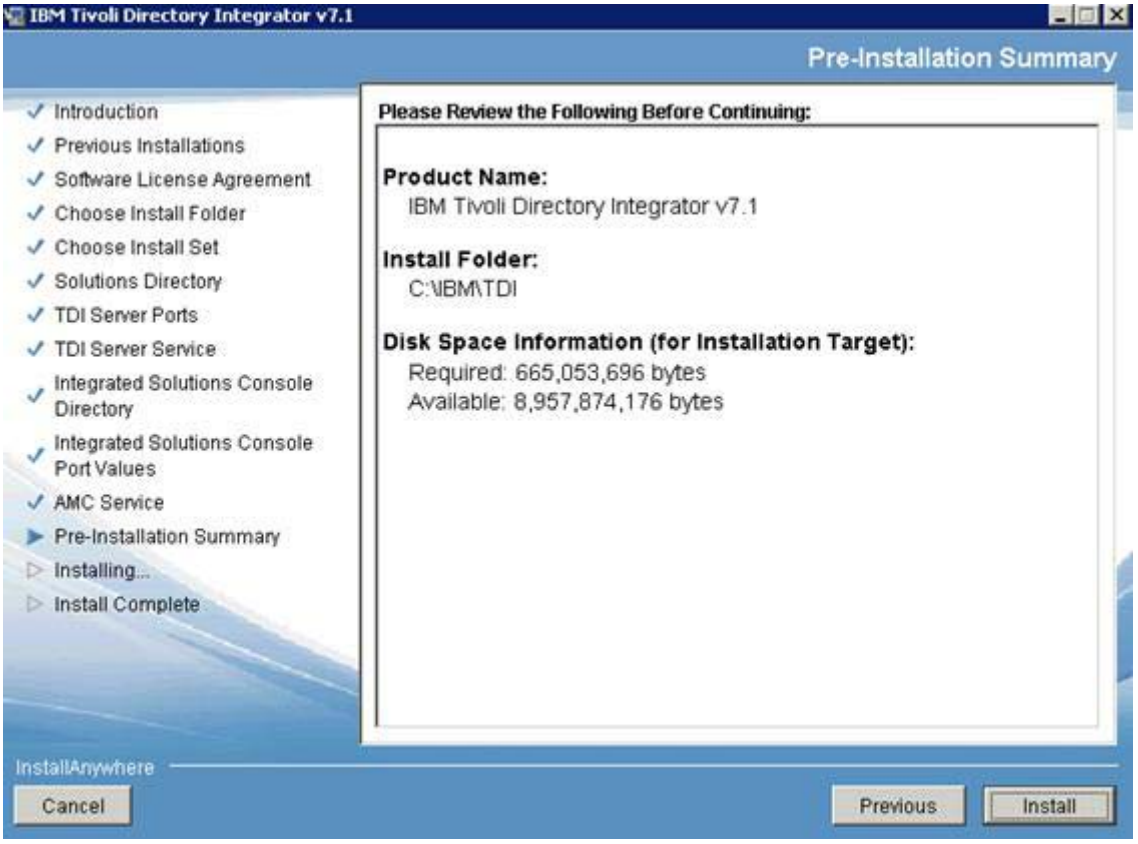


Figure 89. IBM Tivoli Directory Integrator v.7.1: Pre-installation Summary

The integrator installation begins.

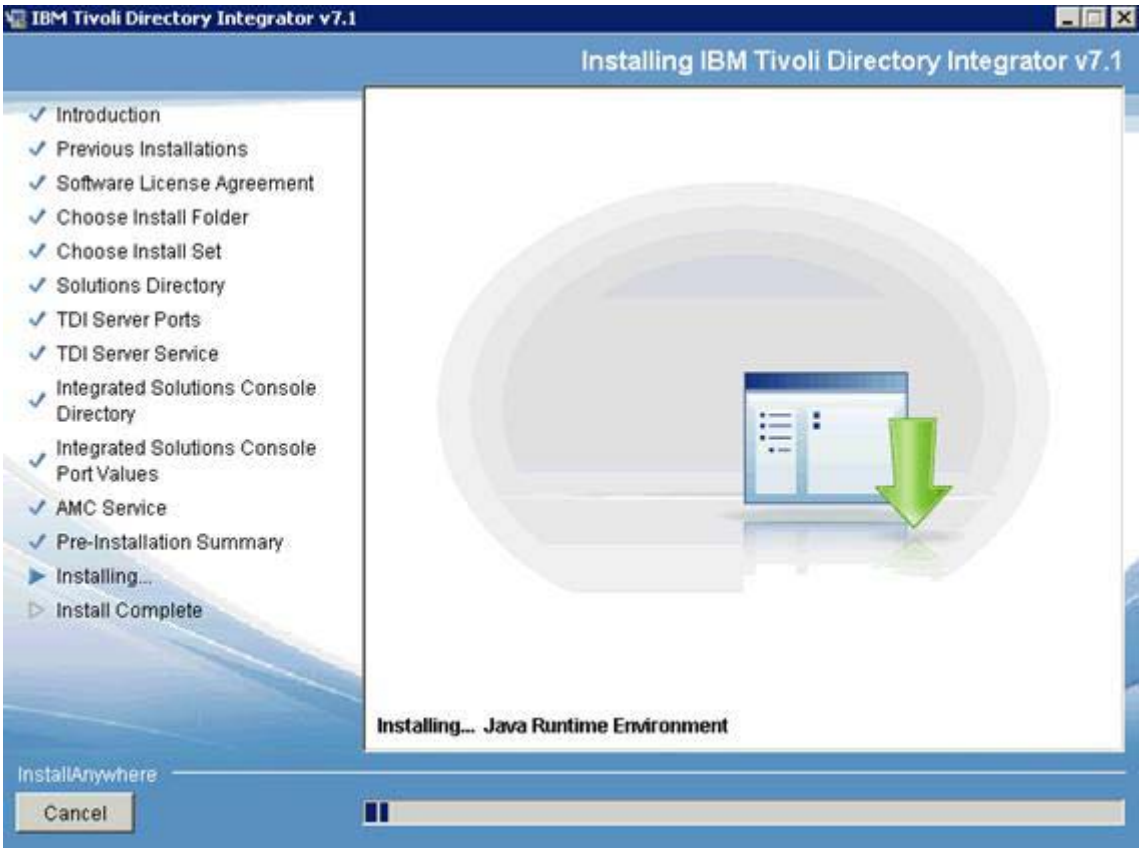


Figure 90. IBM Tivoli Directory Integrator v.7.1: Installing IBM Tivoli Directory Integrator v7.1

__ 15. When the installation finishes, click **Done** to quit the installer.

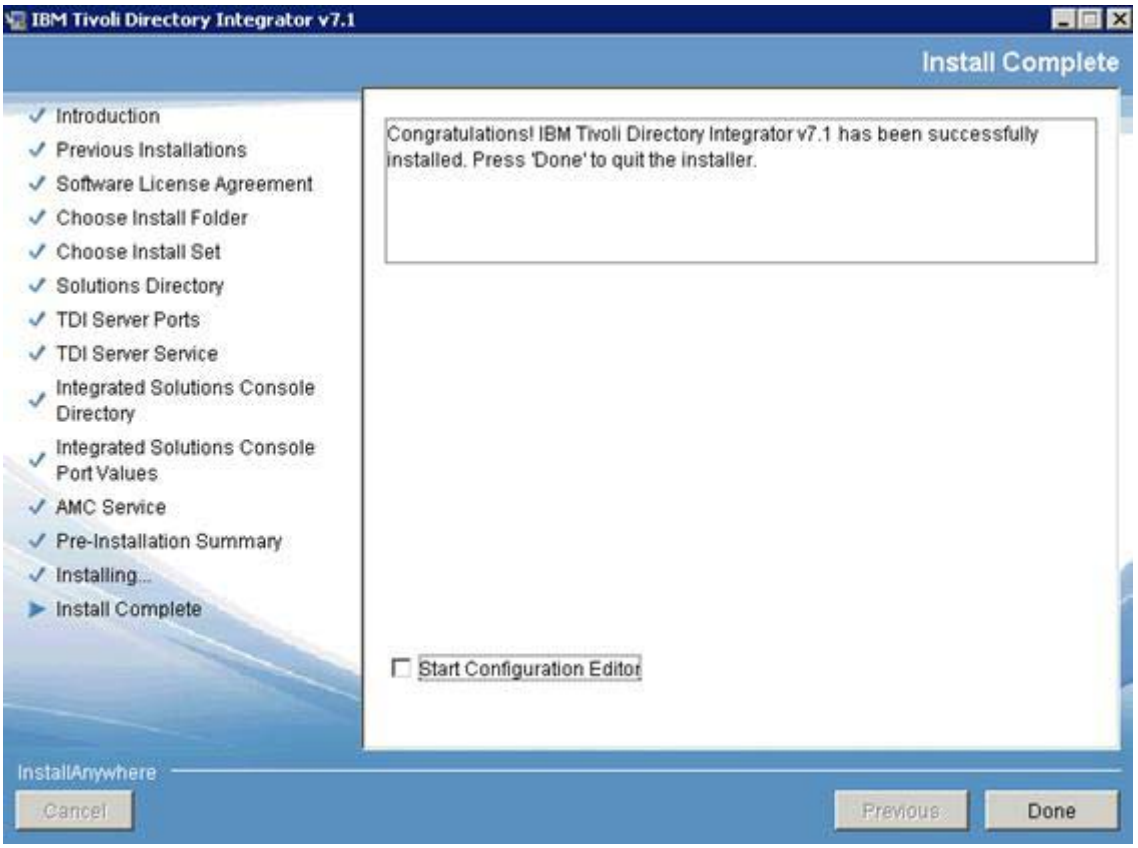


Figure 91. IBM Tivoli Directory Integrator v.7.1: Installation Complete

Apply fix pack 5 to Tivoli Directory Integrator

__ 1. Extract the file `7.0.0-TIV-TDI-FP0005.zip`. This creates a folder with the same name (in this example, it is extracted in `C:\`). In this directory, locate the `.jar` file, `UpdateInstaller.jar`.

__ 2. Copy this file and paste it into the directory `C:\IBM\TDI\V7.0\maintenance`, replacing the existing file with the same name.

__ 3. Go in the directory `C:\IBM\TDI\V7.0\bin`, and run the command `applyUpdates.bat -update C:\7.0.0-TIV-TDI-FP0005\TDI-7.0-FP0005.zip` as follows:

```
C:\IBM\TDI\bin>applyUpdates.bat -update C:\Users\Administrator\Downloads\7.1.0-T
IV-TDI-FP0005\7.1.0-TIV-TDI-FP0005\TDI-7.1-FP0005.zip
CTGDK0023I Applying fix 'TDI-7.1-FP0005' using backup directory 'C:\IBM\TDI\main
tenance\BACKUP/TDI-7.1-FP0005'.
CTGDK0027I Updating SERVER.
CTGDK0027I Updating CE.
CTGDK0027I Updating EXAMPLES.

C:\IBM\TDI\bin>applyUpdates.bat -queryreg
Information from .registry file in: C:\IBM\TDI
Edition: Identity
Level: 7.1.0.5
License: None

Fixes Applied
=-=-=-=-=-=-=
TDI-7.1-FP0005(7.1.0.0)

Components Installed
=-=-=-=-=-=-=-=-=-=-=
BASE
SERVER
   -TDI-7.1-FP0005
CE
   -TDI-7.1-FP0005
JAVADOCS
EXAMPLES
   -TDI-7.1-FP0005
EMBEDDED WEB PLATFORM
AMC
   Deferred: false


C:\IBM\TDI\bin>_
```

Figure 92. Command applyUpdates.bat

Creating Connections databases on MS SQL Server

__ 1. Copy the `Lotus_Connections_4.0_wizards_win.exe` to your computer and extract it.

__ 2. Then, go into the Wizard folder and run `dbWizard.bat`. The following result is shown. Select **Next** to continue.

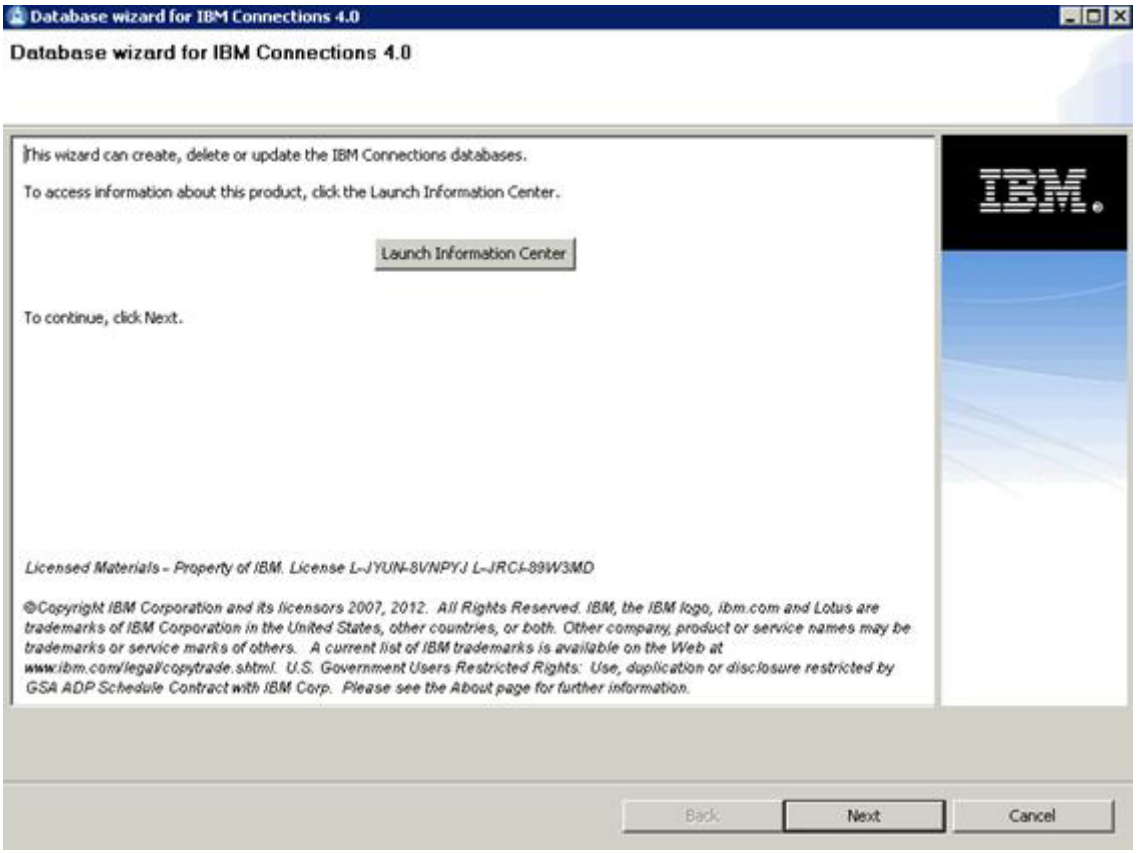


Figure 93. Database wizard for IBM Connections 4.0

__ 3. Choose whether to create, delete, or upgrade. Select **Create** and click **Next** to continue.

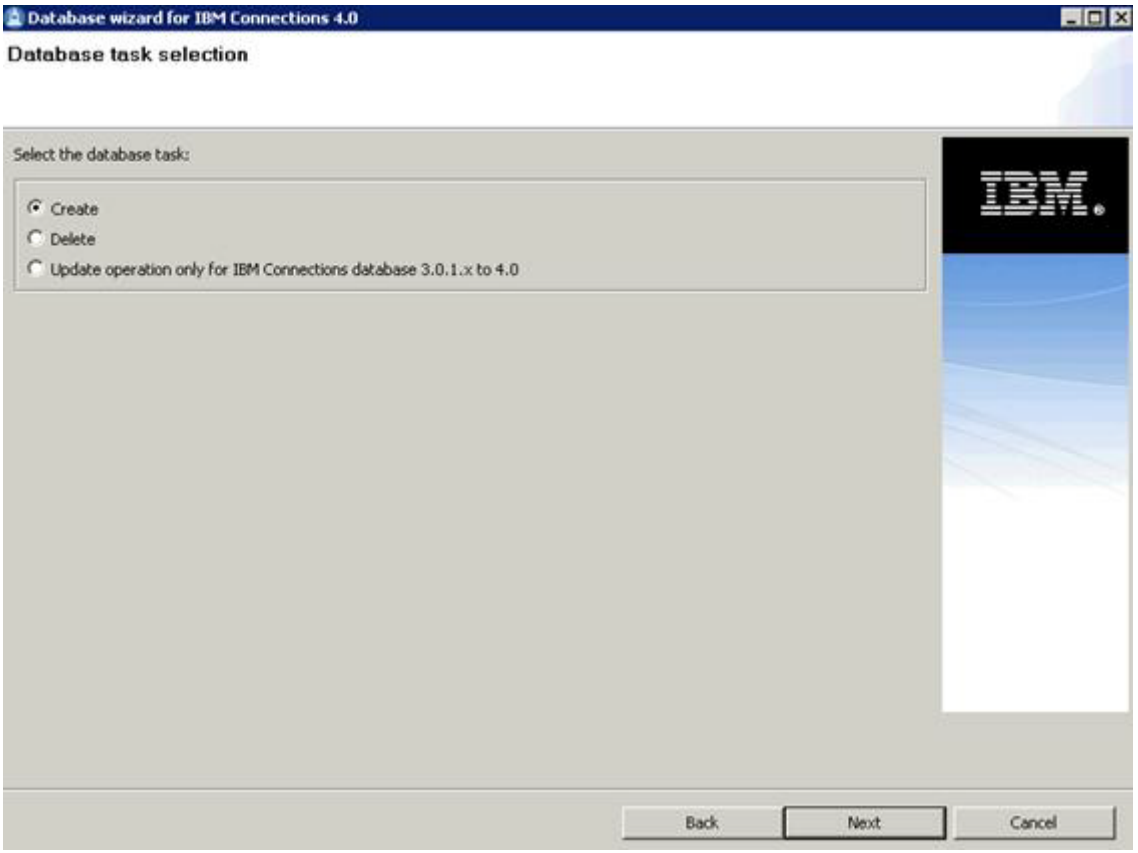


Figure 94. Database wizard for IBM Connections 4.0: Database task selection

__ 4. Select the path for the database installation location, and the database instance name. Click **Next** to continue.

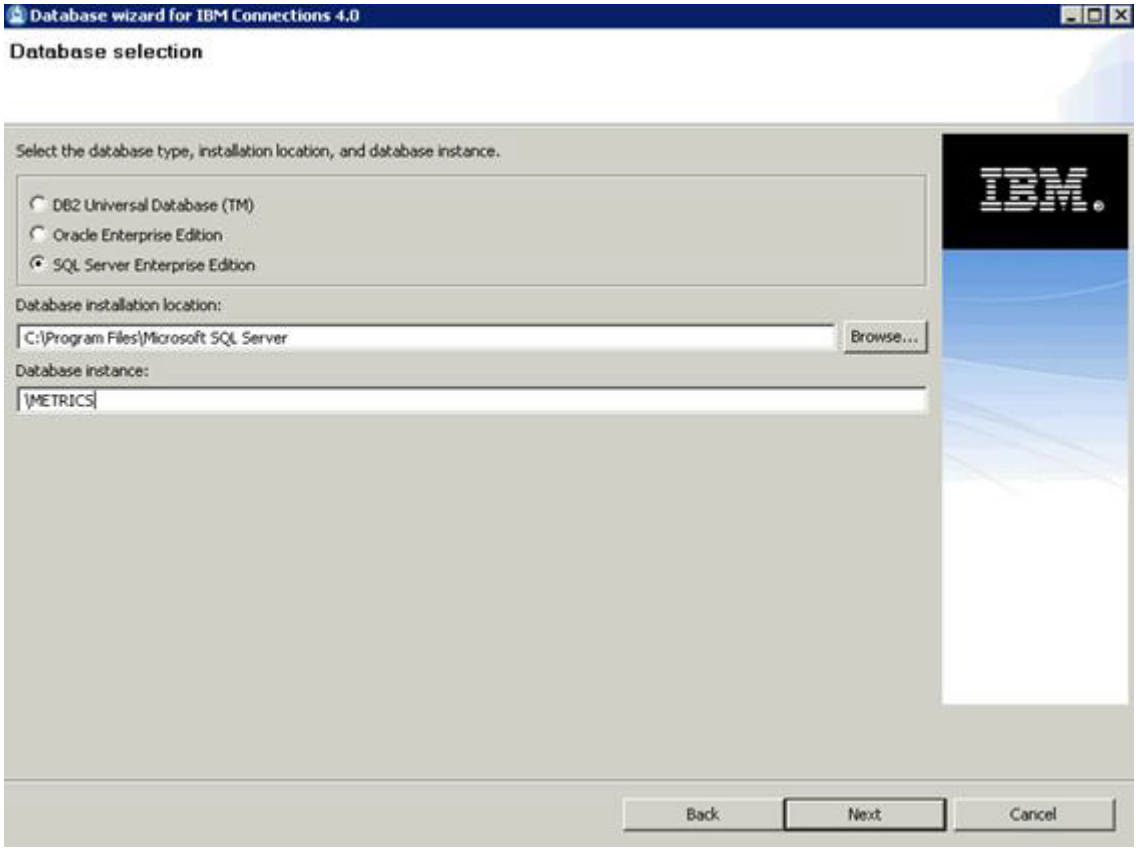


Figure 95. Database wizard for IBM Connections 4.0: Database selection

__ 5. Select the database instance to create from the list of applications and click **Next**.

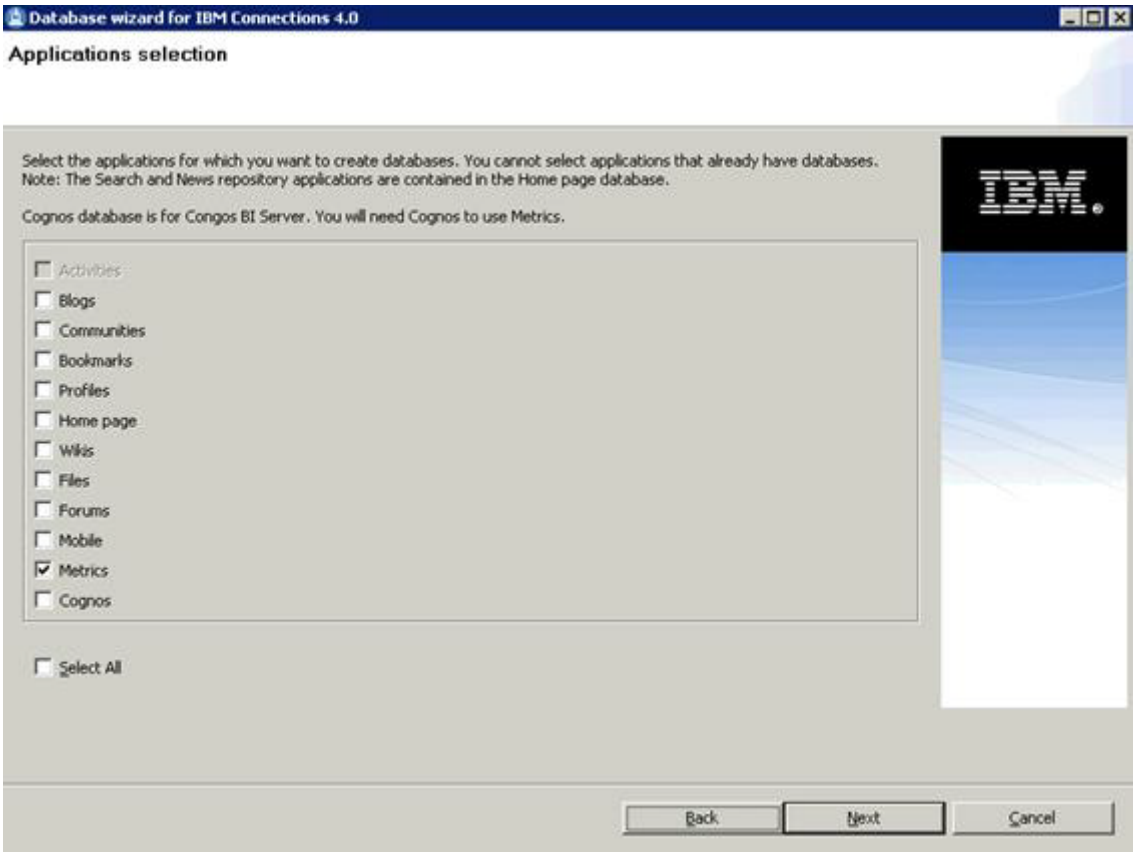


Figure 96. Database wizard for IBM Connections 4.0: Applications selection

__ 6. Enter and confirm the password for the database instance to create and click **Next**.

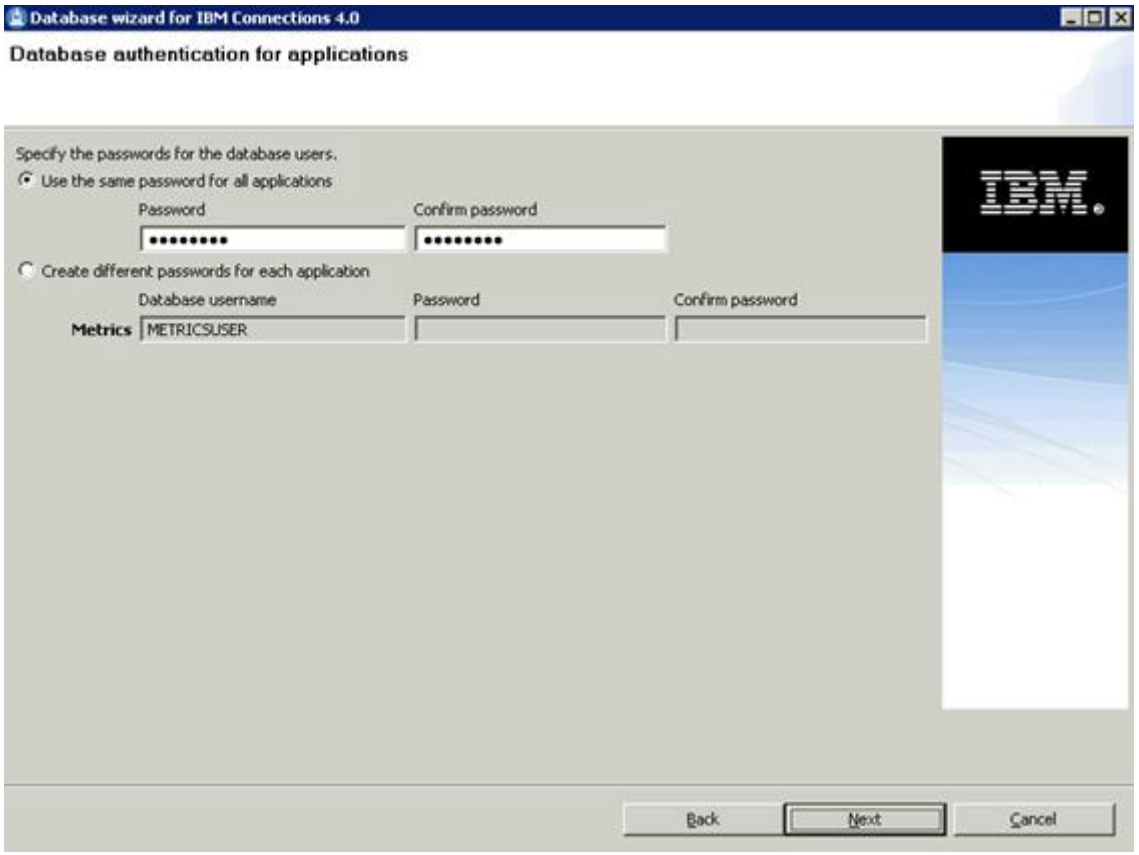


Figure 97. Database wizard for IBM Connections 4.0: Database authentication for applications

__ 7. Select 'Use the same database file location for all applications" and enter the file location. Then, click **Next** to continue.

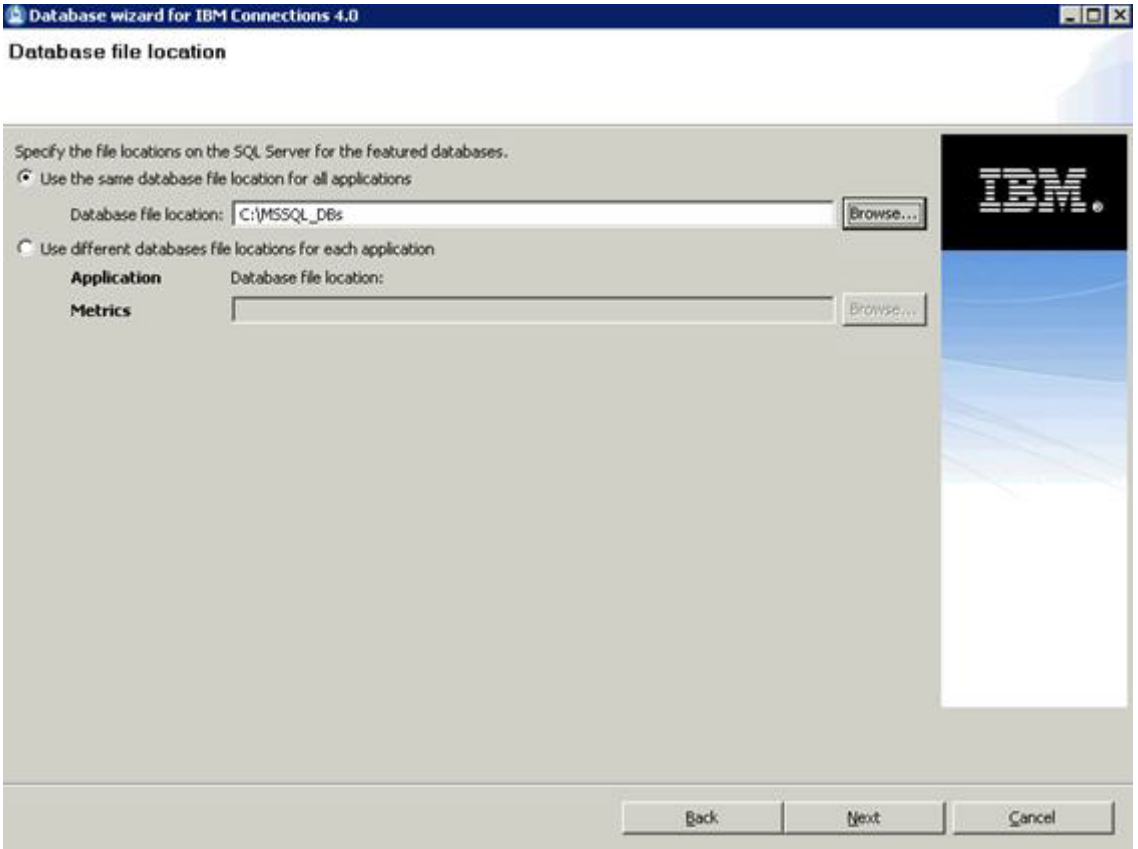


Figure 98. Database wizard for IBM Connections 4.0: Database file location

__ 8. Review the summary screen and click **Create** to continue.

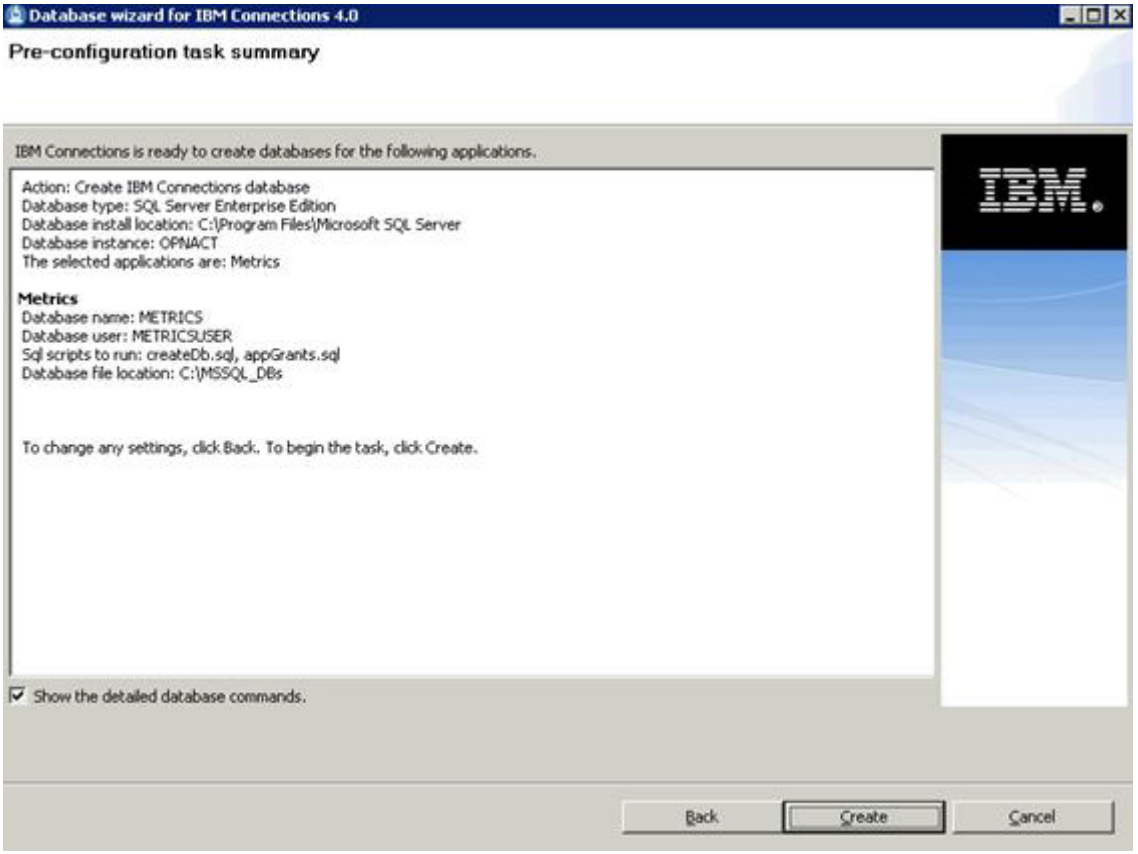


Figure 99. Database wizard for IBM Connections 4.0: Pre-configuration task summary

__ 9. Click **Execute** to start creating the database. After finishing, remember to rerun the wizard again for each instance to create the appropriate database for each instance.

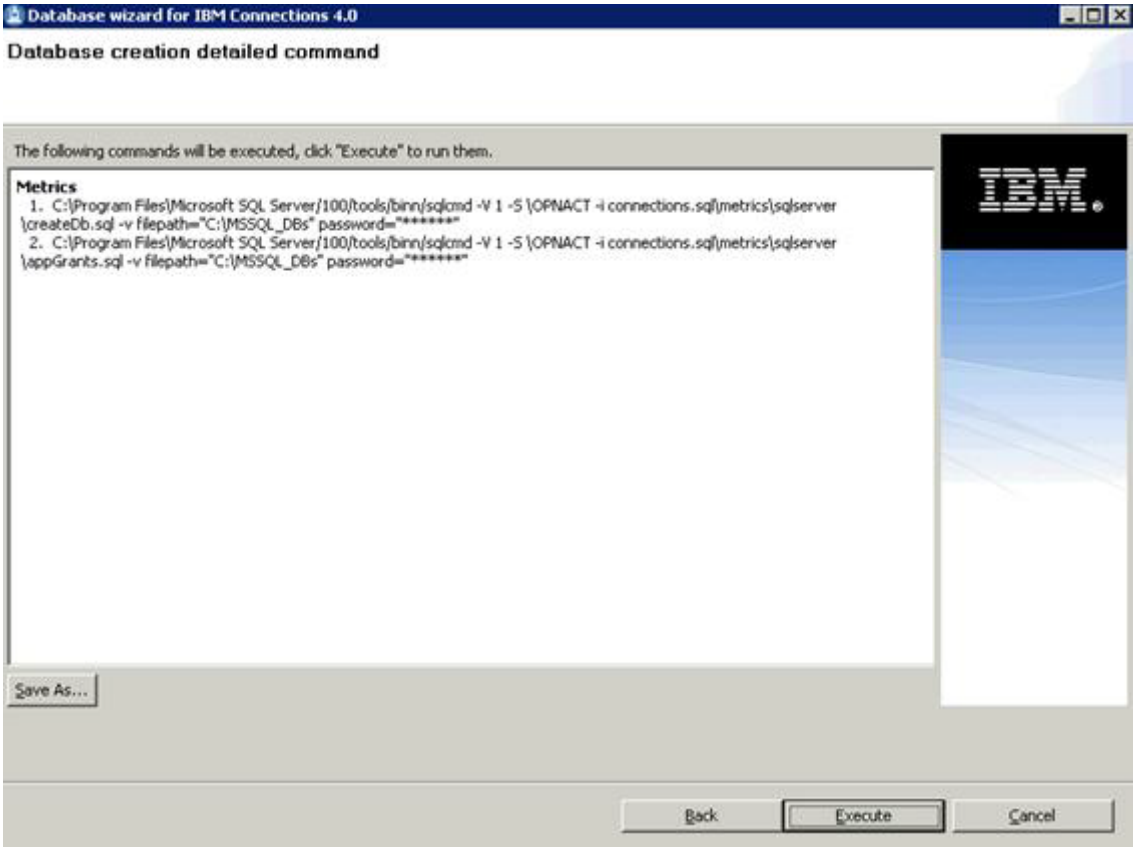


Figure 100. Database wizard for IBM Connections 4.0: Database creation detailed command

Populating the Profiles database

__ 1. Go to the Wizard folder and run the `populationWizard.bat`. Profiles population wizard for IBM Connections 4.0 opens. Click **Next** to continue.

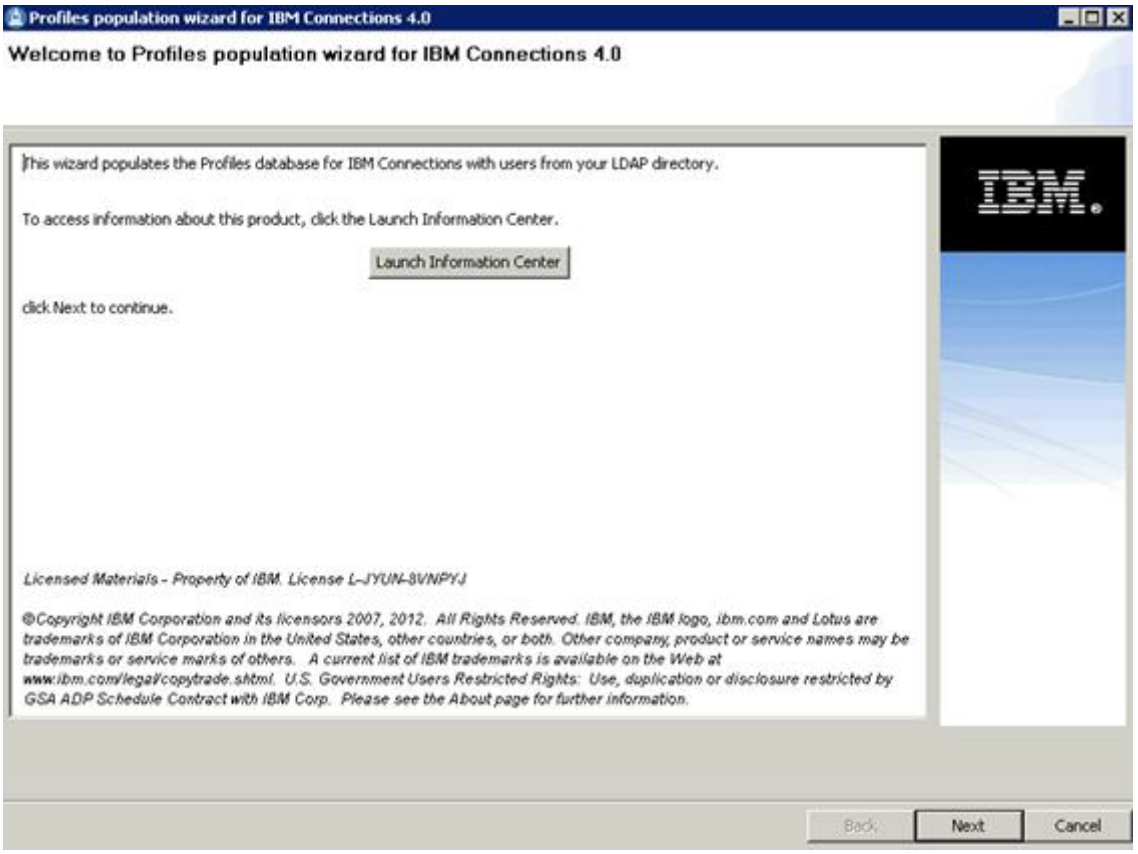


Figure 101. Profiles population wizard for IBM Connections 4.0: Welcome

__ 2. Select the installation directory and click **Next** to continue.

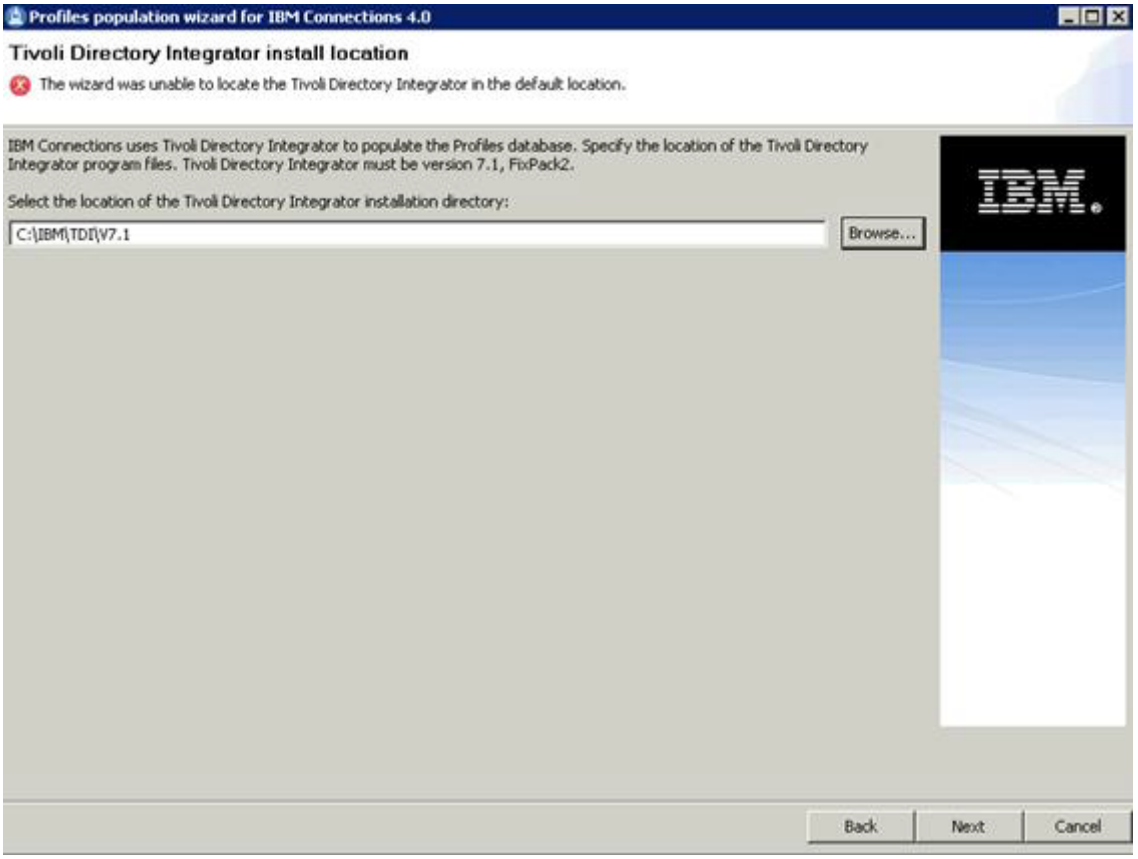


Figure 102. Profiles population wizard for IBM Connections 4.0: Tivoli Directory Integrator installation location

__ 3. Select the database type and click **Next** to continue.

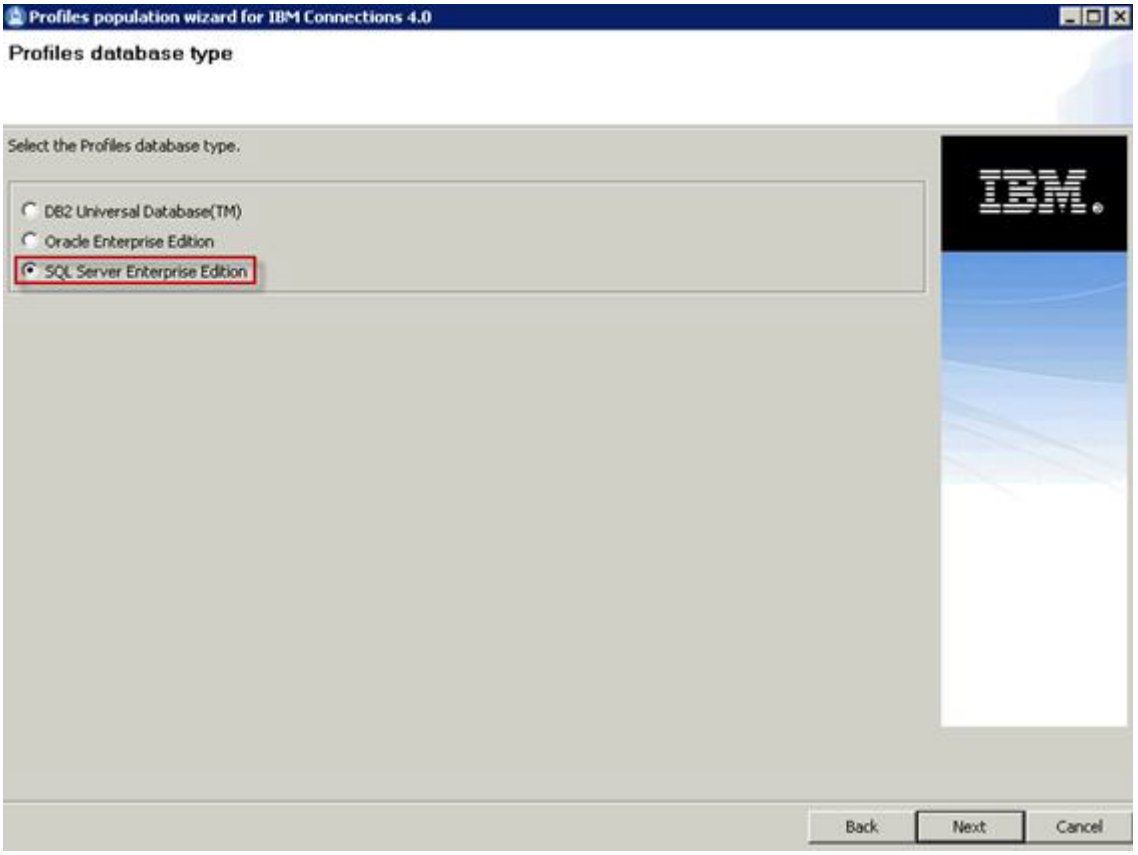


Figure 103. Profiles population wizard for IBM Connections 4.0: Profiles database type

__ 4. Now enter the database information for where your PEOPLEDB database is located, and click **Next** to continue.

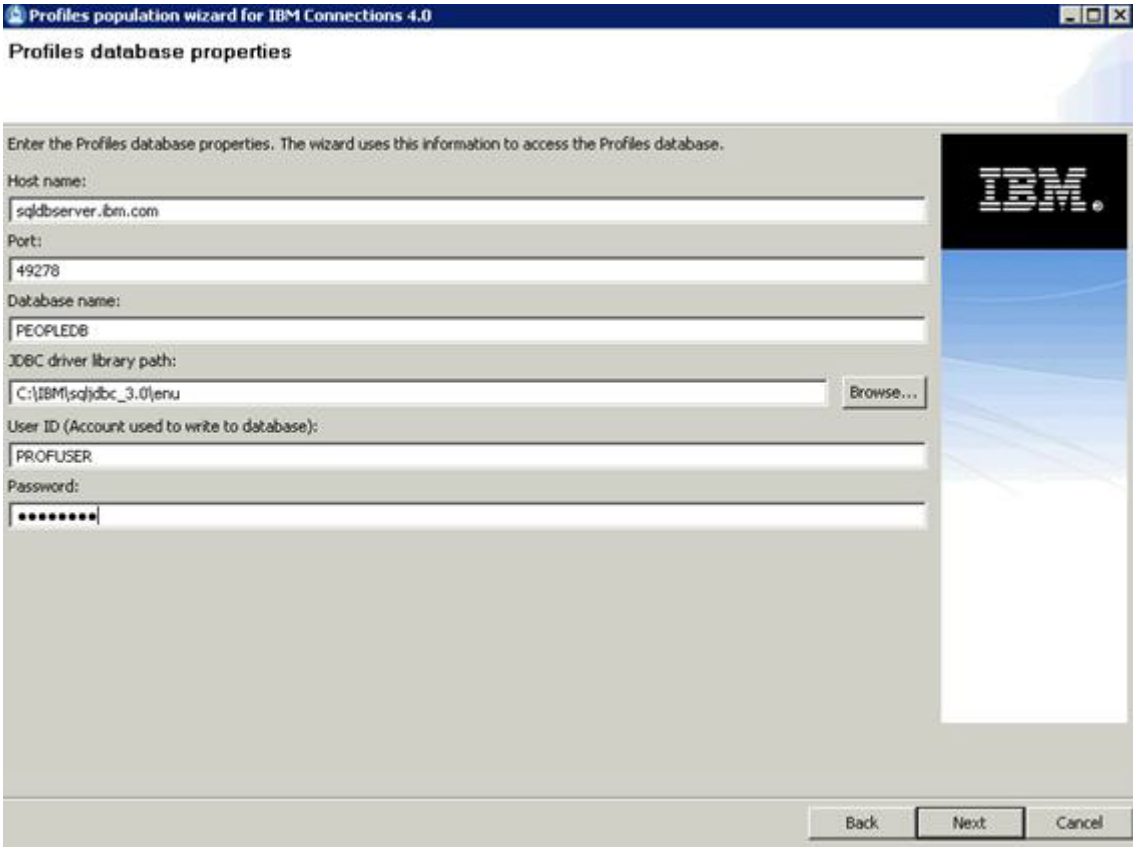


Figure 104. Profiles population wizard for IBM Connections 4.0: Profiles database properties

__ 5. Enter the LDAP server name and port number. Then, click **Next** to continue.

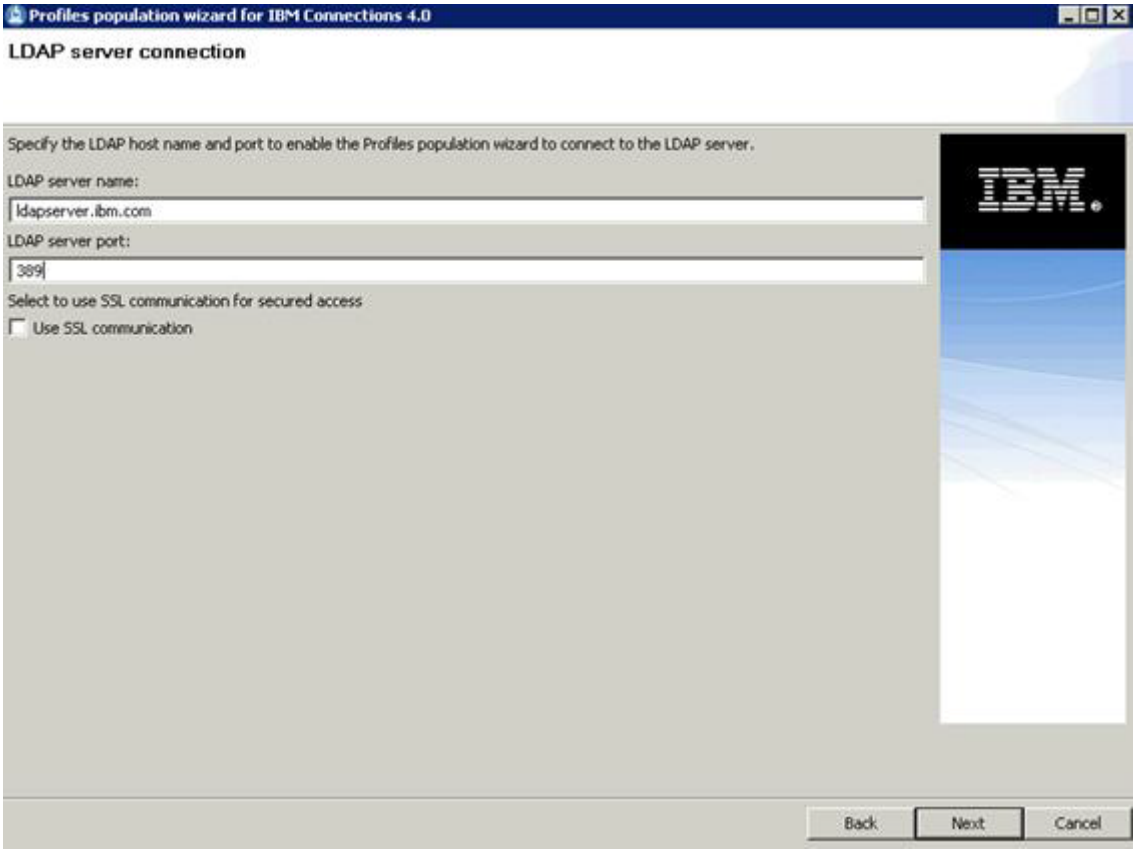


Figure 105. Profiles population wizard for IBM Connections 4.0: LDAP server connections

__ 6. Now enter your LDAP bind user authentication details and password. Then, click **Next** to continue. In this case, it is:

`cn=wpsbind,cn=users,l=SharedLDAP,c=US,ou=Lotus,o=Software Group,dc=ibm,dc=com`

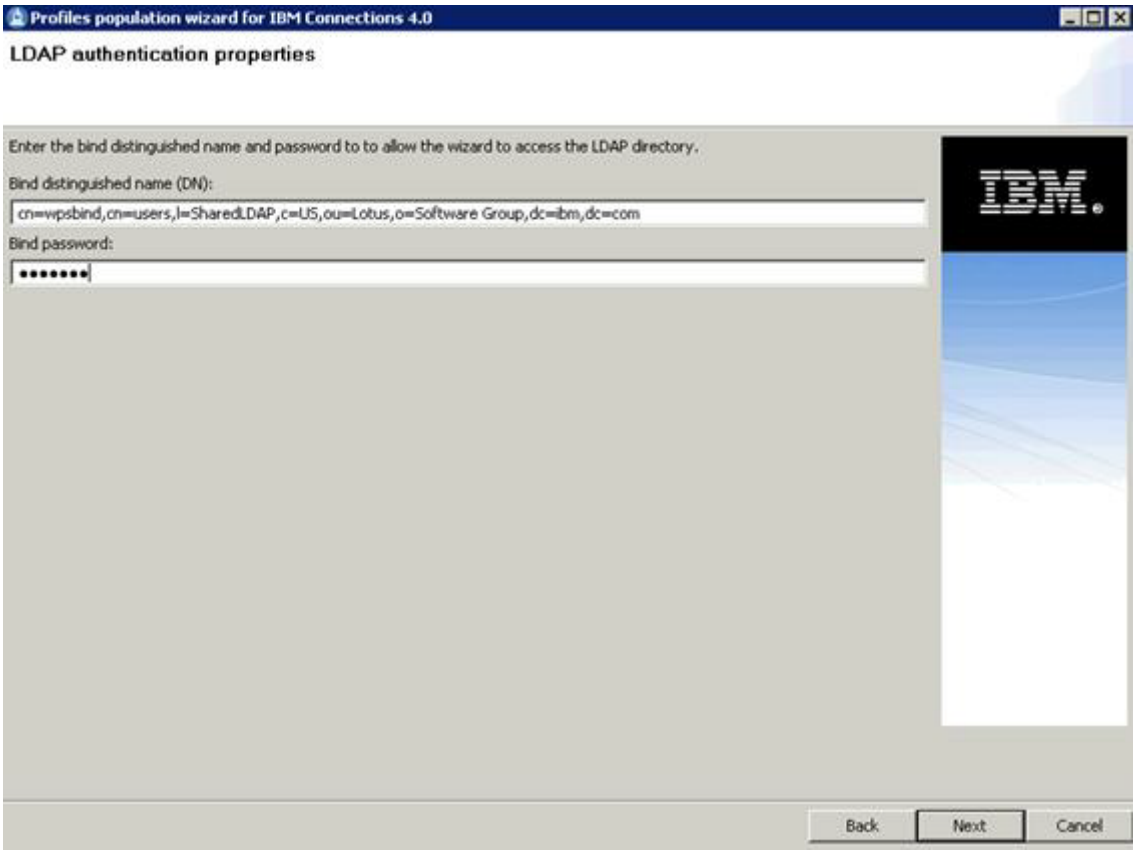


Figure 106. Profiles population wizard for IBM Connections 4.0: LDAP authentication properties

__ 7. Now enter the search base and the search filter. Then, click **Next** to continue.

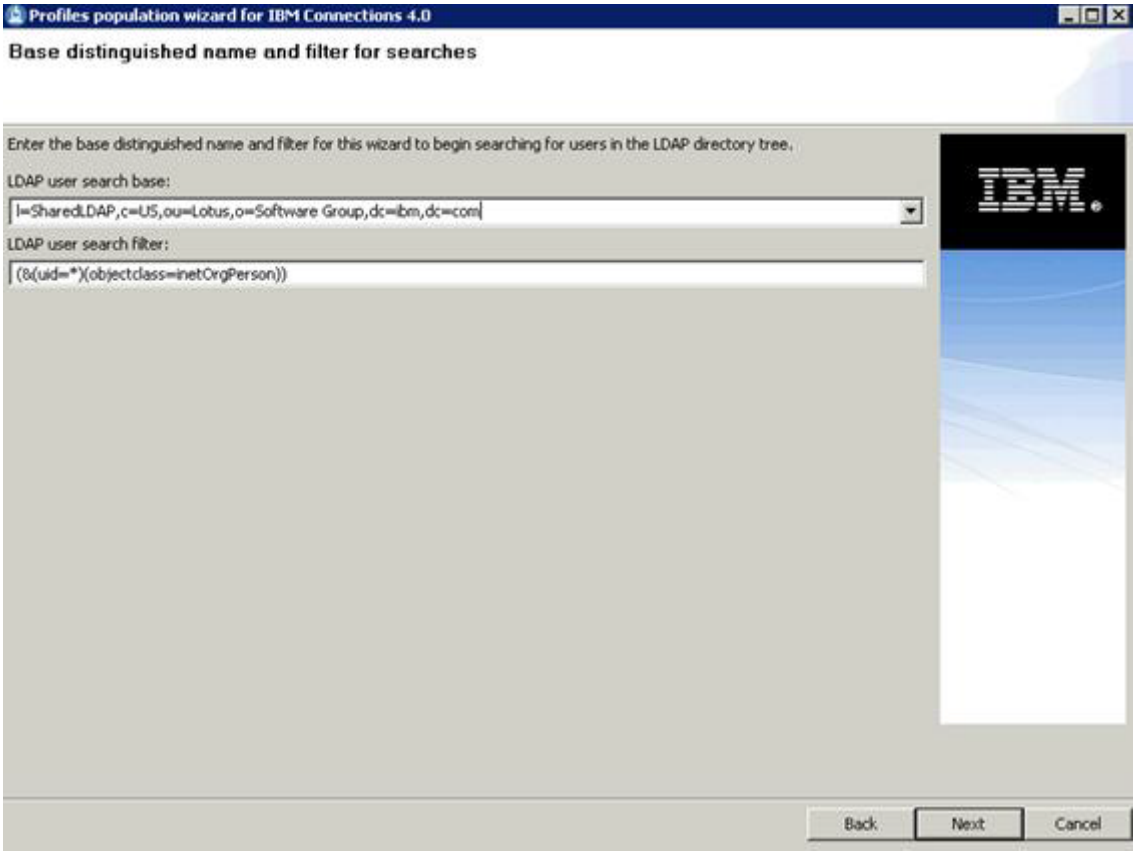
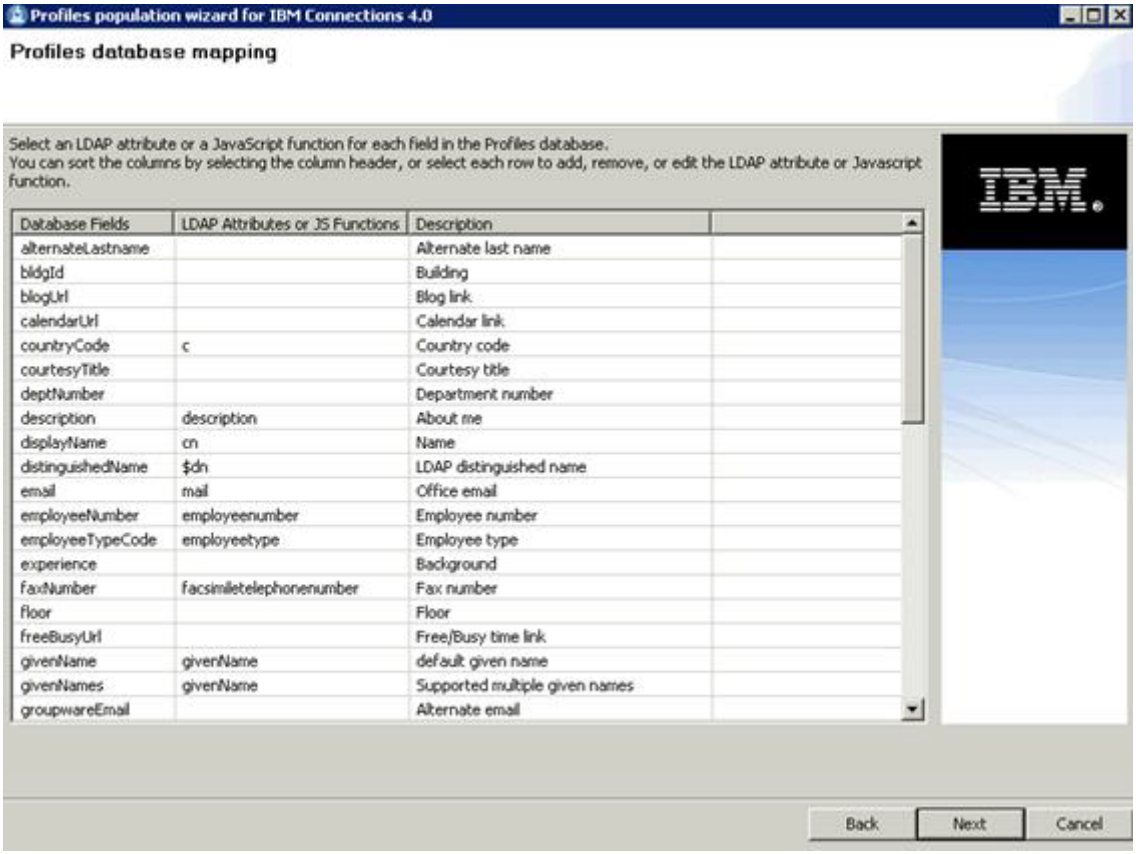


Figure 107. Profiles population wizard for IBM Connections 4.0: Base distinguished name and filter for searches

__ 8. Accept the default database mappings, and click **Next** to continue.



Database Fields	LDAP Attributes or JS Functions	Description
alternateLastname		Alternate last name
bldgId		Building
blogUrl		Blog link
calendarUrl		Calendar link
countryCode	c	Country code
courtesyTitle		Courtesy title
deptNumber		Department number
description	description	About me
displayName	cn	Name
distinguishedName	$dn	LDAP distinguished name
email	mail	Office email
employeeNumber	employeenumber	Employee number
employeeTypeCode	employeetype	Employee type
experience		Background
faxNumber	facsimiletelephonenumber	Fax number
floor		Floor
freeBusyUrl		Free/Busy time link
givenName	givenName	default given name
givenNames	givenName	Supported multiple given names
groupwareEmail		Alternate email

Figure 108. Profiles population wizard for IBM Connections 4.0: Profiles database mapping

__ 9. Accept the default mapping, and click **Next** to continue.

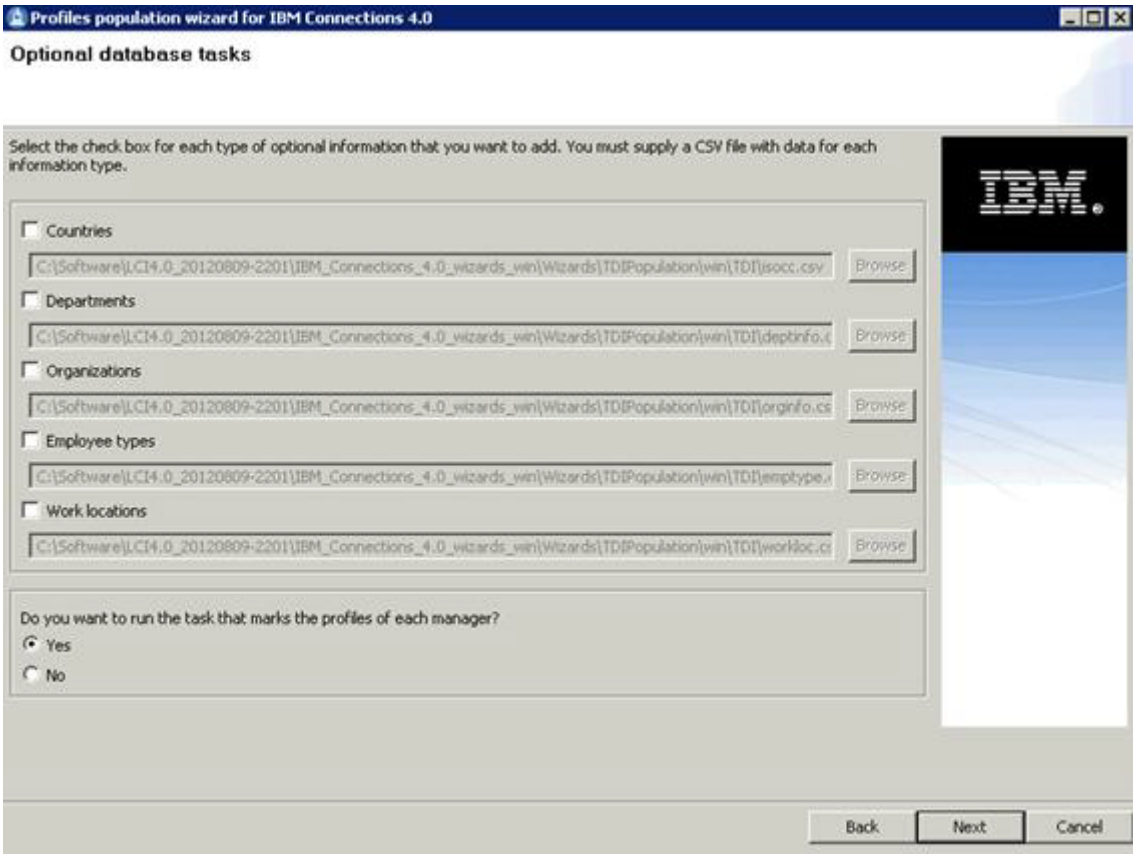


Figure 109. Profiles population wizard for IBM Connections 4.0: Optional database tasks

__ 10. Review the summary, and click **Configure** to start the population of the Profiles database.

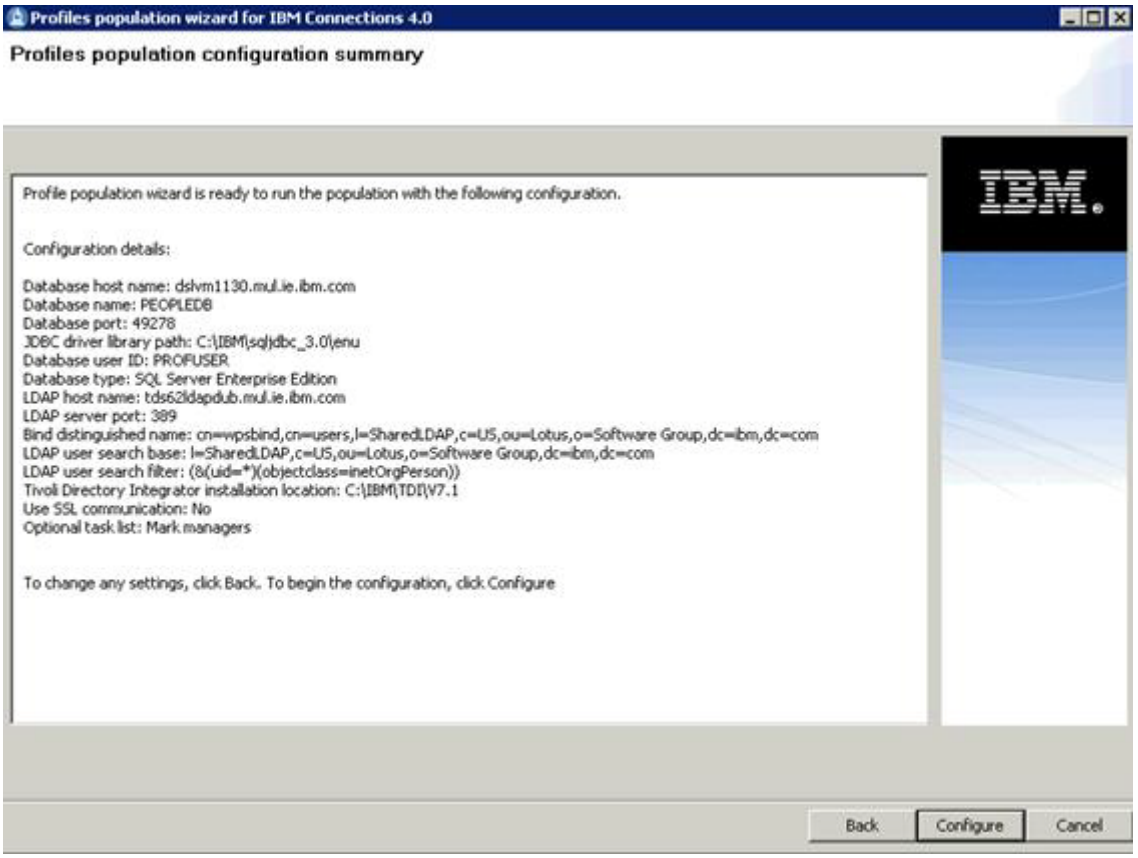


Figure 110. Profiles population wizard for IBM Connections 4.0: Profiles population configuration summary

__ 11. The population of Profiles database takes several hours to complete. When it is completed (without any errors), click **Finish**.

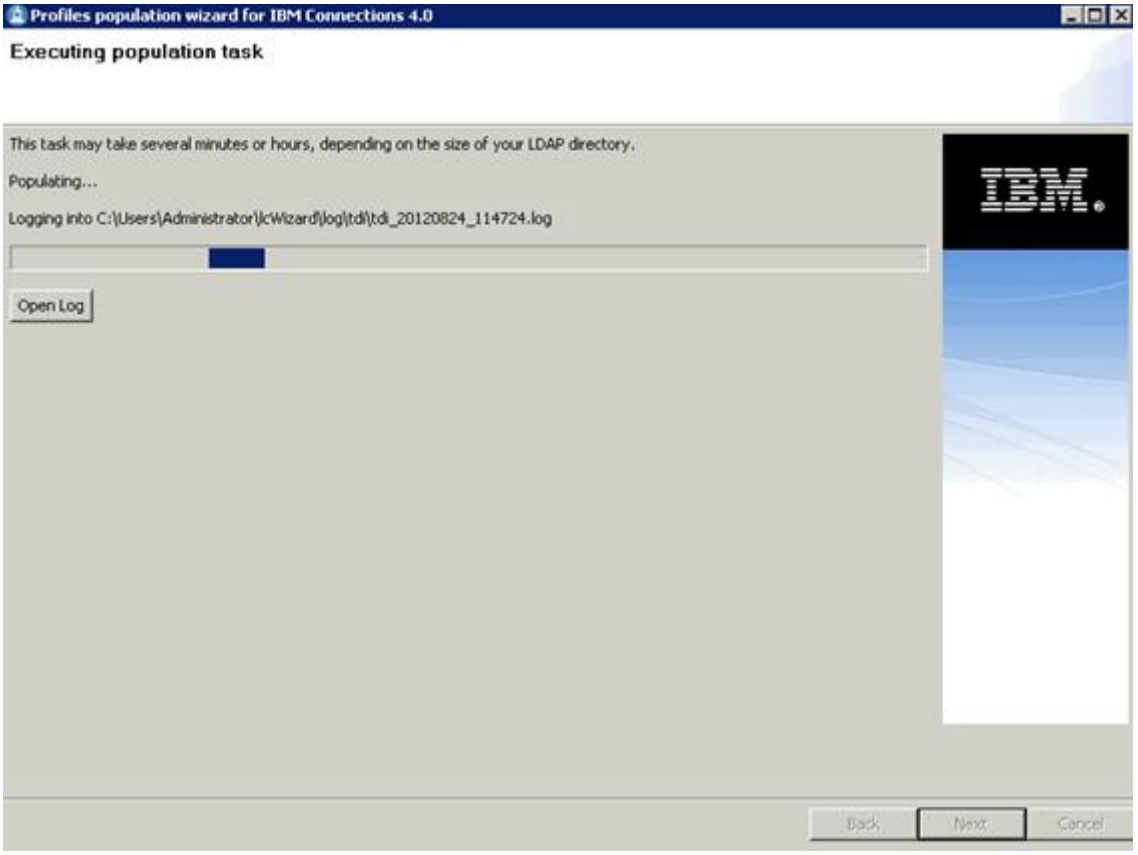


Figure 111. Profiles population wizard for IBM Connections 4.0: Executing population task

Installing IBM Connections 4.0

Before beginning the installation

Before beginning the installation, take note of the following points:

- **Rational Installation Manager:** IBM Connections 4.0 uses the Rational Installation Manager to provide an enhanced installation experience. Before beginning the installation, you should uninstall any previous versions of Rational Installation Manager since you are prompted to install this product when you run the IBM Connections 4.0 Installer.
- **Deployment Manager and nodes:** Remember to start the Deployment Manager before running the installation wizard. Node agents should also be started so that resynchronization is possible between the Deployment Manager and nodes when required.
- **DB2.** Before beginning to install IBM Connections 4.0, you must copy the JDBC driver from the DB2 server, `db.example.com`, to a local directory on the Deployment Manager and both nodes. The same local directory must be used on `dm.example`, `node1.example.com`, and `node2.example.com`. That directory is named `C:\IBM\JDBC_Drivers`. IBM Connections uses these drivers to connect to the database.

  On the DB2 computer, these drivers are in `C:\IBM\SQLIB\java`. The names of the required drivers are `db2jcc.jar` and `db2jcc_licence_cu.jar`.

  For different databases, different JDBC drivers are required. The following table describes which drivers are required for which database. No matter which database is used, these drivers must be copied to this location on the machine that hosts IBM Connections 4.0.

Table 2: Database type

Database type	JDBC driver name
Oracle	ojdbc6.jar
MS SQL Server	sqljdbc4.jar

Shared Data folder: For a networked, multi-node configuration, there must be a shared space between the Deployment Manager and nodes. This space is used as a data store for IBM Connections. This shared space can be a shared network folder on Windows or Linux, or be part of a storage area network (SAN) in large deployments. In this scenario, the directory `C:\IBM\LotusConnections\data\shared` on `dm.example.com` is shared between both nodes.

To share the folder, follow these steps:

__ 1. Open the folder `C:\IBM` on the Deployment Manager, open the properties of this folder, and switch to the Sharing tab.

__ 2. Click **Share**.

__ 3. The folder is then shared along with all its subdirectories.

The folder is now shared; however, any clients that want to connect to this client must authenticate with this computer.

__ 4. Map the shared folder to both node computers. If the credentials are different on the node computer and the Deployment Manager, select Connect using different credentials. Be sure to select Reconnect at logon.

__ 5. Post installation: The Lotus Connections data folder is created and can be accessed at this location on each node:

__ a. Extract the IBM Connections installation files to a directory on `dm.example.com` and run `launchpad.exe` to begin the installation.

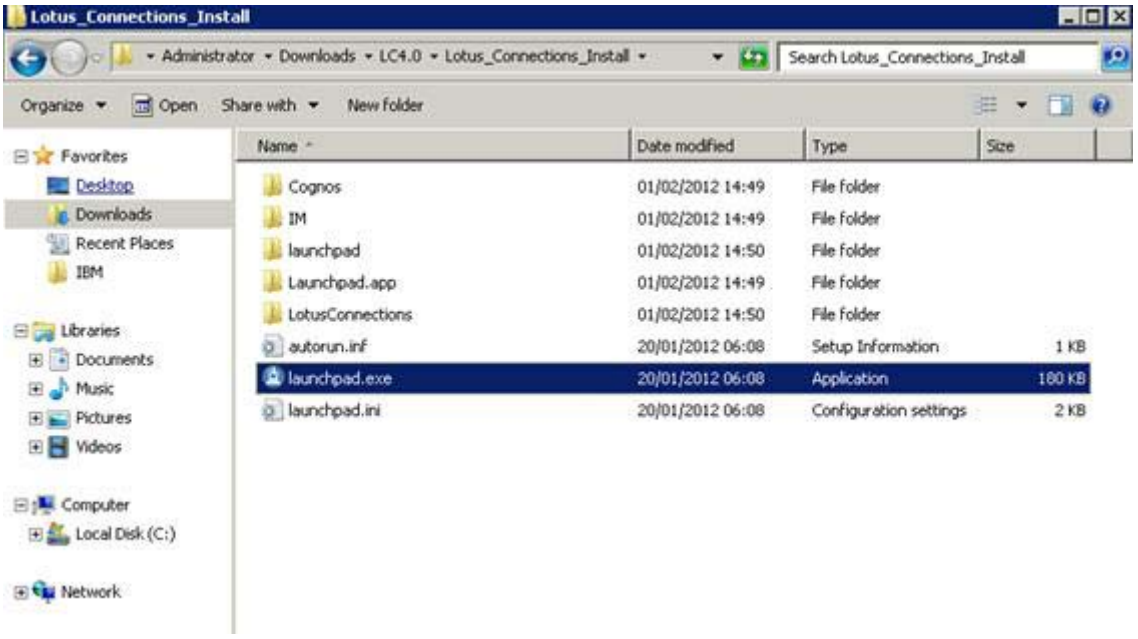


Figure 112. Lotus Connections Install: Launchpad

__ b. Click **Install IBM Connections 4.0.0**.

Figure 113. IBM Connections 4.0.0: Install IBM Connections 4.0.0

__ c. Click **Install** to continue.

Figure 114. IBM Installation Manager: Install software packages

__ d. The following figure shows more about Rational Installation Manager and includes an important note about starting the Deployment Manager before beginning the installation. See the Starting and Stopping IBM Connections section to find out how to start the Deployment Manager. After the Deployment Manager is started, click **Launch the IBM Connections 4.0.0 install wizard**.

Select to install both the Installation Manager and IBM Connections 4.0.0 and click **Next** to continue.

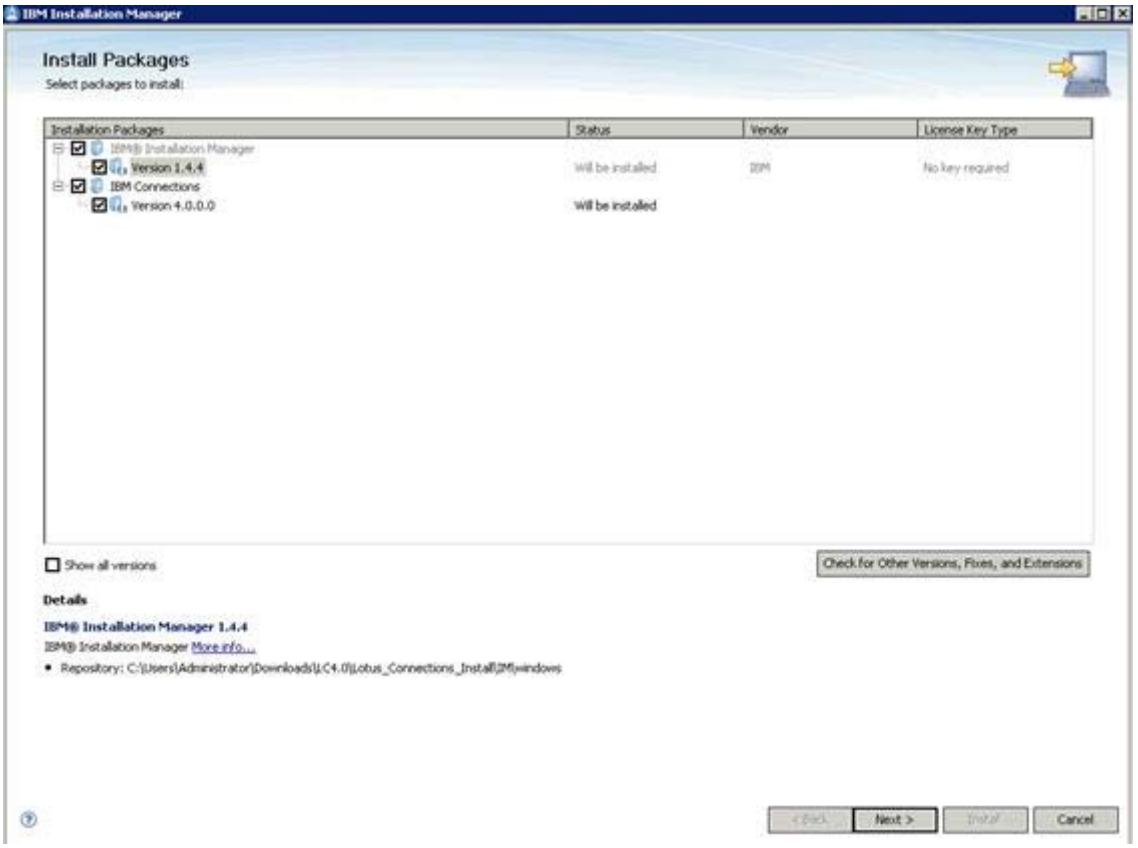


Figure 115. IBM Installation Manager: Installation Packages

__ e. Accept the license agreement and click **Next** to continue.

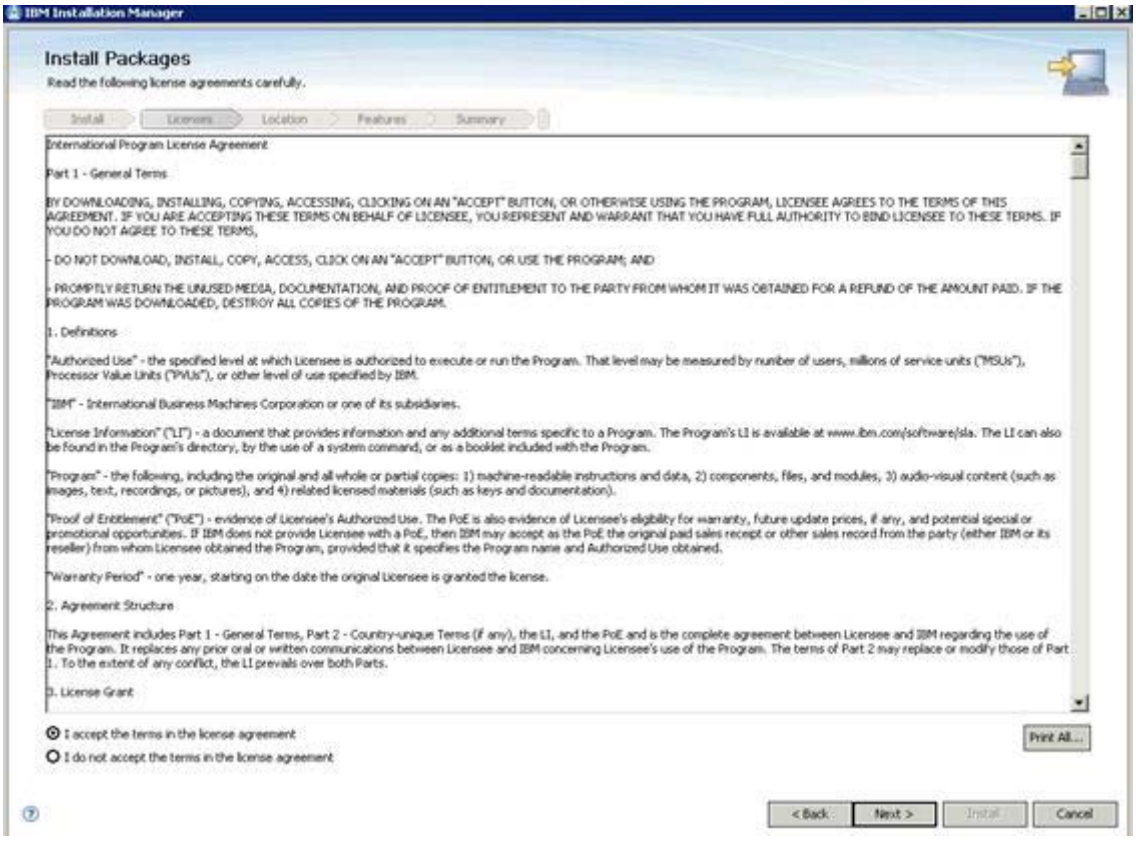


Figure 116. IBM Installation Manager: License agreement

__ f. Select the location to install Rational Installation Manager and the shared resources directory. Use the locations that are shown in the figure for ease of use and then click **Next** to proceed.

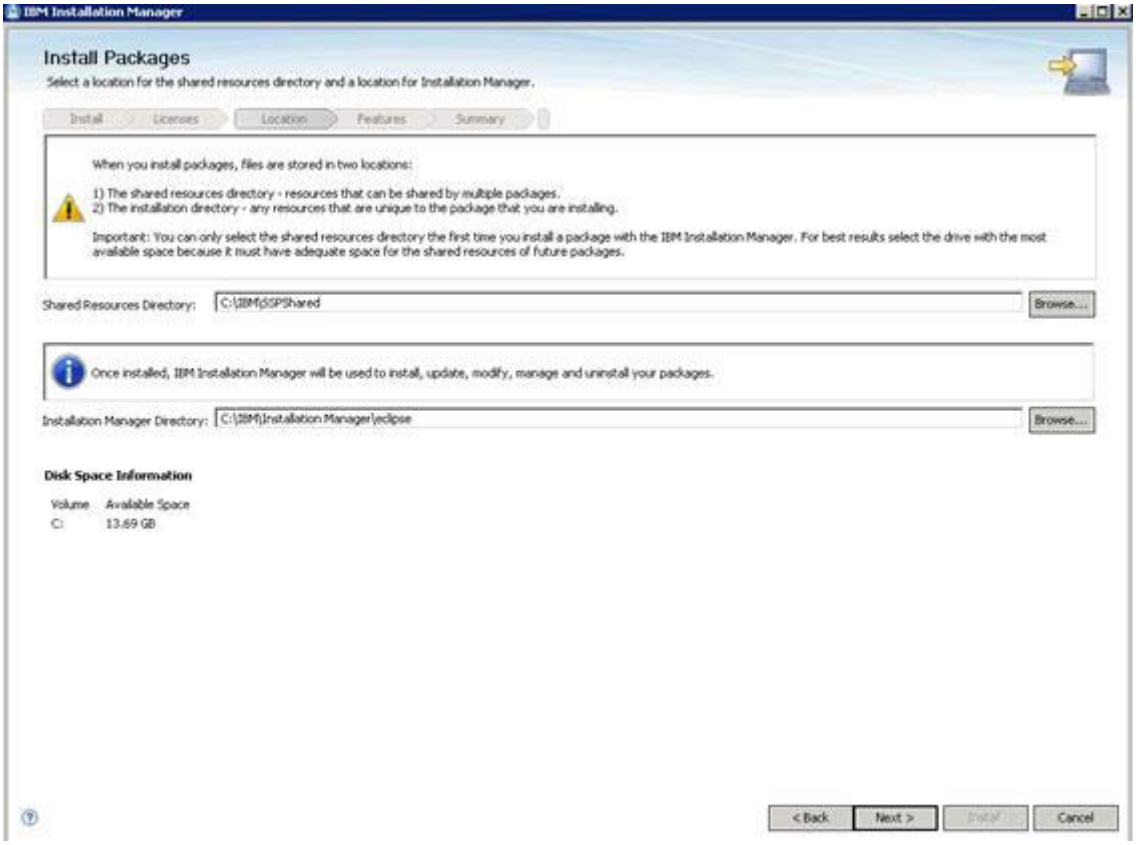


Figure 117. IBM Installation Manager: Installation location

__ g. A new package group is created for IBM Connections. Select the installation directory as shown in the following figure and click **Next** to proceed.

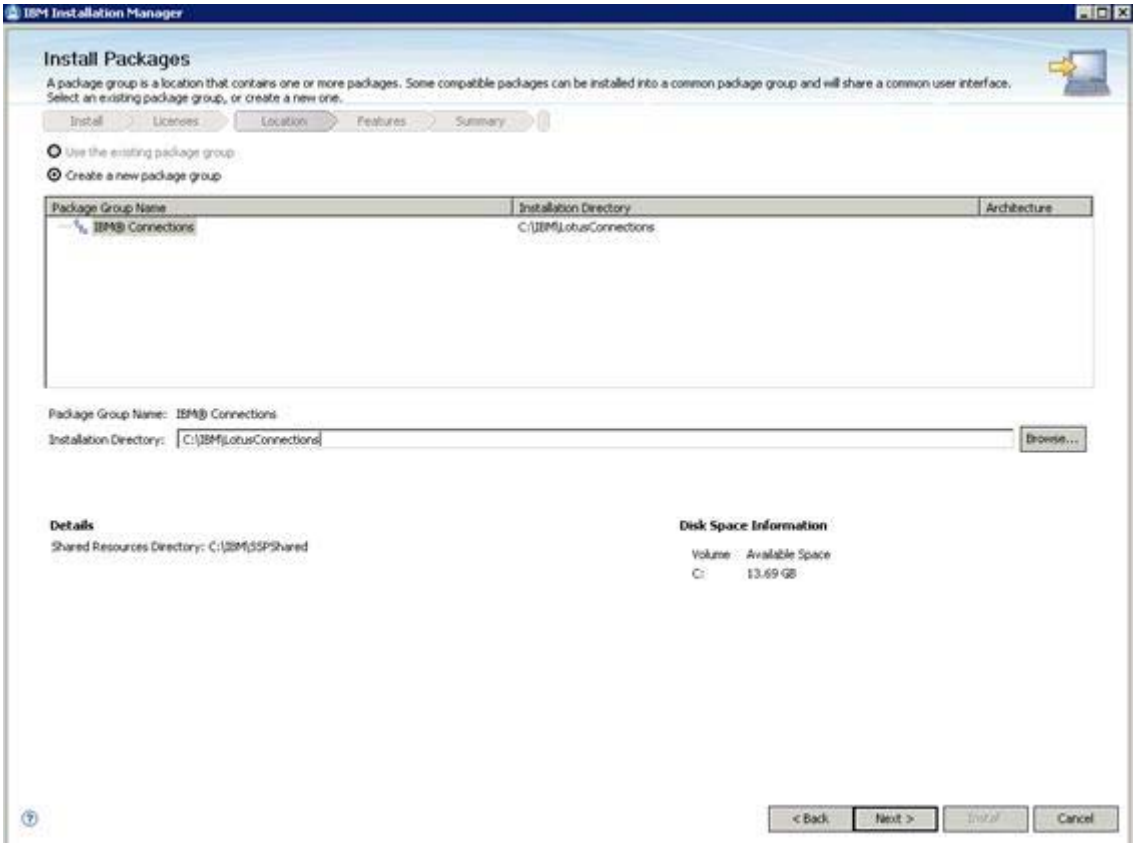


Figure 118. IBM Installation Manager: New package group

__ h. To install all IBM Connections components, ensure that all options are selected except those that are not required, and click **Next** to proceed.

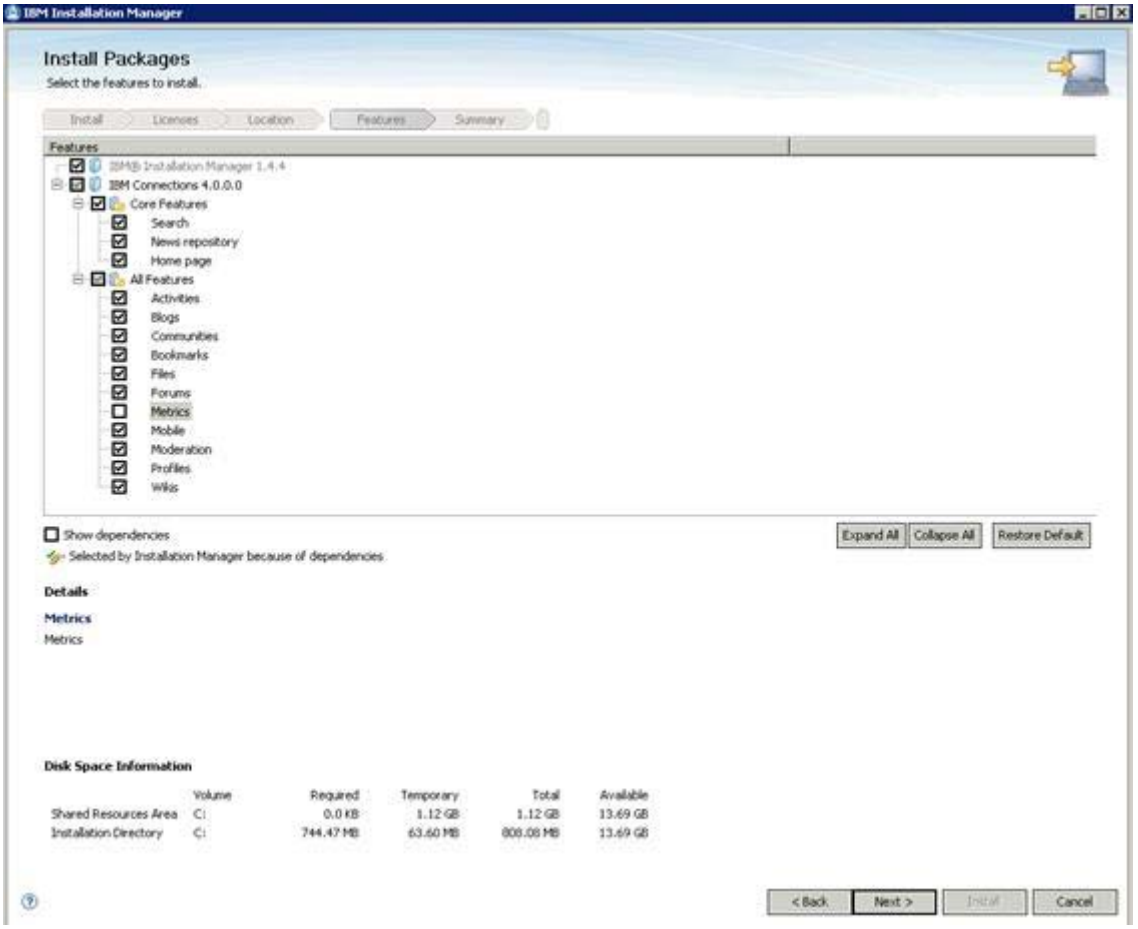


Figure 119. IBM Installation Manager: Features to install

__ i. Complete the host name, dm.example.com, and the Deployment Manager administrator and password. If you plan to deploy your configuration with a third-party security suite, such as Tivoli Access Manager, SiteMinder, or SPNEGO, the administrative user must be specified on both the LDAP and on a Deployment Manager administrator. Click **Validate** to verify these settings before proceeding.

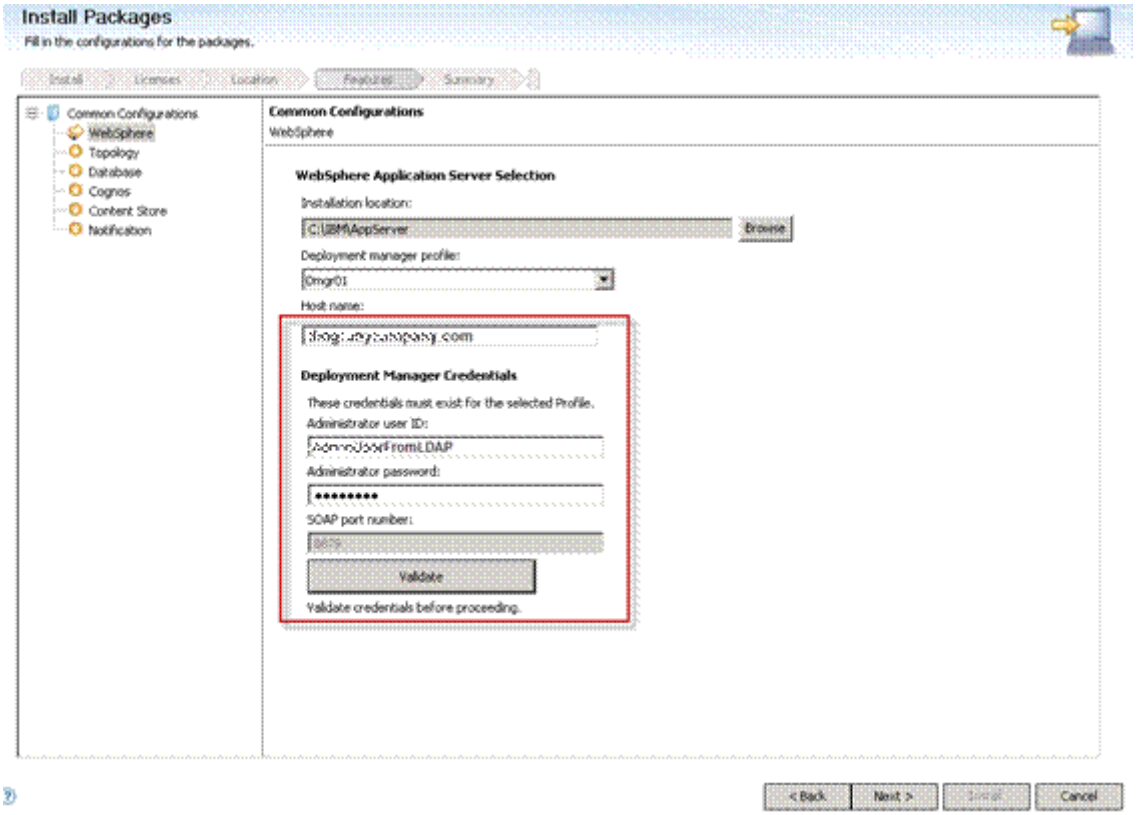


Figure 120. IBM Installation Manager: Configurations for the packages

__ 6. If the validation is successful, click **OK** and then click **Next** to continue.

Figure 121. Information dialog: Validation successful

__ j. Select the **Medium** deployment topology as shown in the figure and click **Same nodes selection for all clusters** to ensure that all applications are installed on both nodes in each cluster. Click **Next** to continue.

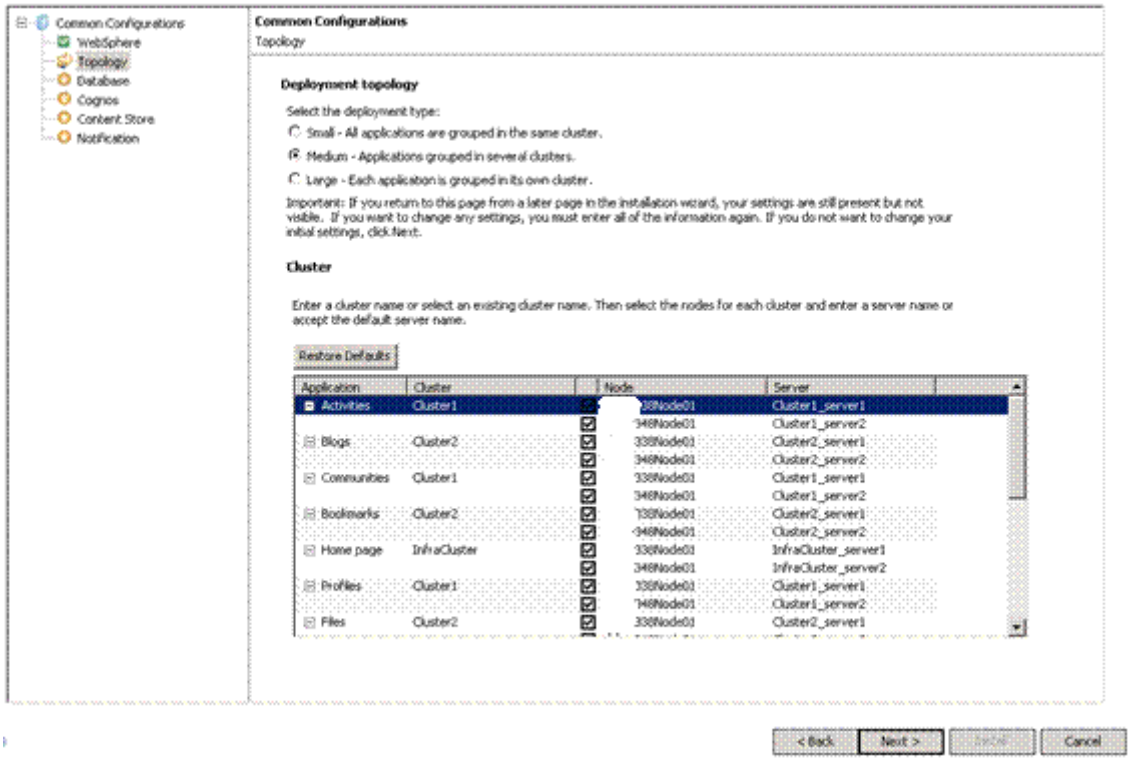


Figure 122. IBM Installation Manager: Topology

__ k. In this instance, each database is on its own instance. Therefore, check the No option at the top of the panel. Select SQL as the database type, and provide the location to the JDBC drivers. For each database, the next step is to provide the host name of the database server, the port numbers that each database can be found under, and the password to access the database. These values are the same as in the table that describes the database topology when setting up SQL. These ports might differ slightly from configuration to configuration. Click **Validate** to ensure all the inputs are correct. The validation starts.

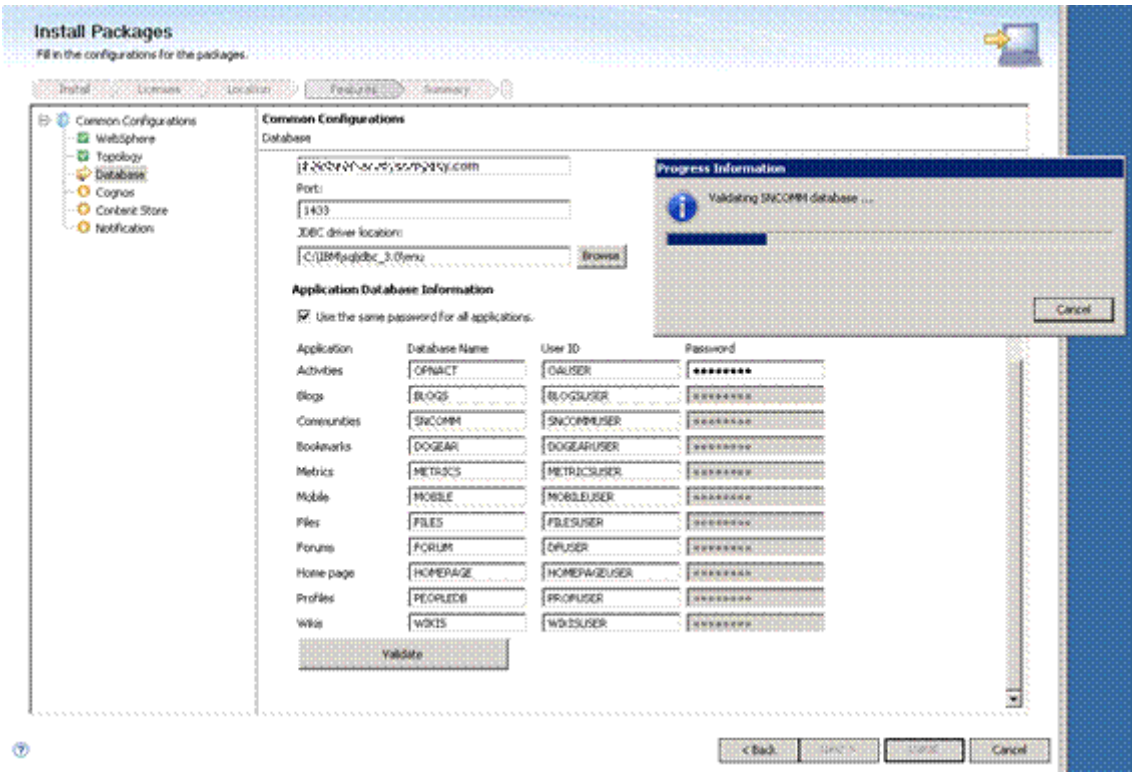


Figure 123. IBM Installation Manager: Database

__ l. Click **Validated**.

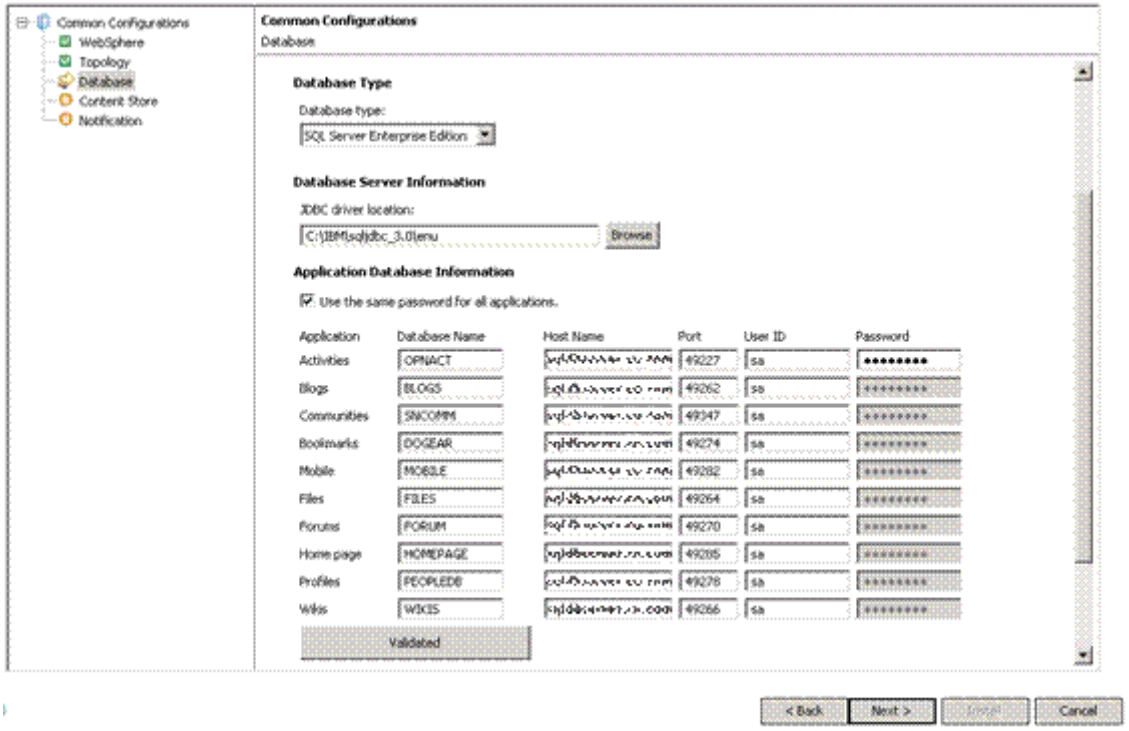


Figure 124. IBM Installation Manager: Database

__ m. The validation finishes. Click **OK** to close the information dialog and then **Next** to continue.

Figure 125. Information dialog: Validation successful

__ n. Provide the location of the local and shared data stores as in the following figure. The shared content store must be specified by using the Windows UNC directory format. The location `\\dm.example.com\IBM\LotusConnections\data\shared` is available to all nodes and is the same physical space. Click **Validate** to verify these settings.

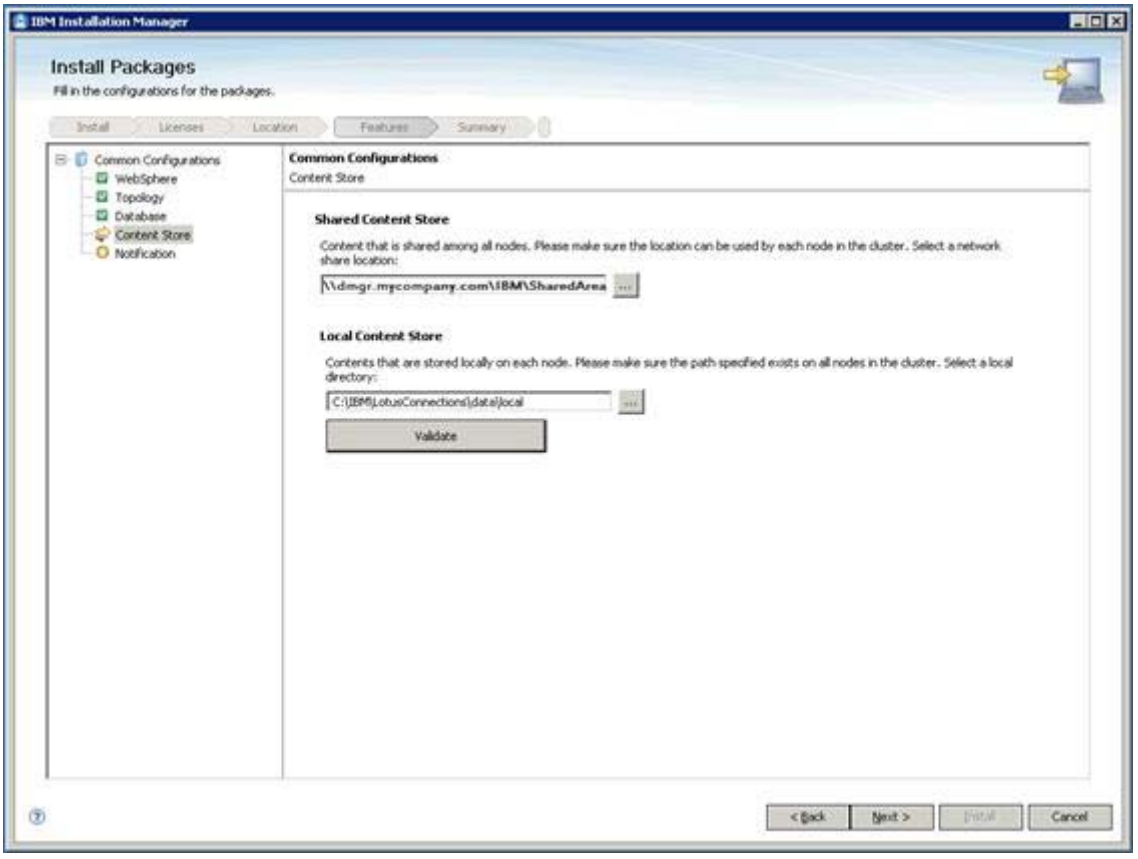


Figure 126. IBM Installation Manager: Content Store

__ o. The validation finishes. Click **OK** to close the information dialog and then **Next** to continue.

Figure 127. Information dialog: Validation successful

__ p. In the following figure, do not enable IBM Connections deployment for mail notifications. Depending on your configuration, you might need to provide more information in the other fields. Click **Next** to continue.

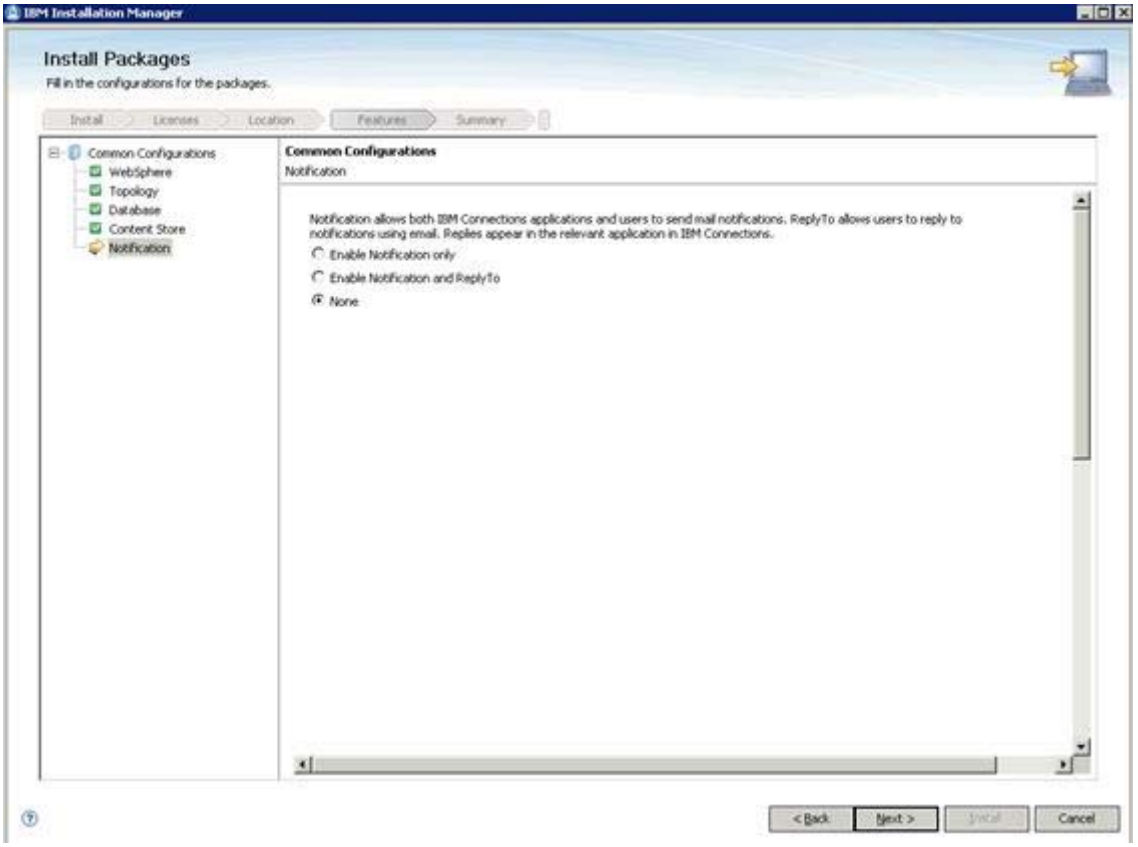


Figure 128. IBM Installation Manager: Notification

__ q. Review the summary panel and click **Install** to begin the installation.

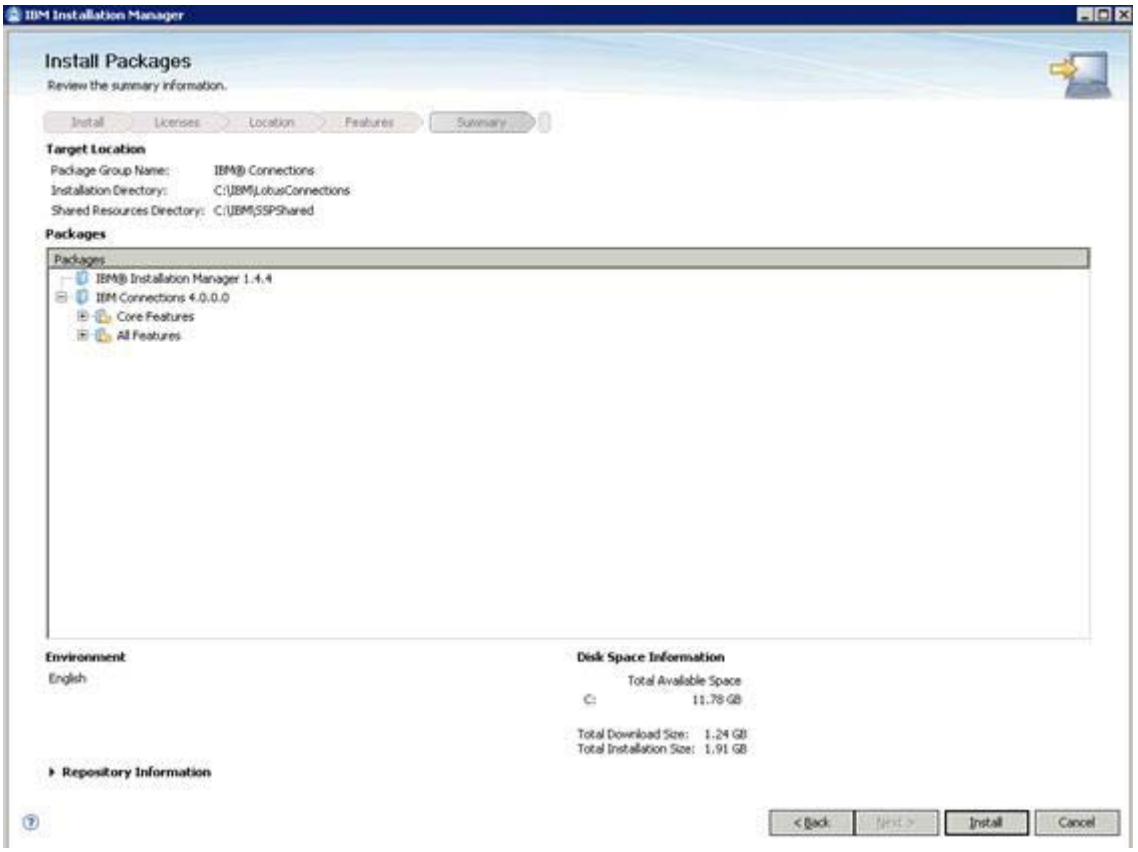


Figure 129. IBM Installation Manager: Summary information

The installation is now in progress and might take up to two hours to complete.

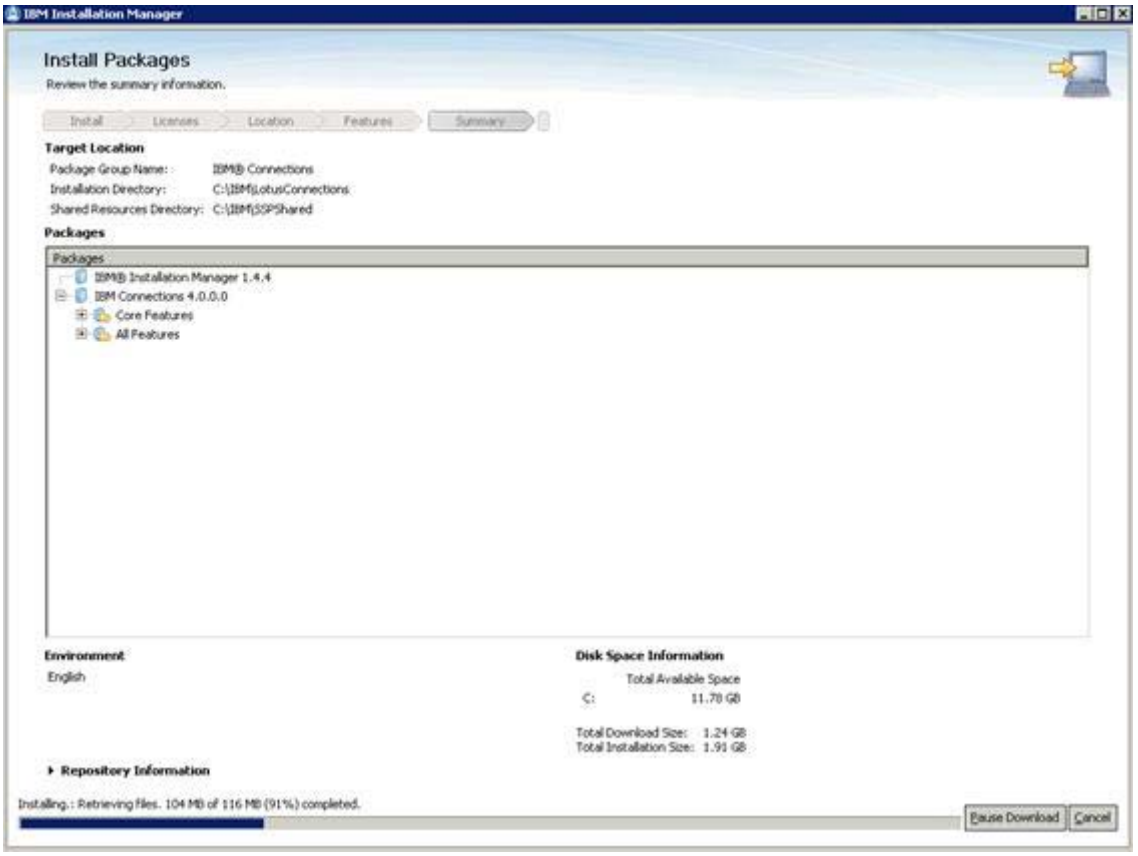


Figure 130. IBM Installation Manager: Installation in progress

__ r. When the installation finishes, the summary panel that is shown in the following figure is displayed and all packages should be installed successfully. Click **Finish** to complete the installation of IBM Connections. There are a number of post installation tasks which must be attended to. Before proceeding to these tasks, you must restart the Deployment Manager for installation changes to take effect. After the Deployment Manager is restarted, move to these steps.

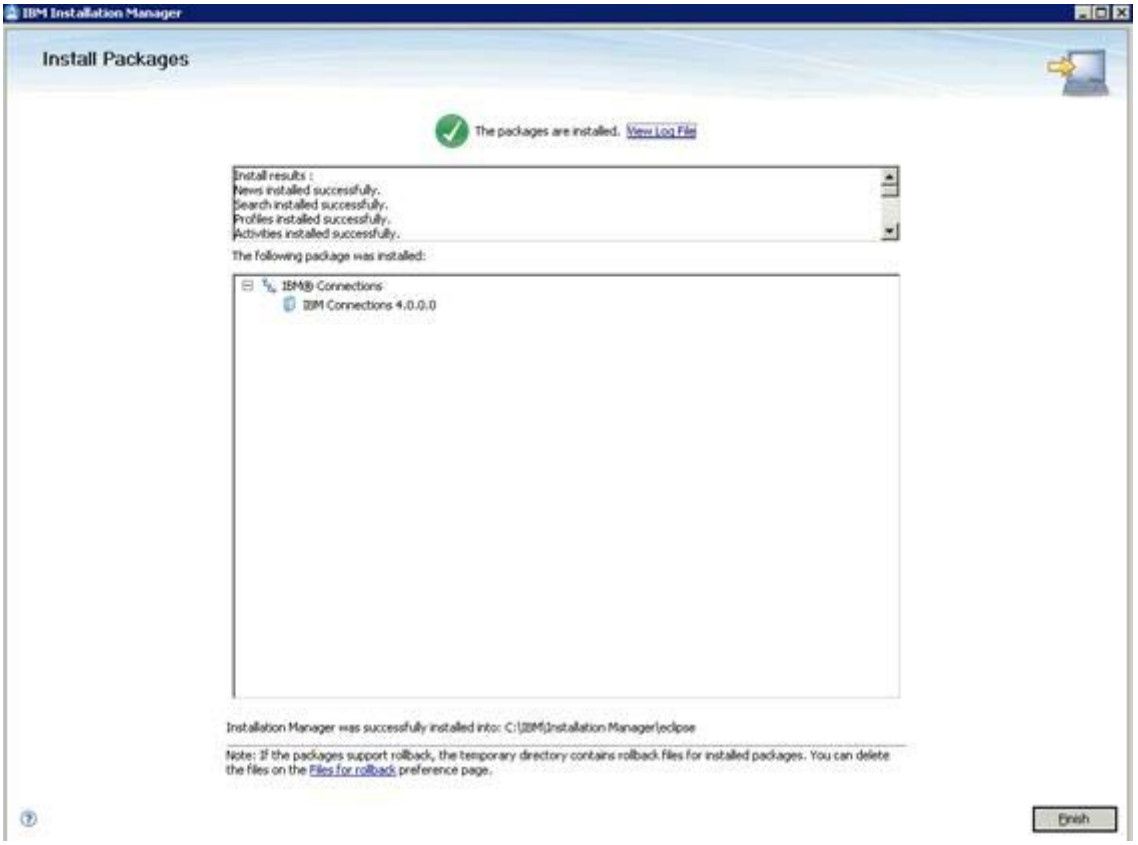


Figure 131. IBM Installation Manager: Installation completion

Configuring the HTTP server

Add web server as an unmanaged node

__ 1. Click **Add Node**.

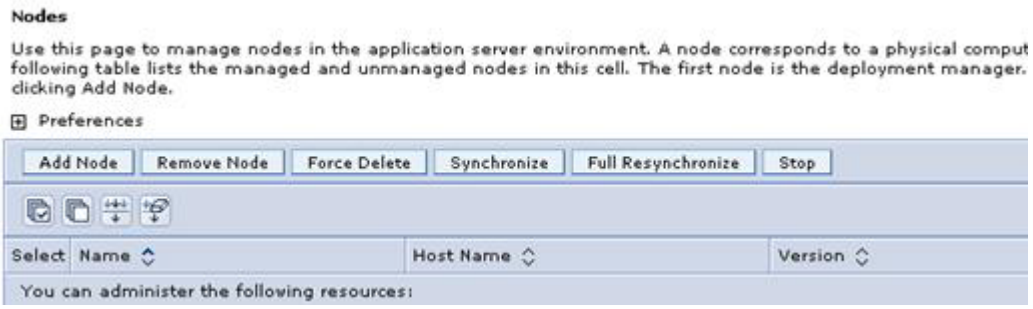


Figure 132. Adding web server as an unmanaged node

__ 2. Click **Unmanaged node**.

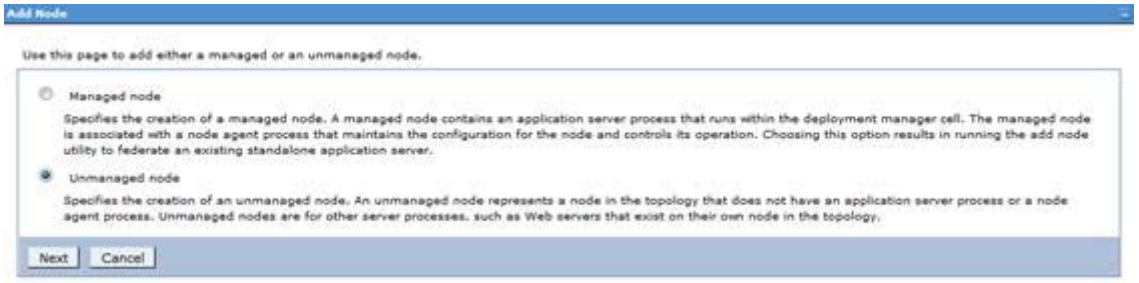


Figure 133. Unmanaged node

__ 3. Enter the name and the host name. Click **Apply** and then **OK**.

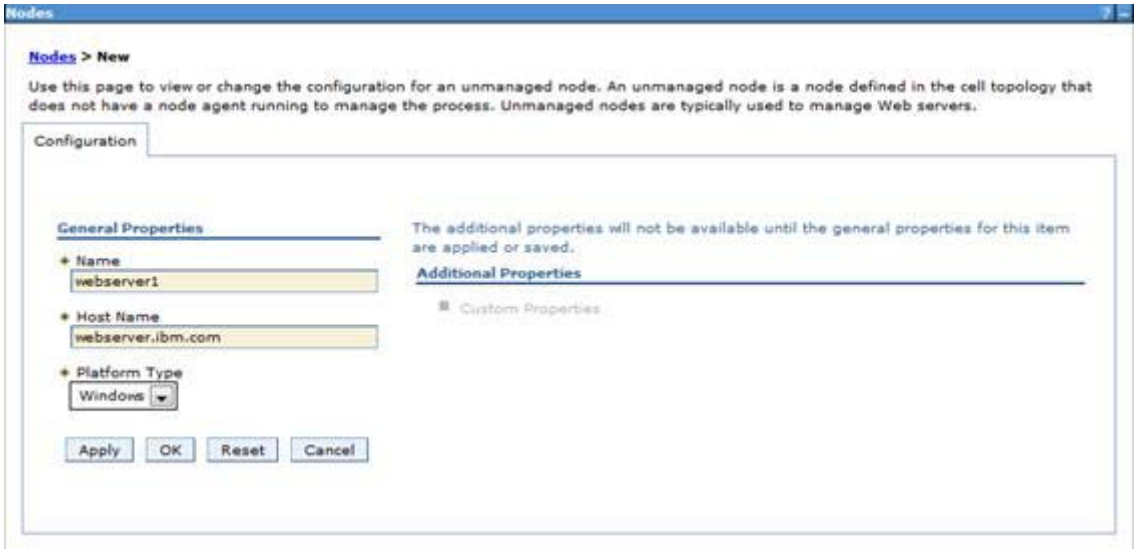


Figure 134. Node configuration

__ 4. Click **Save**.

Figure 135. Messages

__ 5. The web server is added as an unmanaged node.

Figure 136. Web server added as an unmanaged node

Add web server as a server

__ 1. Click **Generate Plug-in**.

Figure 137. Adding web server as a server

__ 2. Enter the Server name and click **Next**.

Figure 138. Selecting a node for the web server and selecting the web server type

__ 3. Select **IHS** as template name and click **Next**.

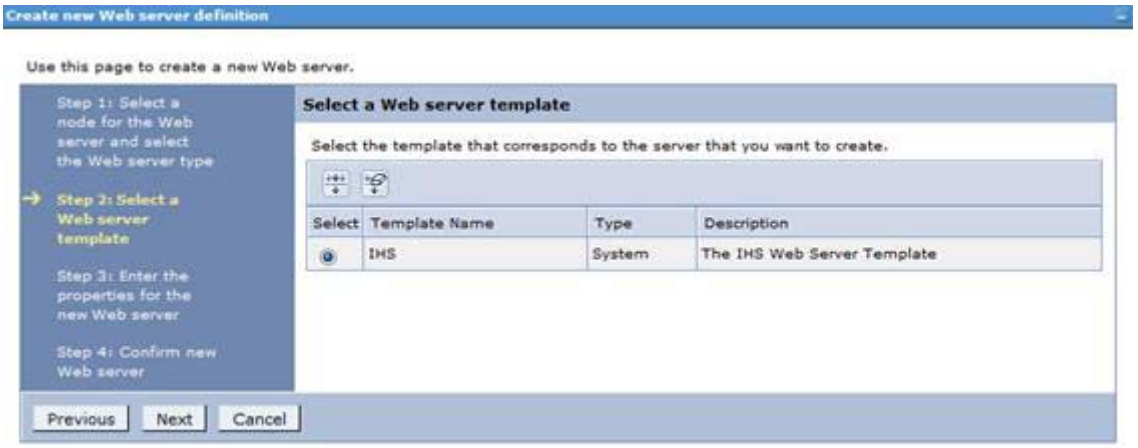


Figure 139. Selecting a web server template

__ 4. Enter the properties for the web server and click **Next**.

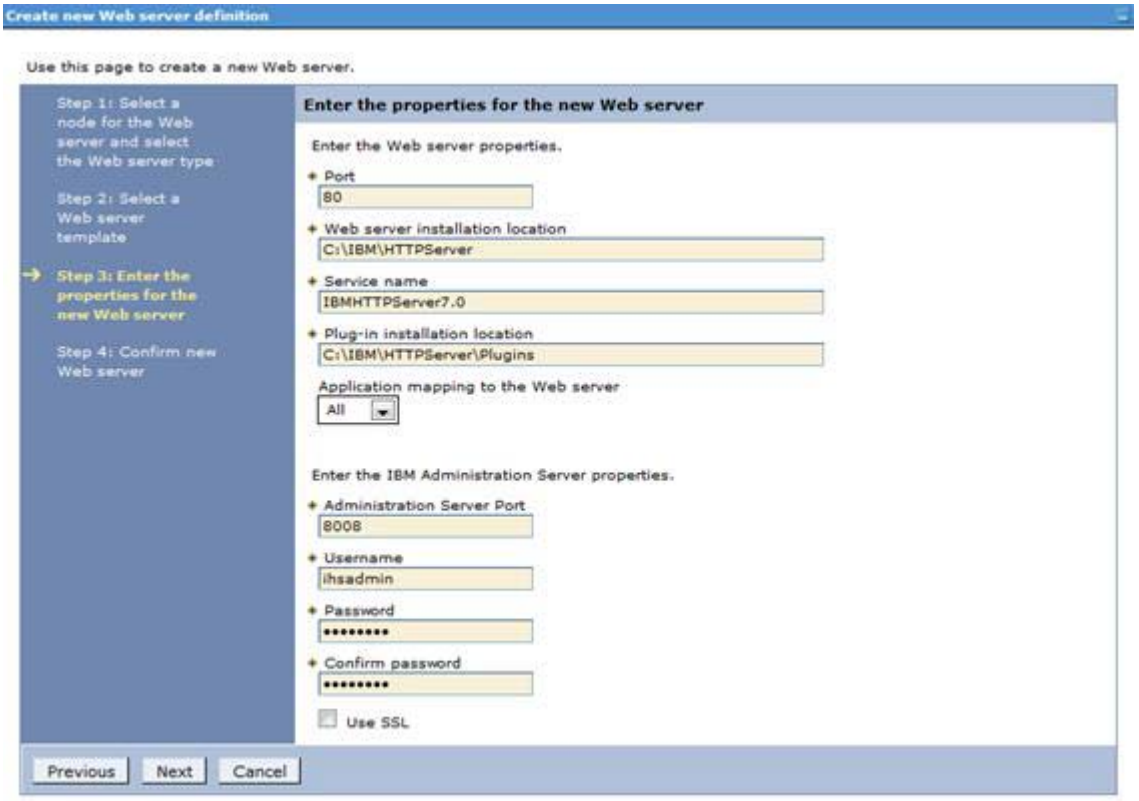


Figure 140. Enter the properties for the new web server

__ 5. Check the summary of your selections and click **Finish**.

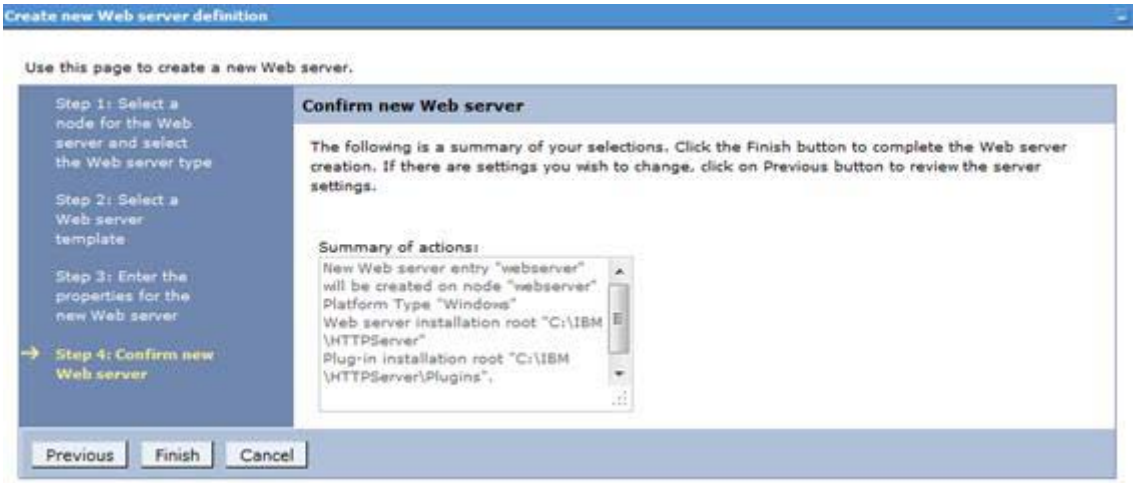


Figure 141. Confirming new web server

__ 6. Click **Save**.

Figure 142. Messages

__ 7. Click **Full Resynchronize**.

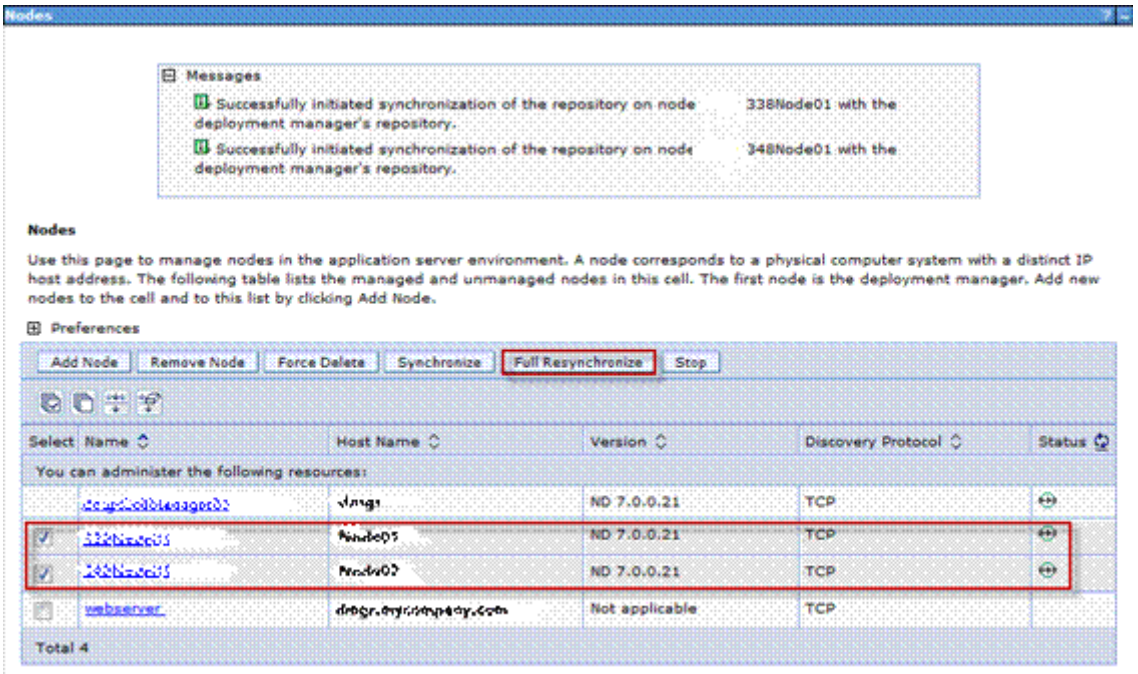


Figure 143. Full resynchronizing

The web server is successfully added as a server.

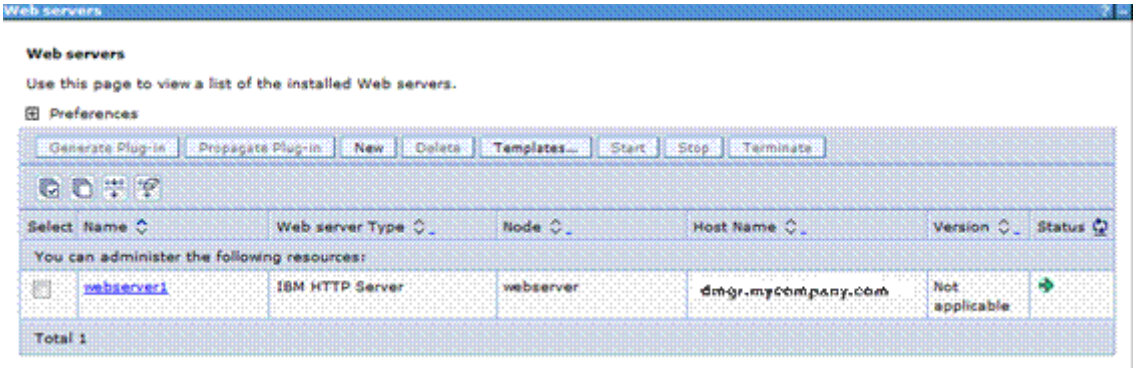


Figure 144. Web server is successfully added as a server

Configuring the HTTP Server for SSL

__ 1. The first step is to create a key file. Start the iKeyman utility by double-clicking the file **ikeyman.bat** from `C:\IBM\HTTPServer\bin`.

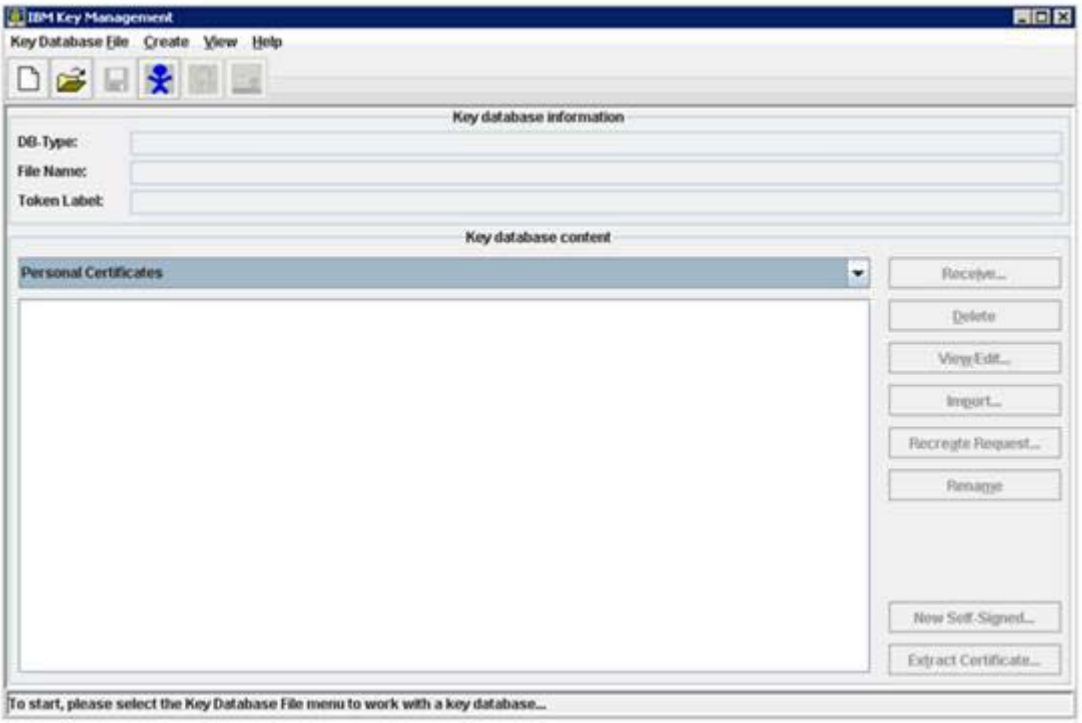


Figure 145. Creating a key file

__ 2. Select **Key Database File > New...**

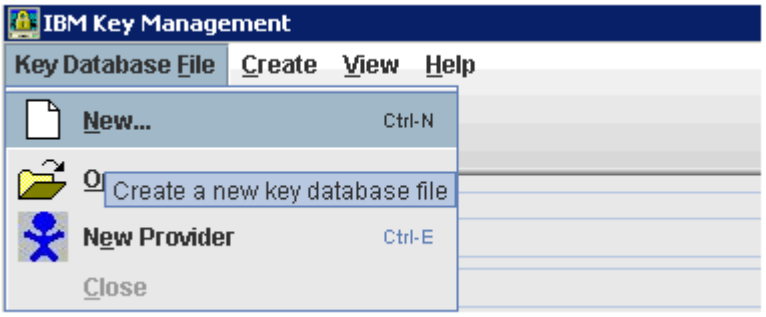


Figure 146. IBM Key Management

__ 3. Ensure that the key database type is selected as CMS. Input a name for the key file and location to store it and click **OK**.

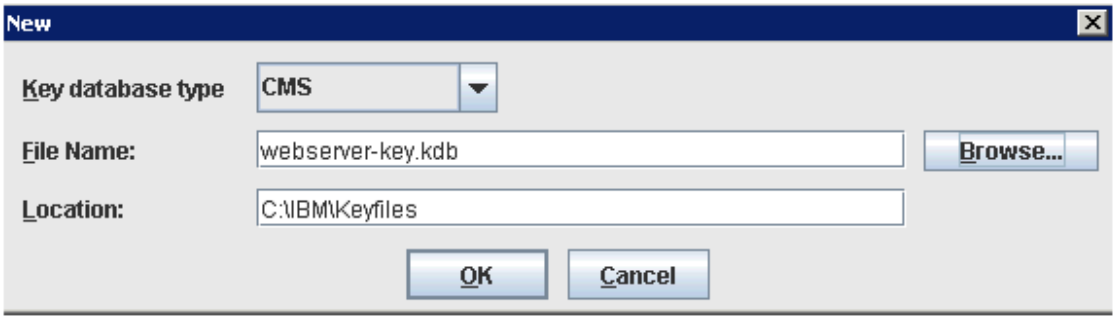


Figure 147. Entering a name and a location

__ 4. Enter a password and select **Stash password to a file**. Click **OK**.

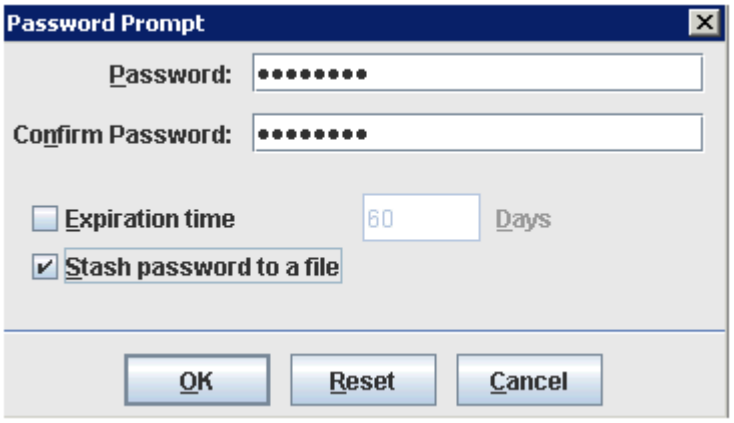


Figure 148. Password Prompt

You are returned to the iKeyman panel with the `webserver-key.kdb` opened.

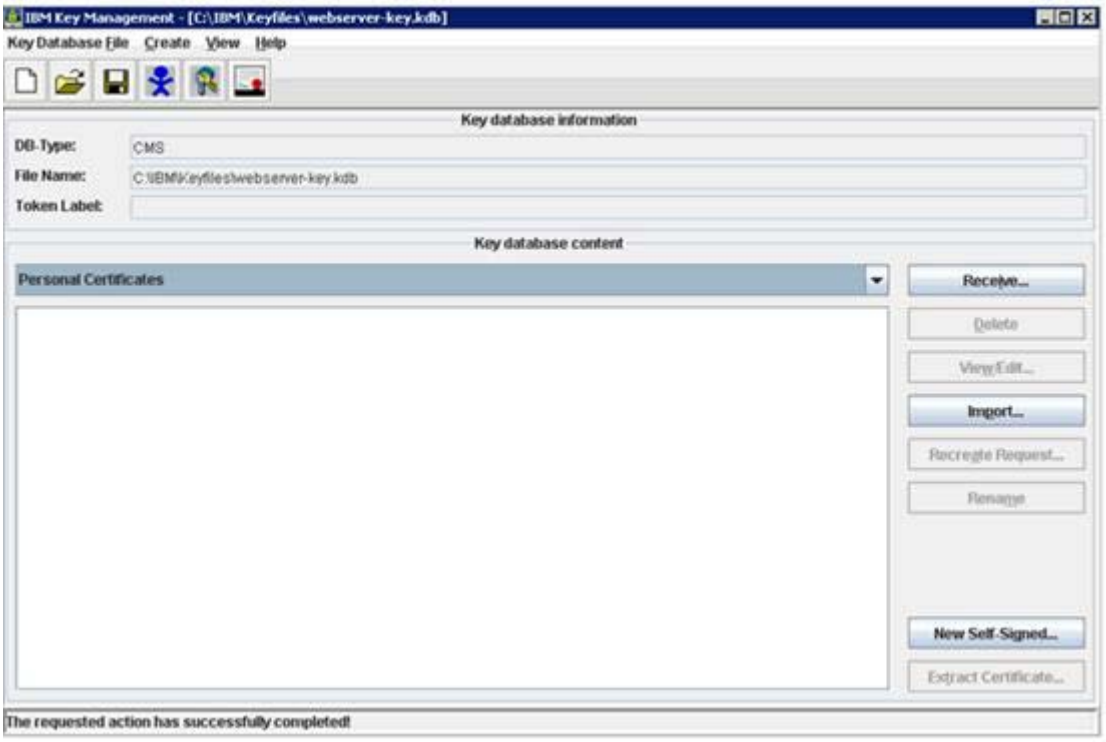


Figure 149. IBM Key Management

__ 5. Now create a self-signed certificate by using **Create > New Self-Signed Certificate**.

Figure 150. Creating a new self-signed certificate

__ 6. Input the label and other details as appropriate. Click **OK** to save the certificate.

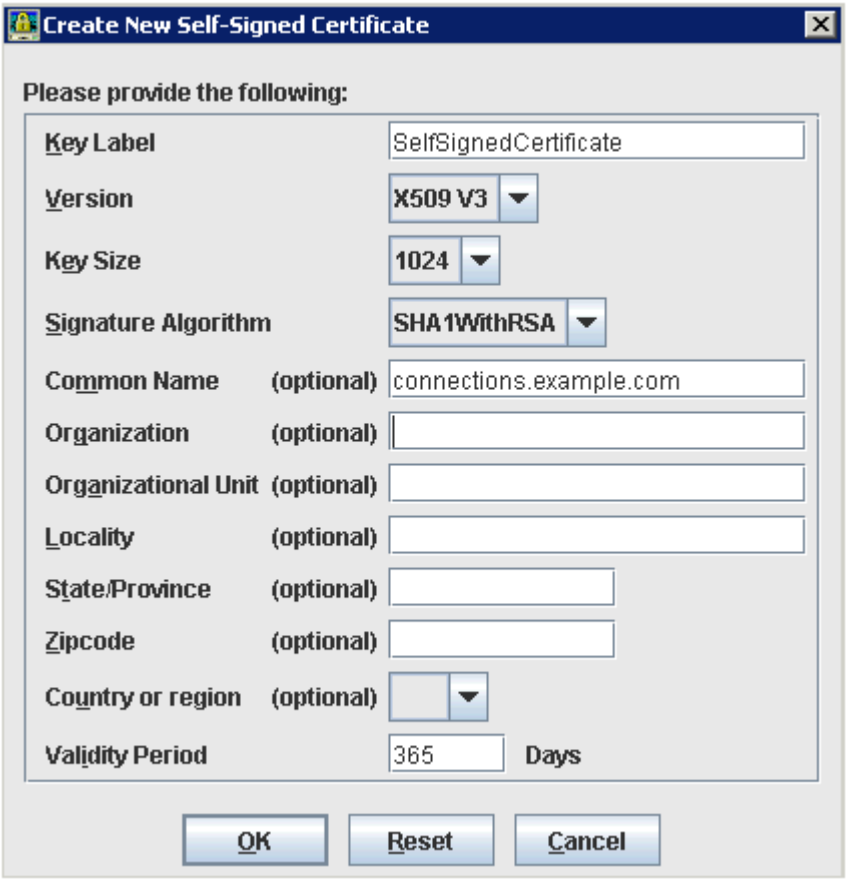


Figure 151. Creating a new self-signed certificate

The certificate now appears in the key file, as the following figure.

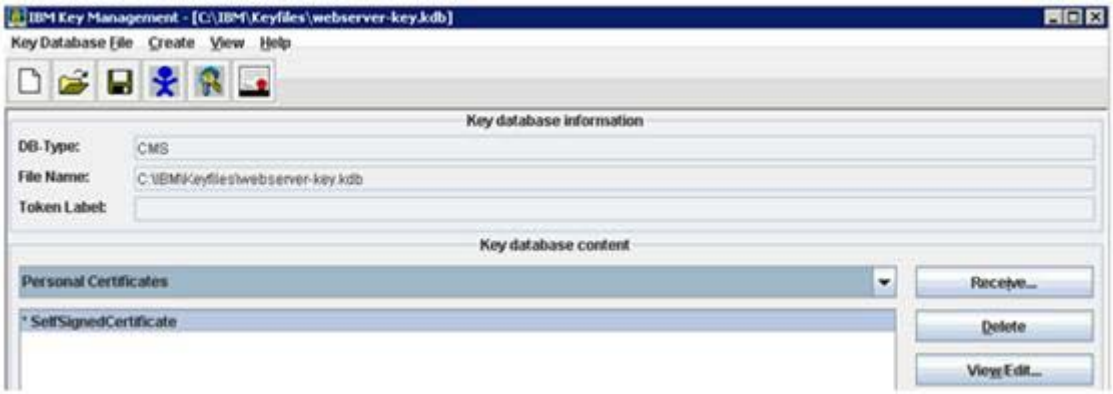


Figure 152. IBM Key Management

__ 7. Stop the IBM HTTP Server if started. When it stops, log in to the administrative console and configure the web server for SSL.

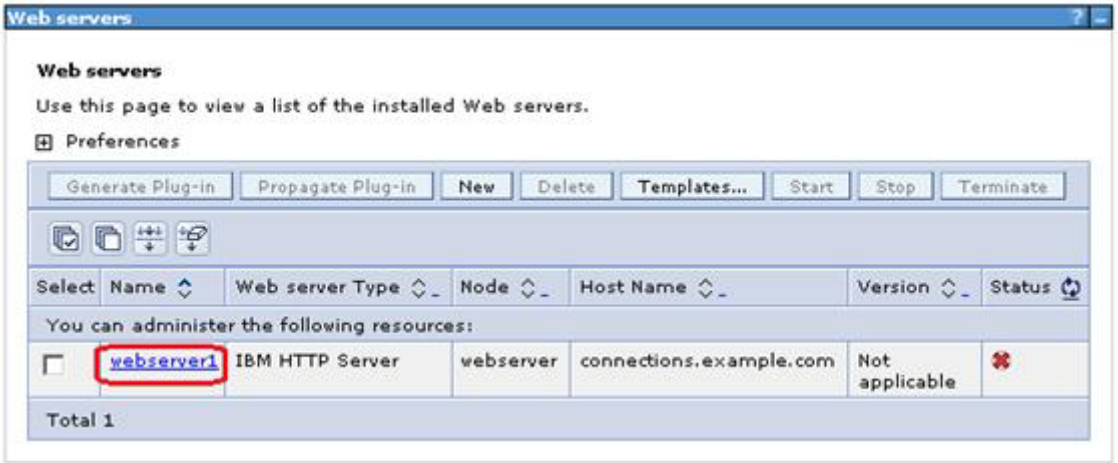


Figure 153. Web servers

__ 8. Click **Configuration File**.

Figure 154. Additional Properties > Configuration File

The `httpd.conf` opens in the browser as in the following figure.

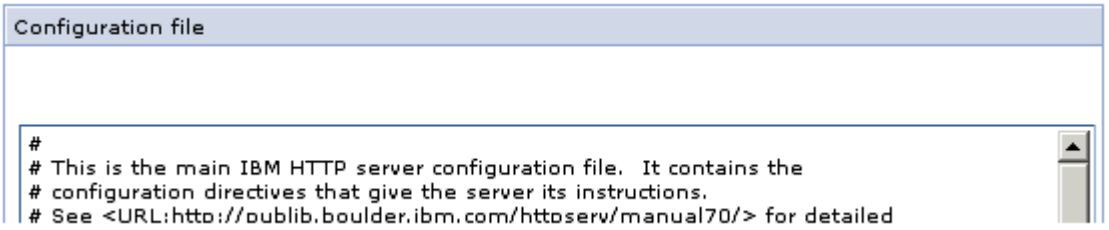


Figure 155. Configuration file

__ 9. At the bottom of the configuration, add the following lines to the `http.conf` file to load the SSL module by using the newly created key file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName dmgr.mycompany.com
SSLEnable
AllowEncodedSlashes On
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "/opt/IBM/Keyfiles/webserver-key.kdb"
SSLStashFile "/opt/IBM/Keyfiles/webserver-key.sth"
```

__ 10. Click **Apply** and then **OK**.

Figure 156. http.conf file

__ 11. Next, start the IBM HTTP Server. To verify that the SSL settings took effect correctly, type `https://connections.example.com` in a browser. If the IBM HTTP Server page appears over https, then this step was successful. You might need to accept the certificate into your browser as it is not signed or trusted. Click **Proceed anyway** to continue

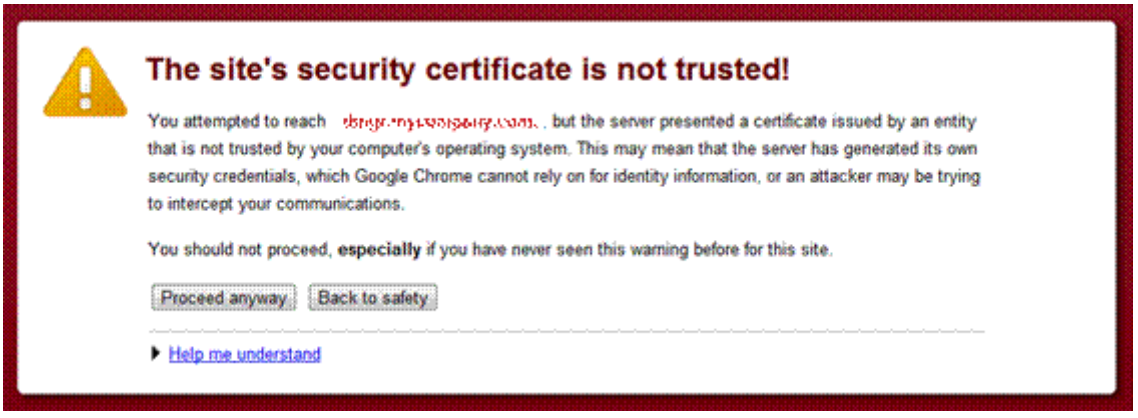


Figure 157. Security certificate

The WebSphere home page is now displayed.

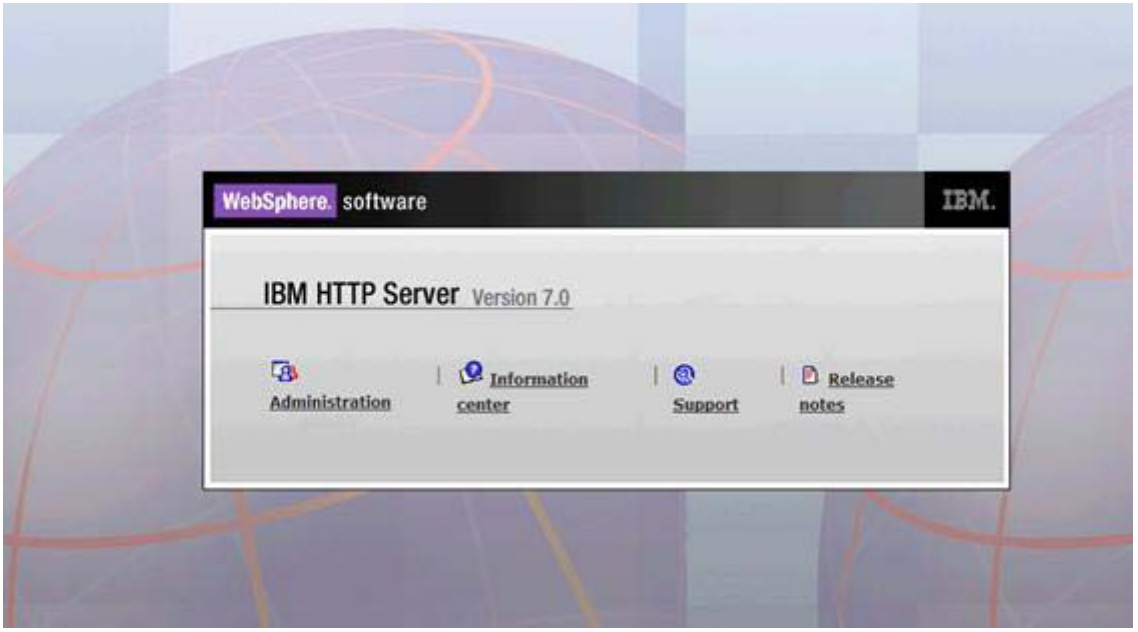


Figure 158. WebSphere software

Adding certificates to WebSphere truststore

__ 1. On the administrative console, go to **Security > SSL Certificate and Key Management > Key stores and certificates**. Click **CellDefaultTrustStore** to continue.

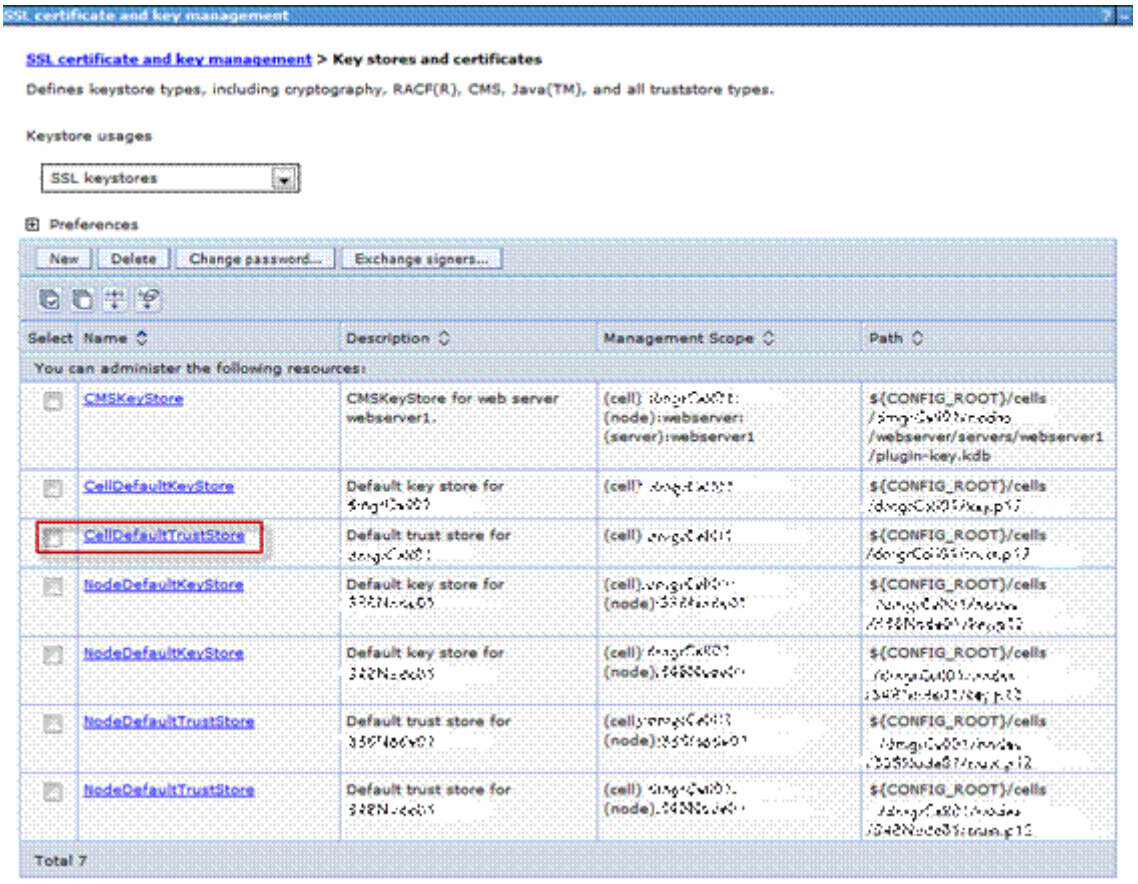


Figure 159. SSL certificate and key management: Key stores and certificates

__ 2. Select **Signer certificates** to continue.

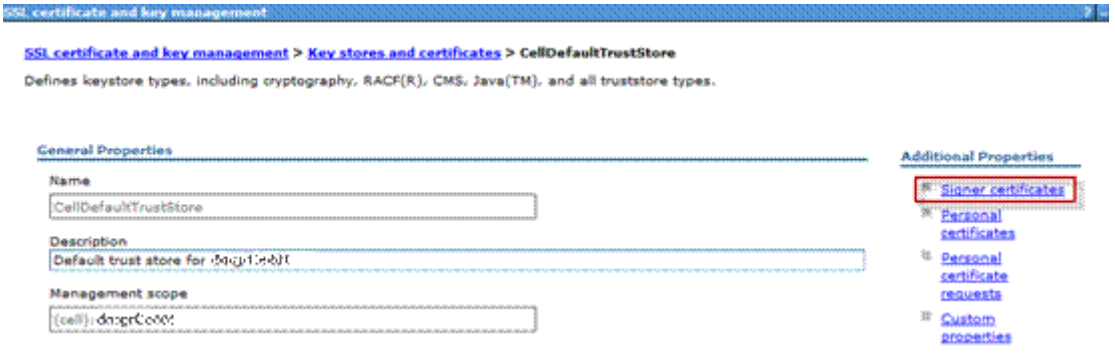


Figure 160. SSL certificate and key management: Key stores and certificates: CellDefaultTrustStore

__ 3. Click **Retrieve from port** to continue.

Figure 161. Retrieving from port

__ 4. Enter the host name of the web server and its SSL port (typically 443). Then, click **Retrieve Signer Information**, which retrieves the information that is shown at the bottom of the screen capture. Provide an alias for this signer certificate and click **OK** to add this certificate to the list of signers. Save this change and restart the HTTP server to apply the changes.

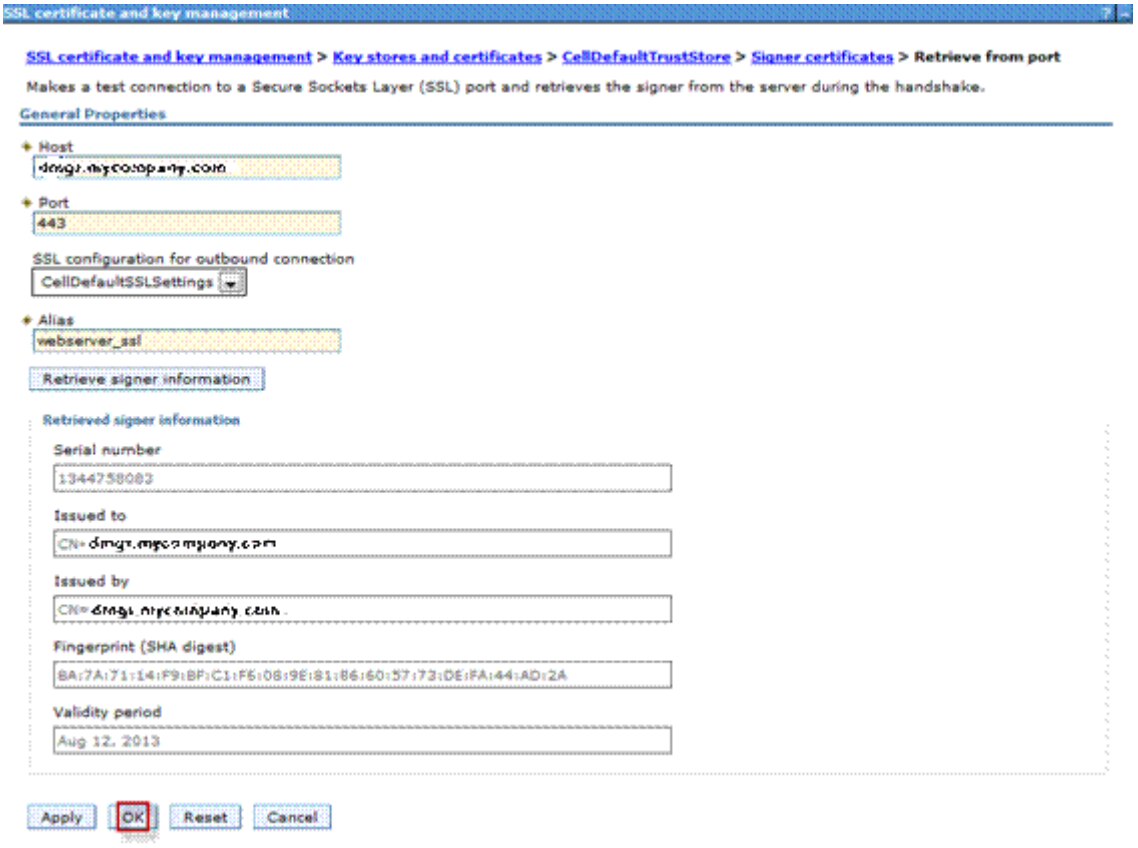


Figure 162. Entering the general properties of the web server

Updating web addresses used by IBM Connections to access content

__ 1. Using the wsadmin client, check out the `LotusConnections-config.xml` to a temporary directory. From this directory, this file must be edited so that all `href` and `ssl_href` values are updated to reflect the host name of the HTTP Server and do not include any port numbers.

```
    <sloc:href>
        <sloc:hrefPathPrefix>/blogs</sloc:hrefPathPrefix>
        <sloc:static href="http://dmgr.mycompnay.com:9084" ssl_href="https://dmgr.mycompnay.com:9444"/>
        <sloc:interService href="https://dmgr.mycompnay.com:9444"/>
    </sloc:href>
</sloc:serviceReference>

<sloc:serviceReference acf_config_file="acf-config-mf.xml" bootstrapHost="" bootstrapPort="" clusterName="CommunitiesCluster"
    <sloc:href>
        <sloc:hrefPathPrefix>/communities</sloc:hrefPathPrefix>
        <sloc:static href="http://dmgr.mycompnay.com" ssl_href="https://dmgr.mycompnay.com"/>
        <sloc:interService href="https://tamserver.mycompany.com"/>
    </sloc:href>
</sloc:serviceReference>

<sloc:serviceReference profiles_directory_service_extension_enabled="true" serviceName="directory"/>

<sloc:serviceReference acf_config_file="acf-config.xml" bootstrapHost="" bootstrapPort="" clusterName="DogearCluster" enabled
    <sloc:href>
        <sloc:hrefPathPrefix>/dogear</sloc:hrefPathPrefix>
        <sloc:static href="http://dmgr.mycompnay.com" ssl_href="https://dmgr.mycompnay.com"/>
        <sloc:interService href="https://tamserver.mycompany.com"/>
    </sloc:href>
</sloc:serviceReference>
```

Figure 163. LotusConnections-config.xml

__ 2. After this process is complete, save the file and check the file back in using the wsadmin client. After the file is checked back in, resynchronize the node so that this change is pushed out.

This completes the web server, SSL, and certificate configuration for this scenario. Now, when the application is started it can be accessed at `https://dmgr.ibm.com/<component`, where `<component` represents any of the Connections applications.

The commands to do all of the above are shown in the following figure (the previous updates take place after the check out command).

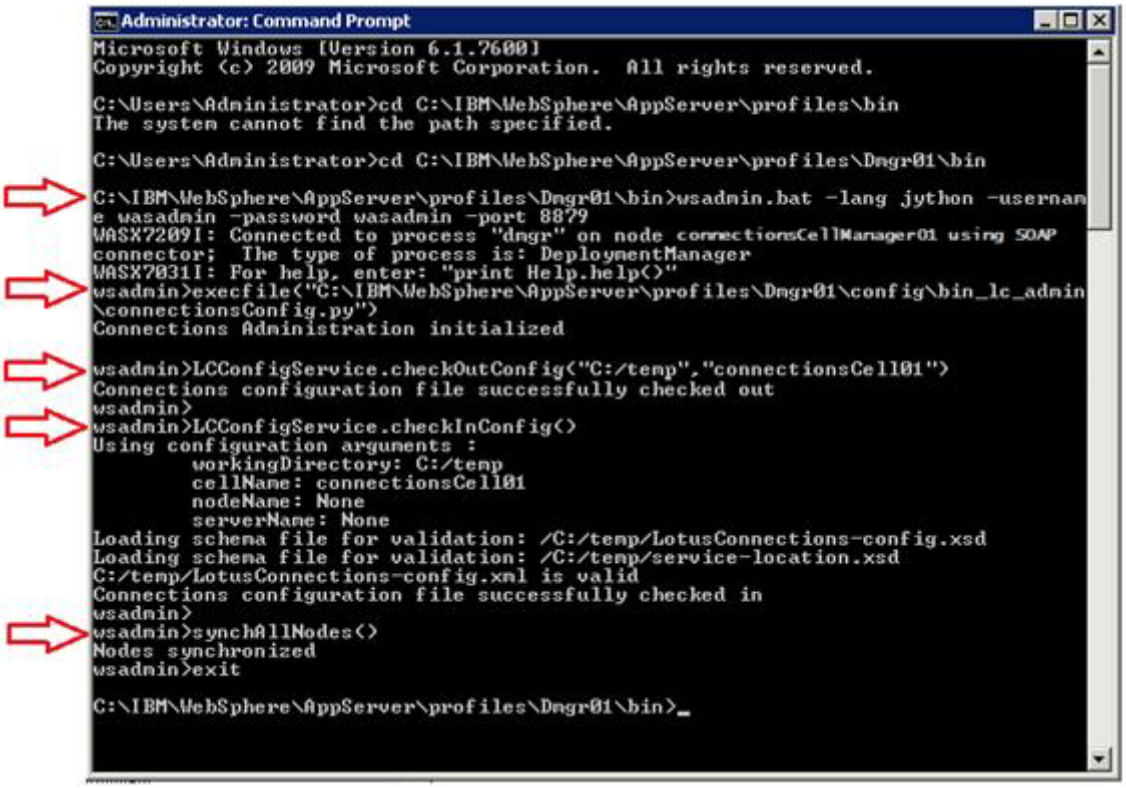


Figure 164. Administrator: Command Prompt

The following list provides the previous commands in a test format so that they can be copied and used again in your own deployment:

```
1: wsadmin.bat -lang jython -username wasadmin -password wasadmin -port 8879
2: execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin\connectionsConfig.py")
3: LCConfigService.checkOutConfig("C:/temp","connectionsCell01")
<Make changes to the checked out file>
4: LCConfigService.checkInConfig()
5: synchAllNodes()
```

Figure 165. Commands

Configuring application administrators for Blogs home page

__ 1. Log in to the administrative console on `dm.example.com` at `http://dm.example.com:9060/admin`.

__ 2. Go to **Applications > Application Types Web >WebSphere Enterprise Applications** and click **Blogs** as shown in the following figure.

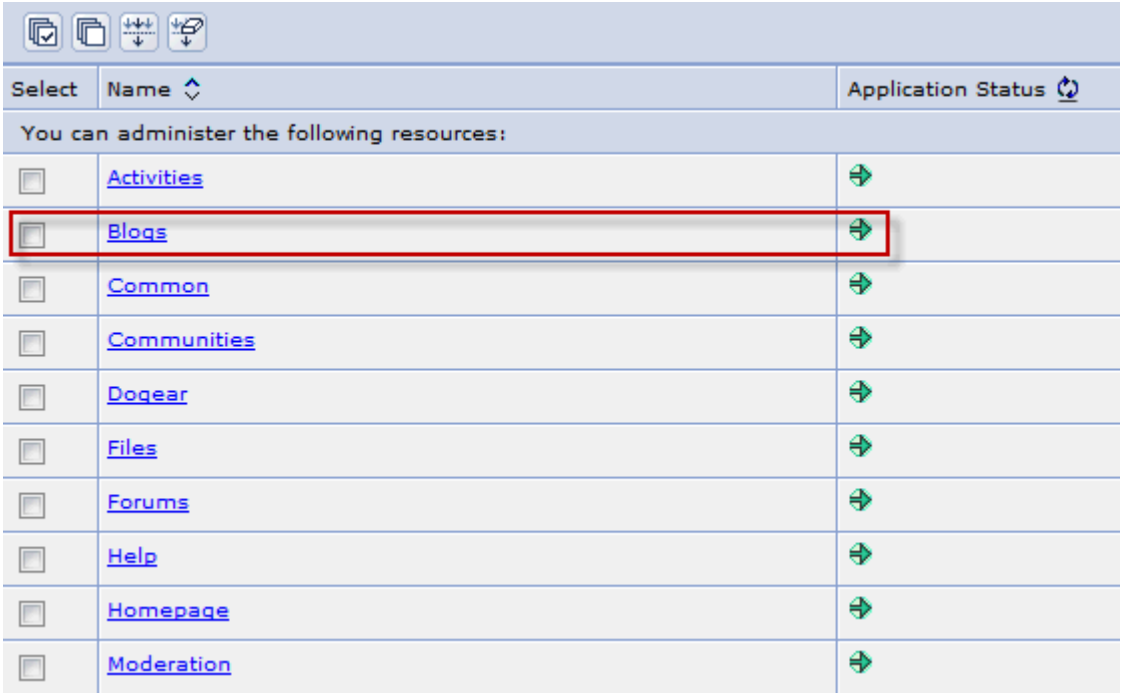


Figure 166. Administering the blog

__ 3. From the list of options for this application, select **Security role to user/group mapping**.

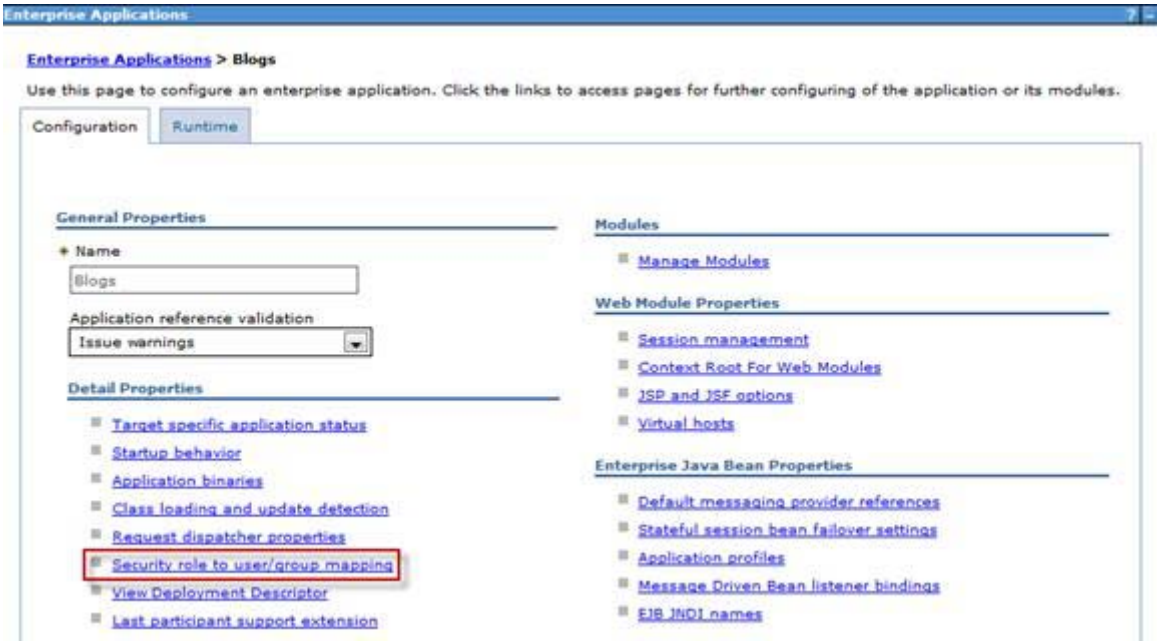


Figure 167. Security role to user/group mapping

__ 4. From the following panel, it is possible to map users and groups to different roles. In this example, no user is assigned as admin. Select admin and then select **Map Users...**

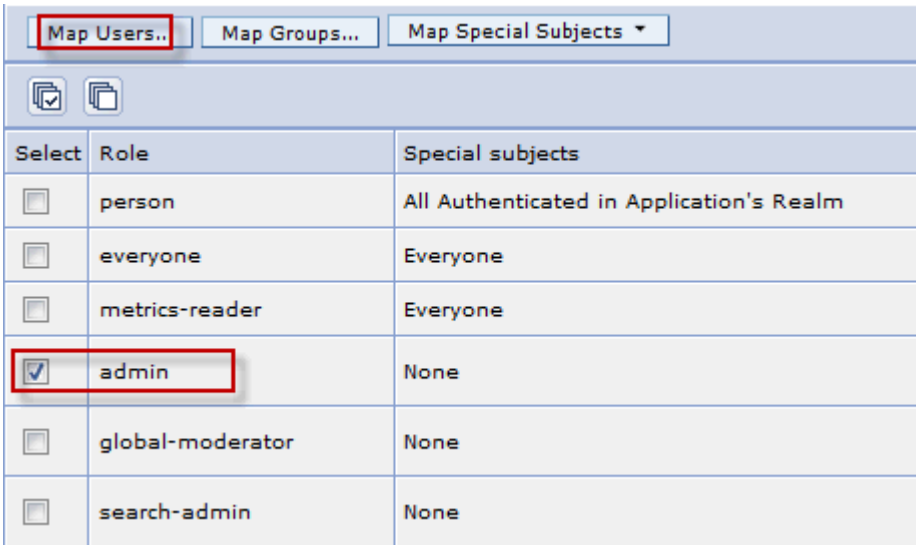


Figure 168. Mapping users

__ 5. Input the user name into the search string and click **Search**. When the required user is found, select their name and click the right arrow to assign this user to the role specified.

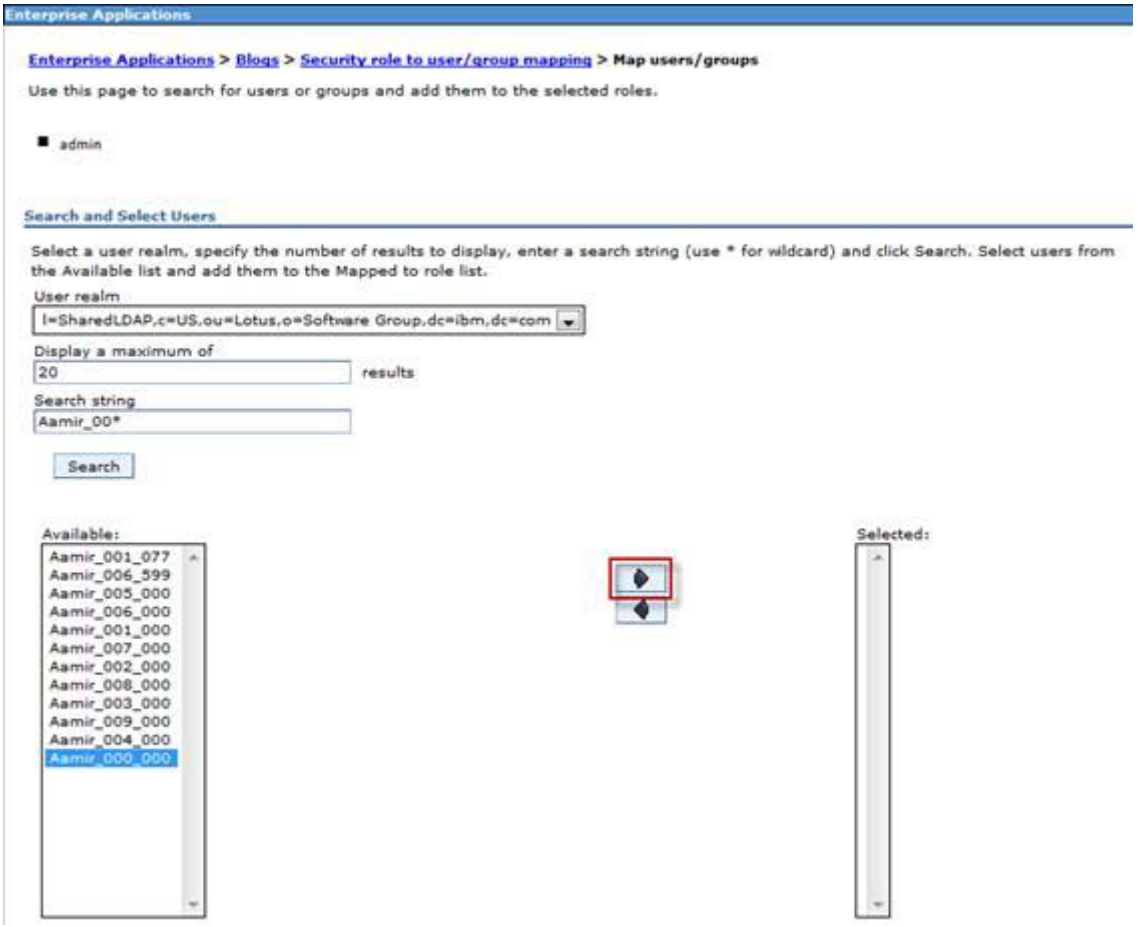


Figure 169. Enterprise Applications: Search and Select Users

__ 6. Click **OK** to return to the user: role mapping panel.

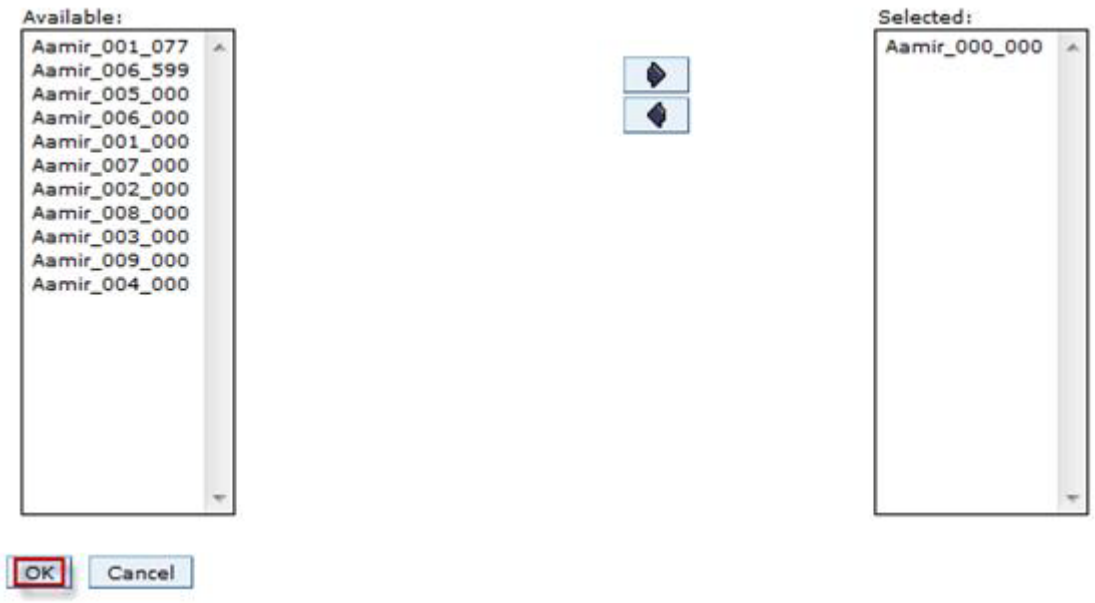


Figure 170. Returning to the user: role mapping panel

__ 7. Now the user `Aamir_000_000` is assigned as an administrator in Blogs. Click **OK** to save this change.

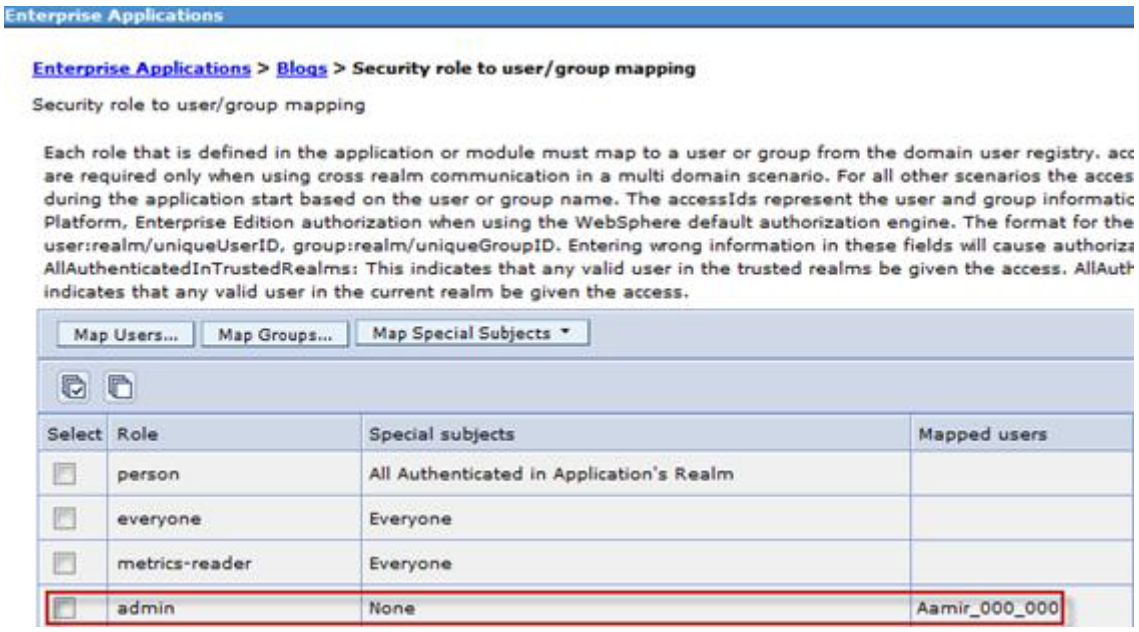


Figure 171. User that is assigned as an administrator in Blogs

__ 8. Save the change by clicking **Save** as shown in the following figure.

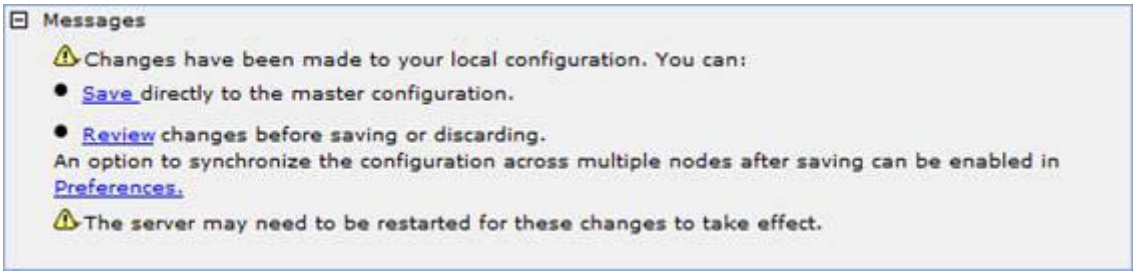


Figure 172. Messages

Now that you assigned an admin user in blogs. Follow the same procedure to map groups or users to different roles in the various applications, such as admin or moderator where appropriate. It is not required to restart the servers for this change to take effect. However, it might take a few minutes for the change to take effect across the nodes in the deployment.

Verification point of application access

Restart the deployment configuration and verify that you can log on to the home page and you can access all applications as an Admin and as a Non-Admin user then do the following things: Create a community, blog, wiki, forum, upload files and so on.

Example

```
http://dmgr.mycompany.com/activities/
http://dmgr.mycompany.com/communities/
http://dmgr.mycompany.com/forums/
http://dmgr.mycompany.com/profiles/
http://dmgr.mycompany.com/blogs/
http://dmgr.mycompany.com/dogear/
http://dmgr.mycompany.com/files/
http://dmgr.mycompany.com/wikis/
http://dmgrmycompany.com/homepage/
http://dmgr.mycompany.com/search/
http://dmgr.mycompany.com/news/
```

Enabling Fast Downloads for Files and Wikis

The last item that we want to do is enable fast download for files and wikis. It is an optional step for customers but it is recommended for all SVT systems to run with it.

__ 1. On your deployment manager, go to `C:\IBM/Connections\plug-ins\ihs\mod_ibm_local_redirect\linux_ia32-ap22`. You see a file that is called `mod_ibm_local_redirect.so` located there.

   __ a. Copy this file your HTTP Server under > C:\IBM\HTTPServer\modules\

Important

Remember to do this step; otherwise, when you download files, the file size is 0.

   __ b. Now edit the `httpd.conf` under `C:\IBM\HTTPServer\conf`:

   - LoadModule ibm_local_redirect_module modules/mod_ibm_local_redirect.so
   - LoadModule env_module modules/mod_env.so (it might already exit to check your existing file).

__ 2. Also, add the following sections. Paths must change based on installation:

```
Alias /downloadfiles C:\IBM\SharedArea\files\upload
Alias /downloadwikis C:\IBM\SharedArea\wikis\upload

<Directory C:\IBM\SharedArea\files\upload>
Order Deny,Allow
Deny from all
Allow from env=REDIRECT_FILES_CONTENT
</Directory>

<Directory C:\IBM\SharedArea\wikis\upload>
 Order Deny,Allow
Deny from all
 Allow from env=REDIRECT_WIKIS_CONTENT
</Directory>

<Location /files>
 IBMLocalRedirect On
 IBMLocalRedirectKeepHeaders
X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ET
ag,Content-Language,Set-Cookie
 SetEnv FILES_CONTENT true
</Location>

<Location /wikis>
 IBMLocalRedirect On
 IBMLocalRedirectKeepHeadErs
X-LConn-Auth,Cache-Control,Content-Type,Content-Disposition,Last-Modified,ET
ag,Content-Language,Set-Cookie
 SetEnv WIKIS_CONTENT true
</Location>
```

__ 3. Finally, edit the `files-config.xml` and `wikis-config.xml` files under `C:\IBM\WebSphere\DeploymentManager\profiles\Dmgr01\config\cells\dmgrCell01\LotusConnections-config` on your deployment manager and change:

```
<download>
<modIBMLocalRedirect enabled="true"
hrefPathPrefix="/downloadfiles" />
<stats>
and
<download>
<modIBMLocalRedirect enabled="true"
hrefPathPrefix="/downloadwikis" />
<stats>
```



```
<download>
  <modIBMLocalRedirect enabled="true"
    hrefPathPrefix="/downloadfiles" />
  <stats>
    <logging enabled="true" />
  </stats>
</download>
```

Figure 173. files-config.xml

```
<download>
  <modIBMLocalRedirect enabled="true"
    hrefPathPrefix="/downloadwikis" />
  <stats>
    <logging enabled="false" />
  </stats>
</download>
```

Figure 174. wikis-config.xml

__ 4. When changed, make sure to synch the changes to your nodes. Restart HTTP server and Connections cluster servers.

Tuning JVM heap sizes

The following JVM tuning is compatible only with a 64-bit operating system as described in this scenario. In non 64-bit environments, consult the IBM Connections tuning guide.

This section contains the suggested values for JVM sizes for servers that host each application. When increasing the heap size, it is a good idea to monitor overall memory consumption to ensure that your system can provide the necessary memory allocations without excessive paging.

Table 1:

Applications	Servers	Initial Heap Size (MB)	Maximum Heap Size (MB)
Activities, Communities, Profiles, Forums	LCCluster1_server1 LCCluster1_server2	512	2048
Blogs, Bookmarks, Wikis, Files	LCCluster2_server1 LCCluster2_server2	512	2048
Search, News, Home page, Mobile	LCInfraCluster_server1 LCInfraCluster_server2	768	3072

In this scenario, the node computers have 12 GB to facilitate the total possible maximum JVM load of just under 7.5 GB, which leaves 4 GB available for the operating system and possible tweaks to the maximum heap sizes in the future based on the system performance over time.

Here is how to set this value for one server (activitiesCluster_server1).

Note

Repeat this process for each subsequent server.

__ 1. Open the Deployment Manager and go to **Server Types > WebSphere application servers**. Click **WebSphere application servers**.

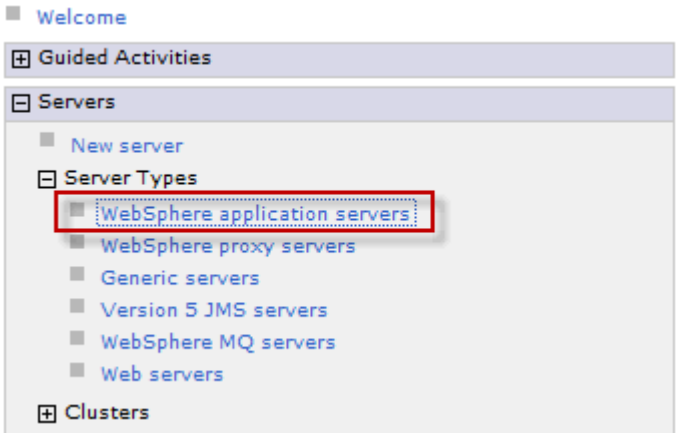


Figure 175. WebSphere application servers

__ 2. Click **LC Clusters server1**.

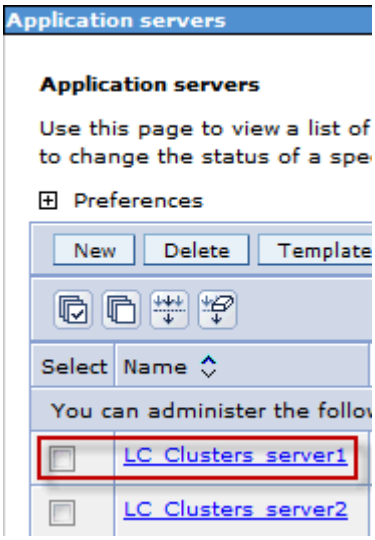


Figure 176. Selecting the application server

__ 3. Find the Server Infrastructure section and click **Process definition**.

Figure 177. Server infrastructure

__ 4. Click **Java Virtual Machine** as shown in the following figure.

Figure 178. Additional Properties

__ 5. Input the initial heap and maximum heap size for this server as per the information included in Table 1.

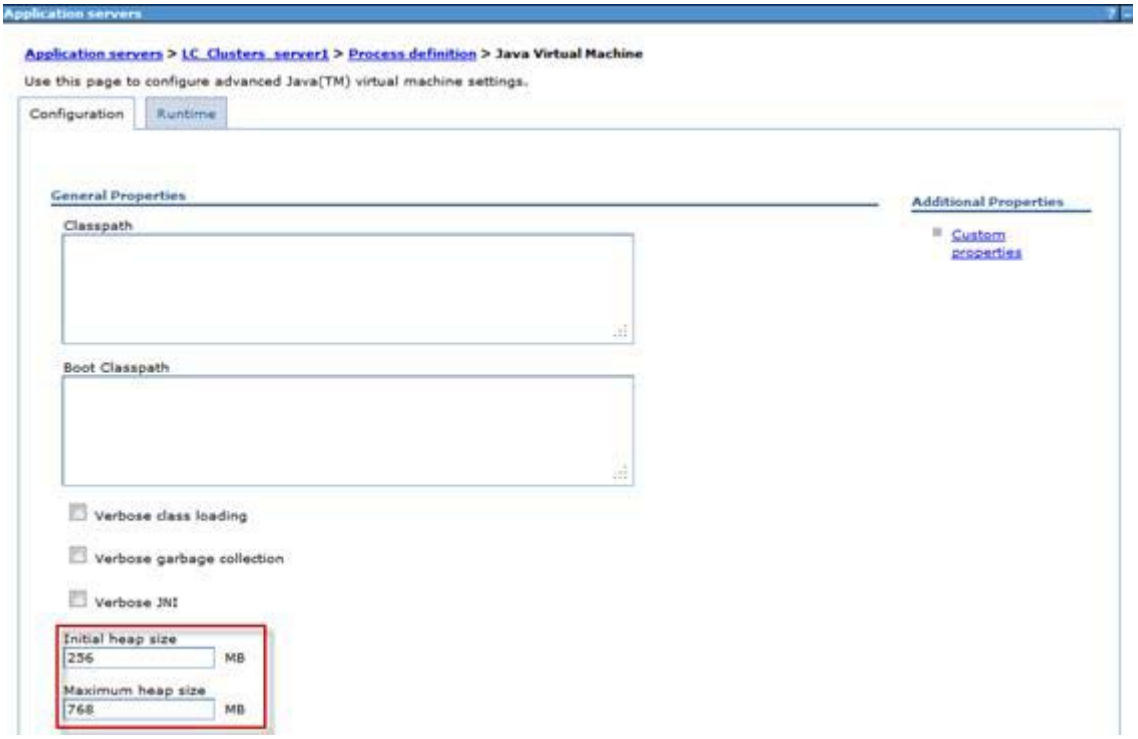


Figure 179. Initial heap size and Maximum heap size

__ 6. Click **OK** and save this change. Repeat this process for all the servers to update.

2. Integration portfolios

Tivoli Access Manager integration

Tivoli Access Manager Prerequisites

Information

Lotus Connections 4.0 is set up and working with the IBM HTTP Server without issue.

The J2C Authentication Alias `connectionsAdmin` is a user who exists on the LDAP and has administrative rights on the administrative console. `ConnectionsBus` is also updated with the same user as your `connectionsAdmin` user.

__ 1. Ensure the realm name in the Federated Repositories section of the Deployment Manager uses the same value as LDAP name, including the port number (for example, `ldap.example.com:389`).

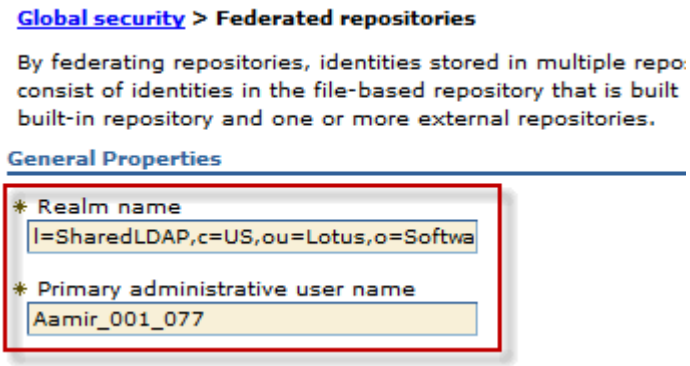


Figure 180. Federated repositories: General Properties

__ 2. Set the Single sign-on domain to the same as on the Tivoli Access Manager server.

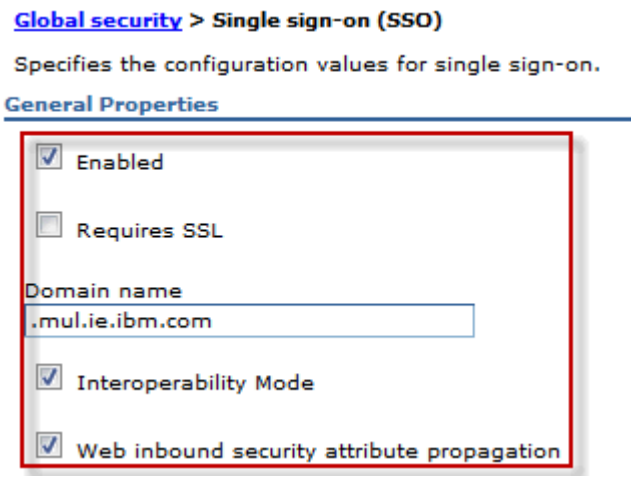


Figure 181. Single sign-on (SSO)

__ 3. Check under **Global security > Web security: General Settings** that the option to use available authentication data when an unprotected URI is accessed is checked. If not, click the **Authenticate only when the URI is protected** and check **Use available authentication data when an unprotected URI is accessed**. Click **OK** and save the change.

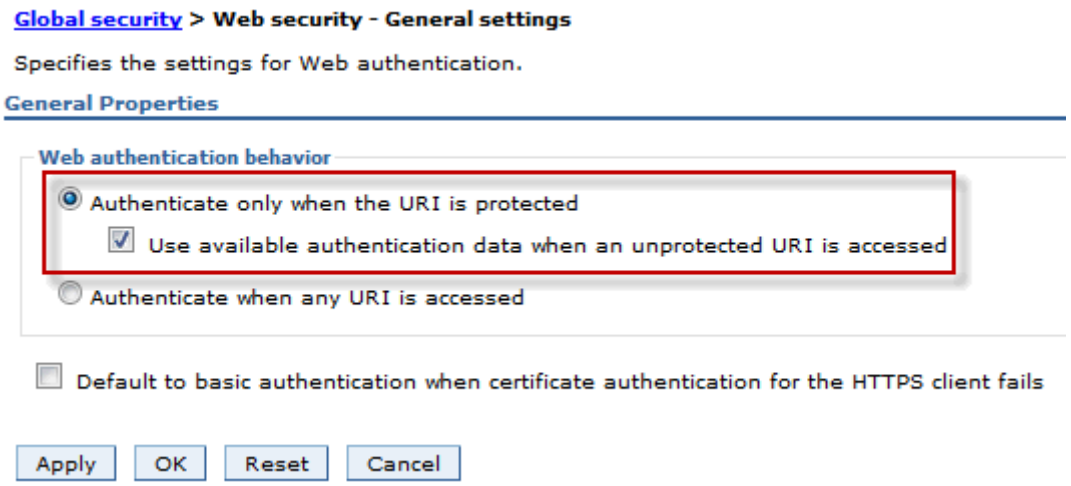


Figure 182. Web authentication behavior

Now you can begin the Tivoli Access Manager integration steps. There are several ways to configure SSO but this procedure describes one approach: using WebSphere Application Server LTPA key and WebSEAL Transparent Junctions.

Extracting the LTPA Token from Deployment Manager

__ 1. On the Deployment Manager, go to **Security > Global Security** and click LTPA from the Authentication section.

Figure 183. Global security: LTPA

__ 2. At the bottom of the following screen is a cross-cell single sign-on section. Enter a password and file name (including full path) and click **Export keys**.

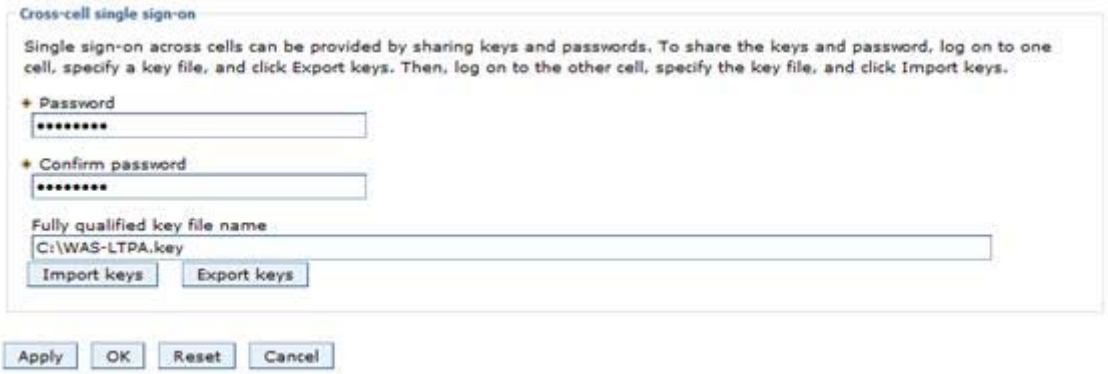


Figure 184. Cross-cell single sign-on

__ 3. The following message indicates success. Now copy this key and append it to the work request.

Figure 185. Message

Note

If you modify any federated repository settings in the future (such as realm name), you must re-export your LTPA keys and copy them to the Tivoli Access Manager server again.

Extracting the IBM HTTP Server SSL certificate

__ 1. Open `HTTPServer\bin\ikeyman.bat` and from there select **Key Database File > Open**. Open the `plug-in-key.kdb` that contains the IBM HTTP Server WebSphere Application Server keys and extract the Personal Certificate.

Note

Default password is `WebAS`.

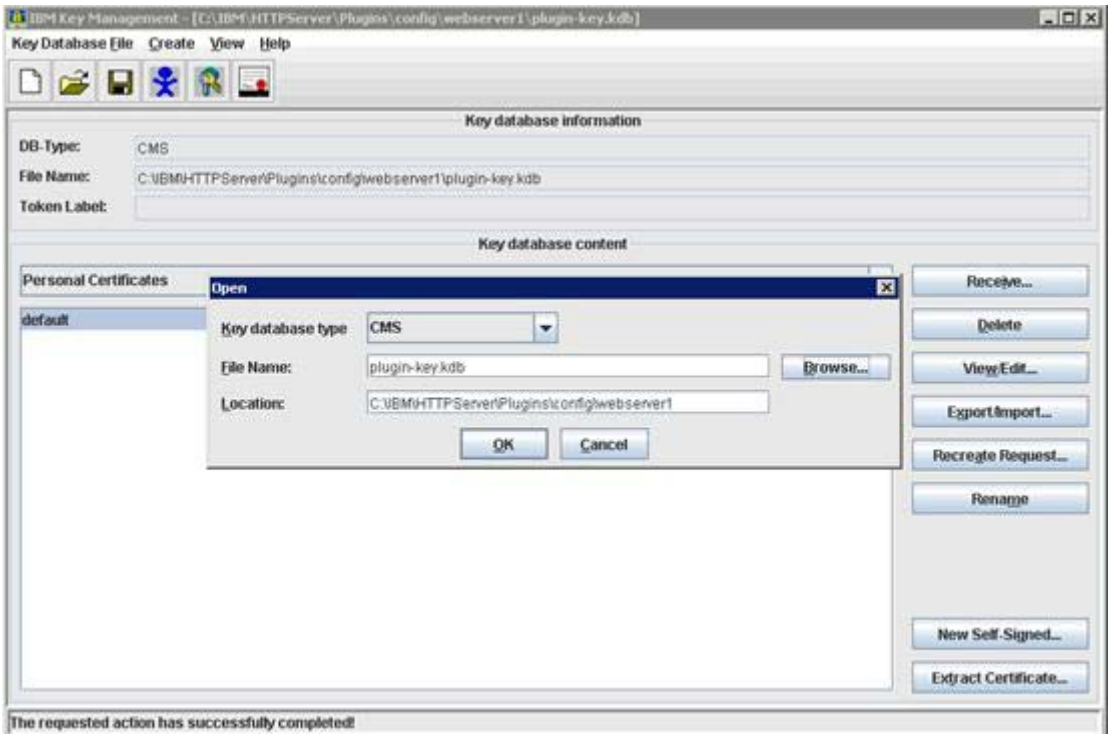


Figure 186. IBM Key Management

__ 2. Click **Extract Certificate** from the personal certificates screen and provide a path and name for the certificate file (leaving the `.arm` extension).

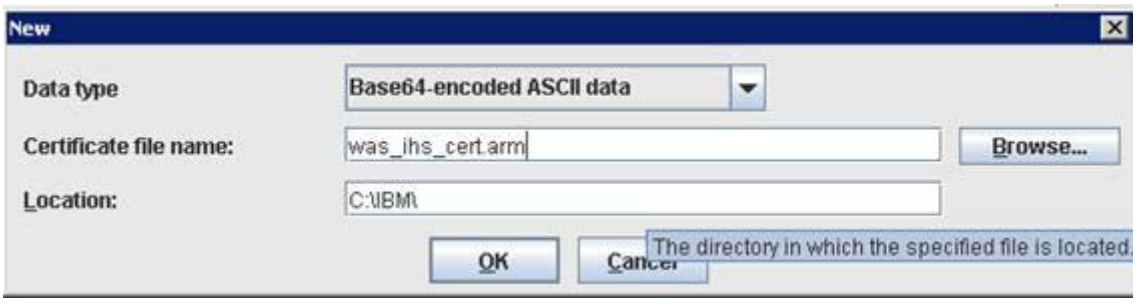


Figure 187. Providing path and name for the certificate file

__ 3. Enter the location where you want to copy the certificate and click **OK** to finish.

Enabling Tivoli Access Manager for Connections

The following iDoc configures IBM Connections for single sign-on with IBM Tivoli Access Manager. You can find the complete process step by step under:

`http://www-10.lotus.com/ldd/lcwiki.nsf/xpDocViewer.xsp?lookupName=IBM+Connections+4.0+documentation#action=openDocument&content=catcontent&ct=prodDoc.`

Configuring the LotusConnections-config.xml

When the WTI request is completed, all of the relevant Tivoli Access Manager junctions and configurations are set up for this deployment. You can now begin to configure Connections and the HTTP Server for Tivoli Access Manager integration. Begin by configuring the `LotusConnections-config.xml` and the `files-config.xml`.

Various changes are required in the LotusConnections-config.xml to enable Connections to work with Tivoli Access Manager. Begin by checking out the configuration file or editing it directly (be careful to make a backup of it if you choose to edit it directly).

__ 1. Open the `LotusConnections-config.xml` in a text editor and make the following changes.

Update the values for dynamicHosts and interservice URL attributes:

__ a. Find the dynamicHosts element and set the enabled flag to true.

__ b. Set the dynamicHost href and ssl_href to that of the Tivoli Access Manager server host name.

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

__ c. Update the interservice URLs for each of the applications to that of the Tivoli Access Manager server host name. For example, the entry for activities becomes:

```
    <sloc:href>
        <sloc:hrefPathPrefix>/dogear</sloc:hrefPathPrefix>
        <sloc:static href="http://dmgr.mycompnay.com" ssl_href="https://dmgr.mycompnay.com"/>
        <sloc:interService href="https://tamserver.mycompany.com"/>
    </sloc:href>
</sloc:serviceReference>
```

Figure 188. Interservice URLs

Hint

Do a find and replace to update these interservice URLS quickly by finding the line that is required with the original href and replacing it with the full new line that includes the Tivoli Access Manager server. For example:

Find: `<sloc:interService href="https://dmgr.mycompany.com"/>`

Replace: `<sloc:interService href="https://tamserver.mycompany.com"/>`

__ d. Save these changes.

__ 2. Add the Tivoli Access Manager customAuthenticator property to the configuration file. In the `LotusConnections-config.xml`, do the following step:

__ a. Find the default `customAuthenticator` setting and comment it out using <!-- and -->. This changes the default entry from:

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

Figure 189. customAuthenticator setting

To:

```
<!--customAuthenticator name="DefaultAuthenticator"/-->
```

Figure 190. customAuthenticator setting

__ b. Now create a `customAuthenticator` called `TAMAuthenticator` and add an attribute that is called `CookieTimeout`. This attribute is set to be equal to or less than the maximum timeout (60 minutes by default) and idle timeout (10 minutes by default) values configured on Tivoli Access Manager (which the WTI team does not change unless requested), so set this value to 10. Now the updated Authenticator looks as follows:

```
<customAuthenticator name="TAMAuthenticator">
  <attribute key="CookieTimeout" value="10" />
</customAuthenticator>
```

Figure 191. Updated Authenticator

__ c. Save these changes.

When all of the above changes are made save the `LotusConnections-config.xml` (and check it in if required). You must resynchronize your nodes and restart Connections for the change to take effect.

Configuring files-config.xml

__ 1. The `files-config.xml` must be updated so that the `reauthenticateAndSaveSupported` property is set to false. This ensures that when an application detects a session timeout, users must log in again through the SSO authentication mechanism.

This change looks as follows:

```
<security reauthenticateAndSaveSupported="false">
<logout href="/files/ibm_security_logout" />
<inlineDownload enabled="false" />
</security>
```

__ 2. Save the change and resynchronize nodes and restart Connections for these changes to take effect.

Configuring HTTP Server for Tivoli Access Manager

The web server must now be configured to handle logout from Tivoli Access Manager correctly.

To correctly configure the web server to handle the user clicking the logout button in a Tivoli Access Manager environment, some changes are required to the `httpd.conf` to implement this post-logout behavior. This ensures that the user is correctly and securely logged out.

__ 1. Open this file in a text editor and add the following rules:

__ 2. Uncomment the line that contains `LoadModule rewrite_module modules/mod_rewrite.so` if not already done so that the rewrite module is enabled.

__ 3. To capture requests to `/ibm_security_logout` and redirect them to `/pkmslogout`, add the following rewrite rules to the http and https sections of the file:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
```

The following example illustrates how it would look in the `httpd.conf` file after the changes are implemented:

```
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName dmgr.mycompany.com
SSLEnable
RewriteEngine On
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteRule ^/(.*) /pkmslogout [noescape,L,R]
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "C:\IBM\HTTPServer\Keys\webserver-key.kdb"
SSLStashFile "C:\IBM\HTTPServer\Keys\webserver-key.sth"
```

__ 4. Save and close the `httpd.conf` file.

__ 5. Restart IBM HTTP Server.

When all of the above changes are made, stop all application servers and all nodes, and then restart the deployment manager, all the nodes, and all the application servers. You should also restart your web server.

IBM Connections with Tivoli Access Manager enabled

The next time that you start Connections, you should access it with the Tivoli Access Manager URLs, that is, `https://tamserver.mycompany.com/profiles`. You then see the Tivoli Access Manager login screen, and when you enter an authenticated LDAP user name you are logged in to Connections successfully as the same user.

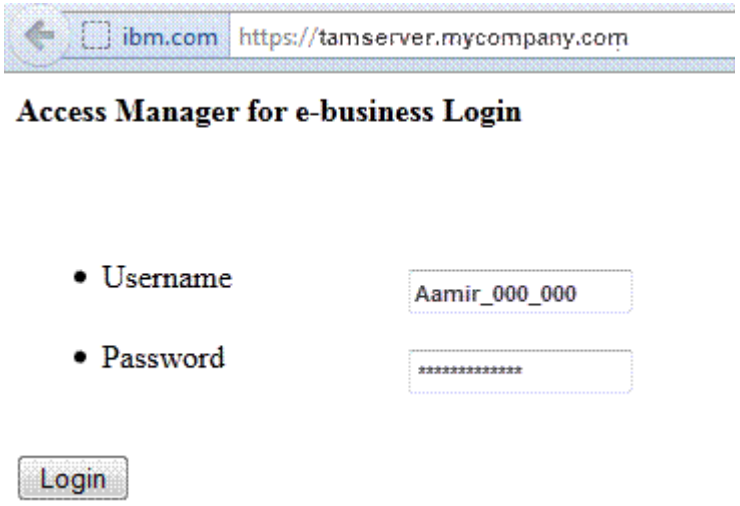


Figure 192. Accessing Manager for e-business Login

Figure 193. Logged in to the Manager for e-business

Troubleshooting Tivoli Access Manager issues

The following few issues occurred in the production of this document and might help in the resolution of other issues that are encountered in subsequent deployments.

1. Can only log in to Profiles:

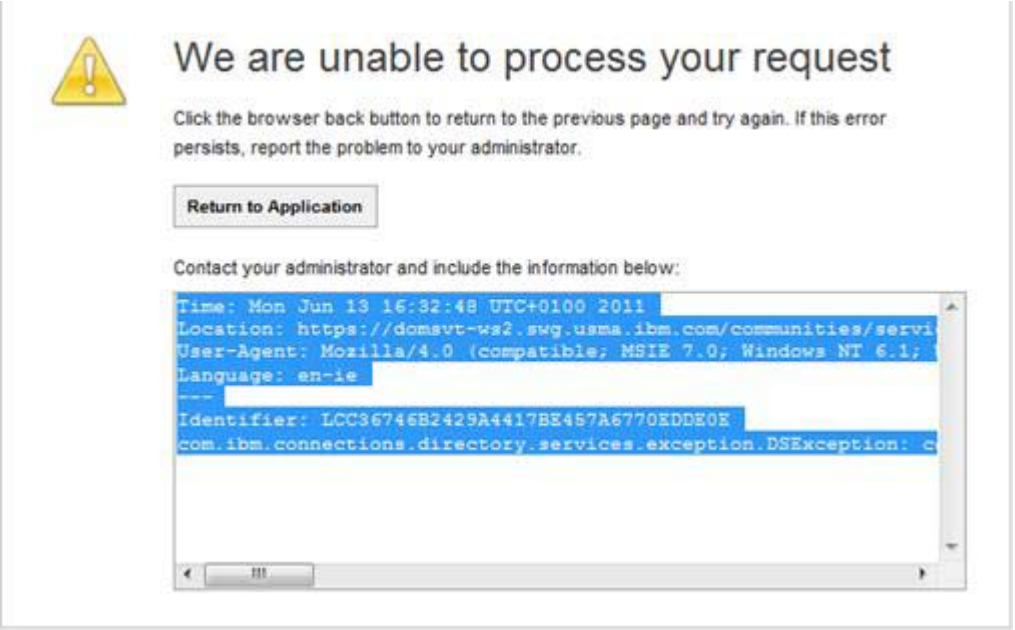


Figure 194. Warning message: We are unable to process your request

```
Time: Mon Jun 13 16:30:13 UTC+0100 2011
Location: https://myserver.example.com/communities/service/html/mycommunities
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64; Trident/5.0;
SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC
6.0; .NET4.0C)
Language: en-ie
---
Identifier: LC1B6AB692CD3E41DCB50F6265121151CB
com.ibm.connections.directory.services.exception.DSException:
com.ibm.connections.directory.services.exception.DSOutOfServiceException:
com.ibm.connections.httpClient.CustomAuthClientRuntimeException: CLFRO0151E:
remote host 'domsvt-ws2.swg.usma.ibm.com' from targeted URL
'https://myserver.example.com/profiles/dsx/instance.do?login=SusanAdams1' is not
qualified by SSO domain name setting!
```

- This issue is caused by having connection in the `.mul.ie.ibm.com` domain and Tivoli Access Manager is in the `.swg.usma.ibm.com` domain. To fix the issue, update the WebSphere Application Server SSO domain to a common name. In this case, just `.ibm.com` as in the following figure. Restart and resynch for the change to take effect.

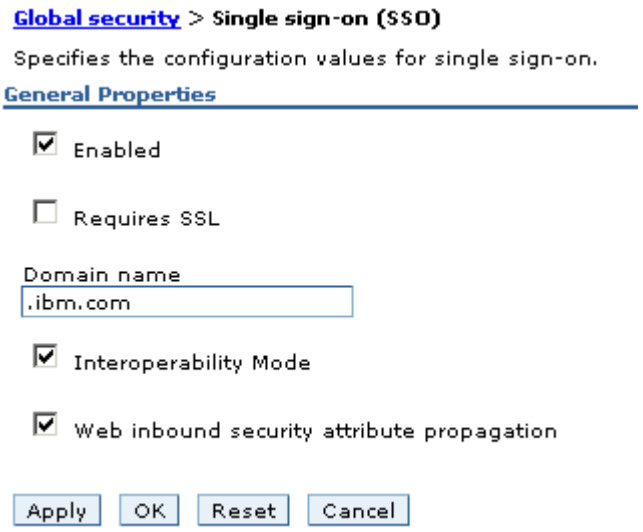


Figure 195. Updating the WebSphere Application Server SSO domain

2. Checking the applications by using the Tivoli Access Manager URLs:

- To check the IBM Connections applications, use the URL supplied for the Tivoli Access Manager reverse proxy server followed by the application name. See the following example:

Example

```
https://tamserver.mycompany.com/activities
https://tamserver.mycompany.com/communities
https://tamserver.mycompany.com/forums
https://tamserver.mycompany.com/profiles
https://tamserver.mycompany.com/blogs
https://tamserver.mycompany.com/dogear
https://tamserver.mycompany.com/files
https://tamserver.mycompany.com/wikis
https://tamserver.mycompany.com/homepage
https://tamserver.mycompany.com/search
https://tamserver.mycompany.com/news
```


Disabling Tivoli Access Manager

__ 1. To disable Tivoli Access Manager authentication you must reverse what was done previously. Open the `LotusConnections-config.xml` in a text editor and make the following changes. Update the interservice URLs for each of the applications to that of the Deployment Manager server host name, from the Tivoli Access Manager server host name.

For example, the entry for dogear becomes:

```
    <sloc:href>
        <sloc:hrefPathPrefix>/dogear</sloc:hrefPathPrefix>
        <sloc:static href="http://dmgr.mycompany.com" ssl_href="https://dmgr.mycompany.com"/>
        <sloc:interService href="https://dmgr.mycompany.com"/>
    </sloc:href>
</sloc:serviceReference>
```

Figure 196. Dogear

__ 2. Find the Tivoli Access Manager customAuthenticator property in the `LotusConnections-config.xml` configuration file, and remove the following section:

```
<customAuthenticator name="TAMAuthenticator">
  <attribute key="CookieTimeout" value="10" />
</customAuthenticator>
```

Figure 197. Tivoli Access Manager customAuthenticator property

__ 3. Now rename the `customAuthenticator` from `TAMAuthenticator` to `DefaultAuthenticator`.

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

Figure 198. Renaming the customAuthenticator

__ 4. When all of the above changes are made, save the `LotusConnections-config.xml` (and check it in if required).

__ 5. Now edit the `files-config.xml` and update it so that the `reauthenticateAndSaveSupported` property is set to true. This change looks like the following example:

```
<security reauthenticateAndSaveSupported="true">
<logout href="/files/ibm_security_logout" />
<inlineDownload enabled="false" />
</security>
```

__ 6. Now save the changes and resynchronize nodes and restart IBM Connections for these changes to take effect.

Figure 199. Restarting IBM Connections

On restart of nodes and applications the user is challenged for login with the IBM Connections login screen. Disablement of Tivoli Access Manager is now successfully completed.

3. Sametime integration

Installing Sametime 8.5.2 manually

This Sametime integration scenario requires the installation of the following Sametime products only which be done manually when files are downloaded:

- IBM DB2
- Sametime Systems Console
- IBM Lotus Domino Server
- Sametime Community Server
- Sametime Proxy Server
- Connection to LDAP Server

Information

For more information about how to manually set up a full IBM Sametime 8.5.2 environment, see: `http://www-10.lotus.com/ldd/stwiki.nsf/dx/Manually_setting_up_a_full_IBM_Sametime_8.5.2_environment_`.

Adding Sametime awareness through Sametime server

Follow the steps that are described in this URL to apply Sametime Awareness through IBM Connections:

`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`

4. Quickr Domino integration

The following integration points exist between Connections 4.0 and Quickr Domino 8.5.x:

- Single Sign On Between Products (SSO).
- Publishing File Attachments from Activities to Quickr Places.
- Association of Quickr Teamspaces and Wikis as part of an IBM Connections Community. This association is achieved with the IBM Connections Connector for Lotus Quickr.
- Enable the business card from the Quickr Domino server so that users can pull profile information directly from Connections while navigating on Quickr UI.

Information

It is optional how many of these integration points are enabled. In this configuration all of the above are enabled and explained in detail.

Enabling SSO between Lotus Connections and Quickr

SSO allows users to log in to Connections or Quickr one time and not be prompted for credentials again during their session on either product. SSO is achieved with a WebSphere LTPA token, which is shared with the Quickr server. To support SSO, there are a number of other conditions to be met, such as a shared LDAP, LDAP Realm, and SSO domain. System clocks must also be in synch between the servers in the configuration or else the SSO might not work correctly.

__ 1. On the administrative console, enable the LDAP realm with **Security > Global Security > Federated repositories** and input the realm in the Realm Name field. It is recommended for the realm name to follow the format `<LDAP_Hostname:<LDAP_Port`, in this case `ldap.example.com:389`. Click **OK** and save this change.

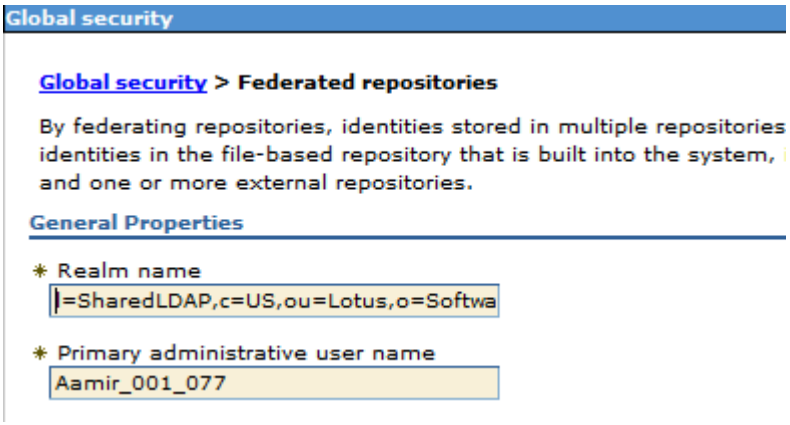


Figure 200. Federated repositories

__ 2. From the Security: Global Security panel, expand the Web and SIP Security option on the right side and click **Single sign-on (SSO)**.

Figure 201. Web and SIP security

__ 3. Select the **Enabled** and **Interoperability Mode** options and input the Domain name. Click **OK** and save this change.

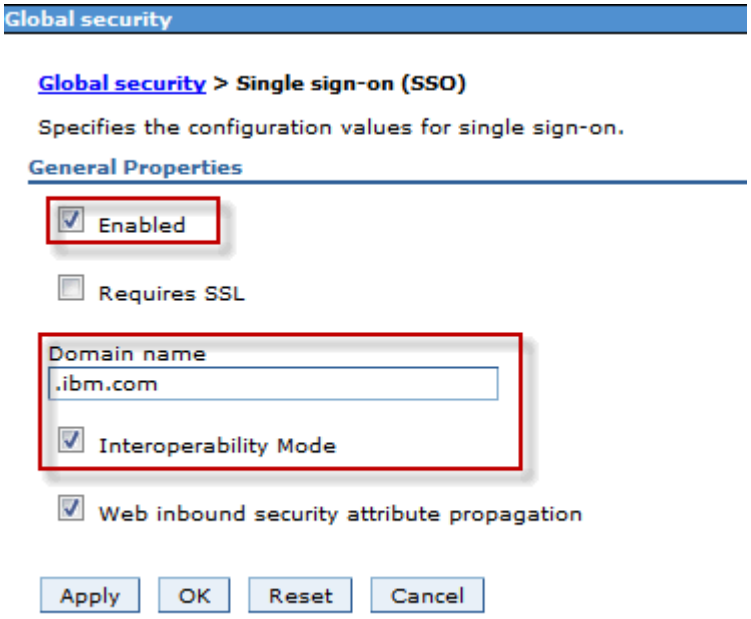


Figure 202. General Properties

__ 4. To export an LTPA token, at the Security: Global Security panel, click the **LTPA**.

Figure 203. Authentication

__ 5. Input a password of your choosing for the LTPA keys to be exported and specify a location to export this key. Click **OK** to export the keys.

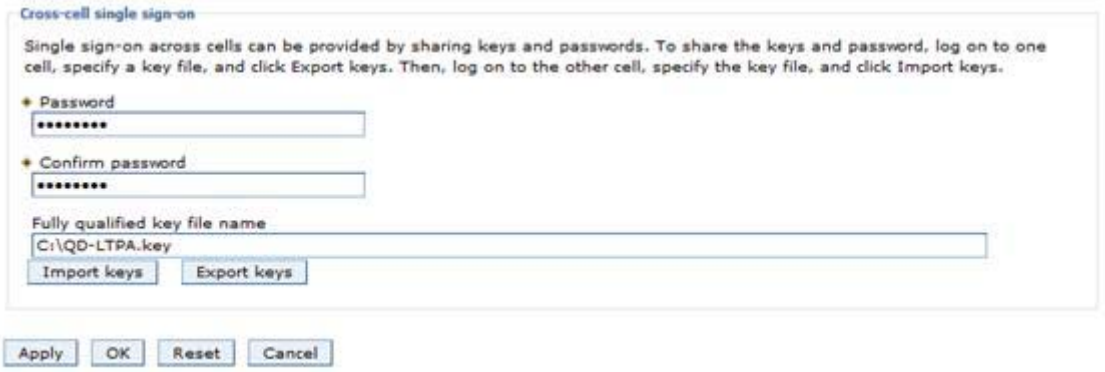


Figure 204. Cross-cell single sign-on

__ 6. When this key is exported, copy it to your Quickr Domino computer and import it to the Quickr Domino configuration with the Domino Administrator console. It is also important to set the correct realm on the Domino configuration.

Information

See the Lotus Quickr Wiki for more information about how to do this on the Domino part of the configuration.

__ 7. The previous steps prepare the Lotus Connections part of the configuration. After the steps to import the LTPA server to the Domino configuration are complete, synchronize the nodes in the configuration and restart Lotus Connections and Lotus Quickr. When the configuration comes back online, SSO is enabled. To verify, open a clean browser and log in to Lotus Connections. After you log in, type the URL of the Domino Quickr server into the address bar. When the page loads, you should still be logged in to Lotus Quickr without being prompted for credentials. Repeat this test from the opposite perspective, starting with Lotus Quickr to verify that SSO is working in both directions. When SSO is working, proceed to the next steps.

Enabling the Connections business card in Quickr Domino

__ 1. Enable the business card on the Quickr Domino server by making the following change to the `qpconfig.xml`, in the following sample location `C:\IBM\Lotus\Domino\data`.

__ 2. Open this file with a text editor and search for a section in this file named `profile_server`. After the sample information, add the following lines to the file:

```
 <profile_server>
<server_name>
   dmgr.ibm.com
</server_name>
<semantic_tag_service_location>
   /profiles/ibm_semanticTagServlet/javascript/semanticTagService.js
</semantic_tag_service_location>
<javelin_tag_location>
   /profiles/html/personTag?template=personTag.jsp
</javelin_tag_location>
</profile_server>
```

Figure 205. profile_server

__ 3. Save the file and restart your Lotus Quickr Domino server for this change to take effect. When restarted, you can now hover over the user name in Quickr Domino and the option to show the business card appears in a similar fashion to that of Connections.

Enabling integration between Connections Activities and Quickr

To enable the publishing of files to Quickr from Activities, the Quickr server must be added to the white list provider for activities and then some changes are required on the `oa-config.xml`.

__ 1. To begin, open the administrative console.

__ 2. Go to **Resources > Resource Environment > Resource Environment Providers** and click **QuickrWhitelistProvider**.

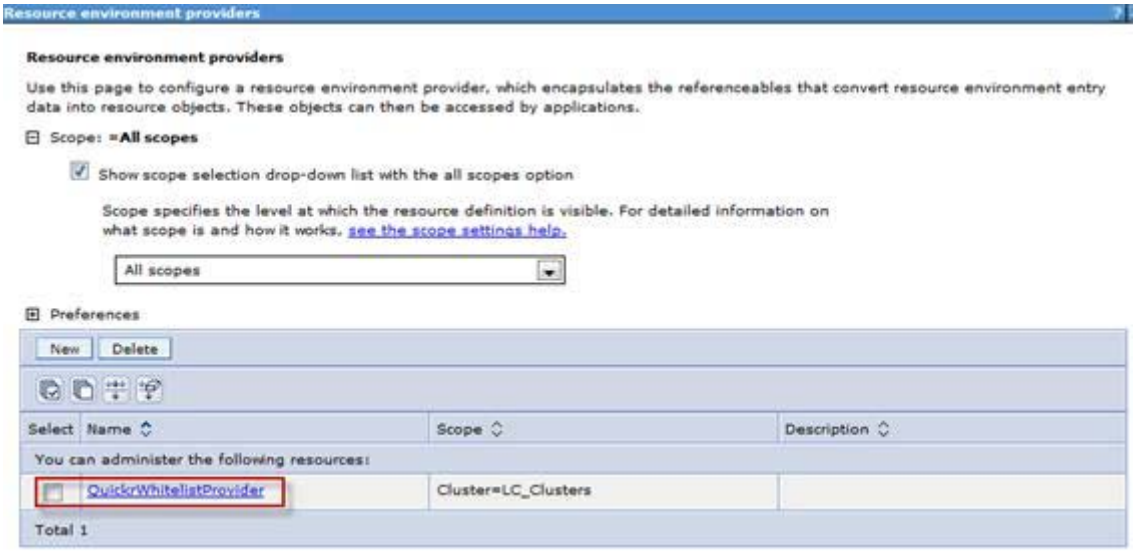


Figure 206. Resource environment providers

__ 3. Click **Custom Properties**.

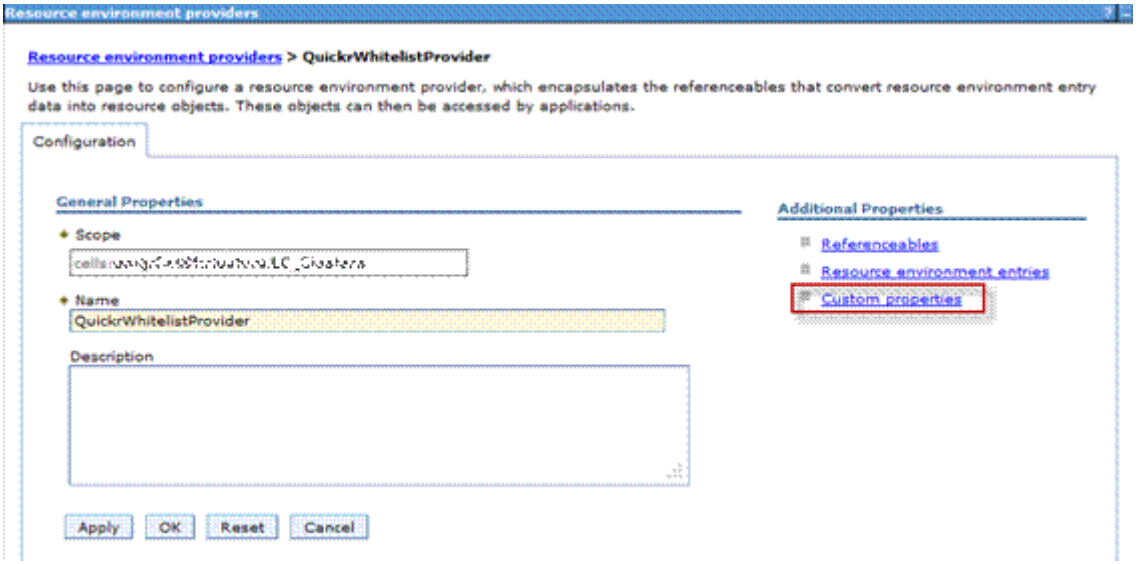


Figure 207. Additional properties

__ 4. Click **New**.

Figure 208. Clicking New

__ 5. Name this new property. Start the name with the word `allow`, in this case `allowQuickr`. The value that is provided should be the host name or IP address of the Quickr server. In this case, the host name of the Quickr server is used (`quickrserver.ibm.com`).

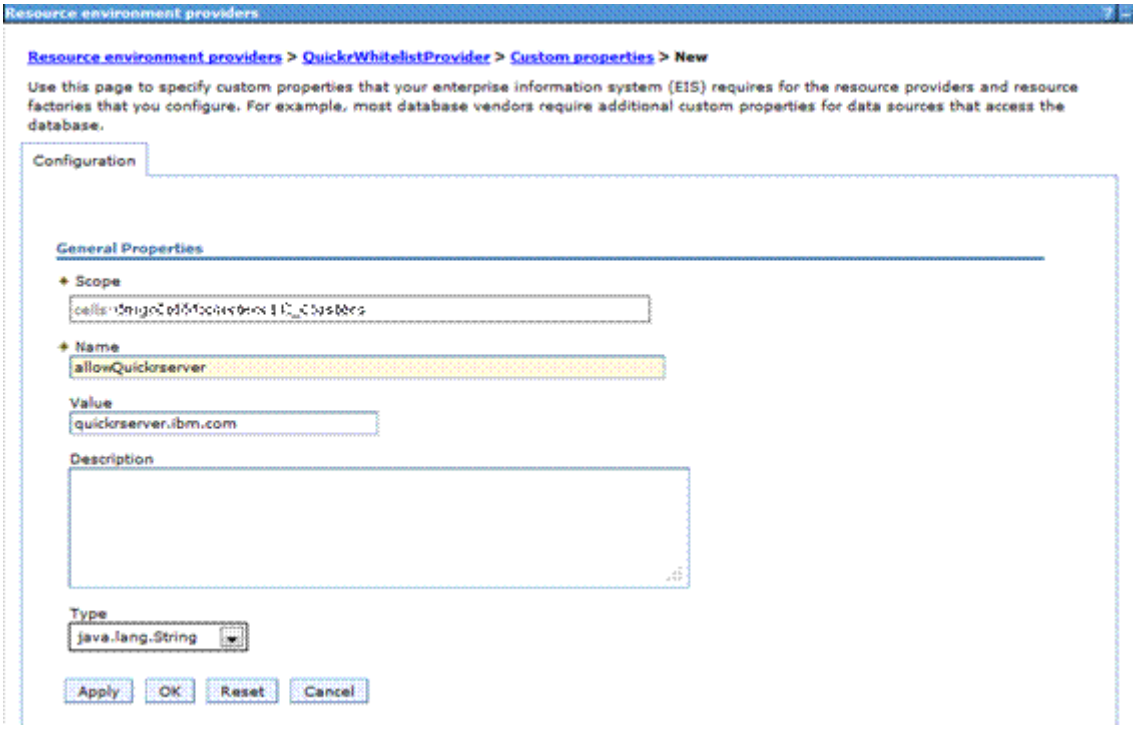


Figure 209. Naming the new property

__ 6. Click **OK** and save this change.

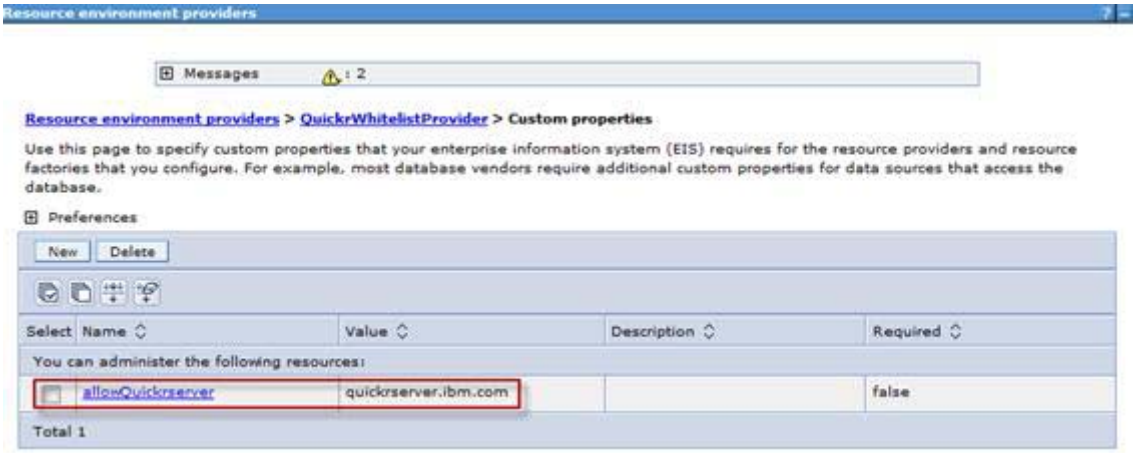


Figure 210. allowQuickrserver

__ 7. Check out the `oa-config.xml` by using the wsadmin client or a text editor. Find the block of code named `PublishFile`. Set the enabled flag to `true`, `requireSSO` to `true` and `allowCustomServers` to `false`.

```
<PublishFile enabled="true" allowCustomServers="false" requireSSO="true">
  <server>http://dmgr.ibm.com</server>
  <server>http://localhost:8080</server>
</PublishFile>
```

Figure 211. oa-config.xml

__ 8. Resynchronize the nodes and restart the Activities component. Now the ability to publish attachments from Activity entries to Lotus Quickr is enabled with **Publish to Lotus Quickr**.

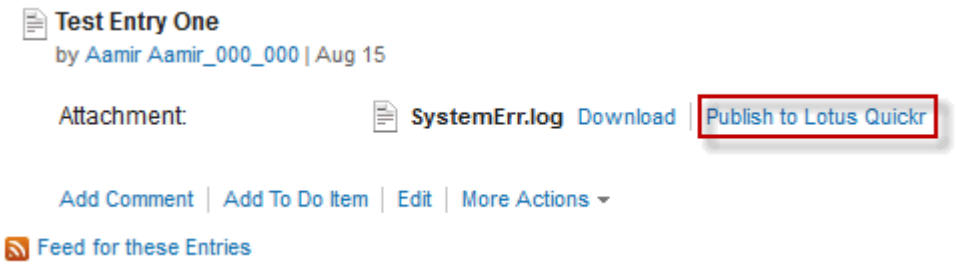


Figure 212. Test Entry One

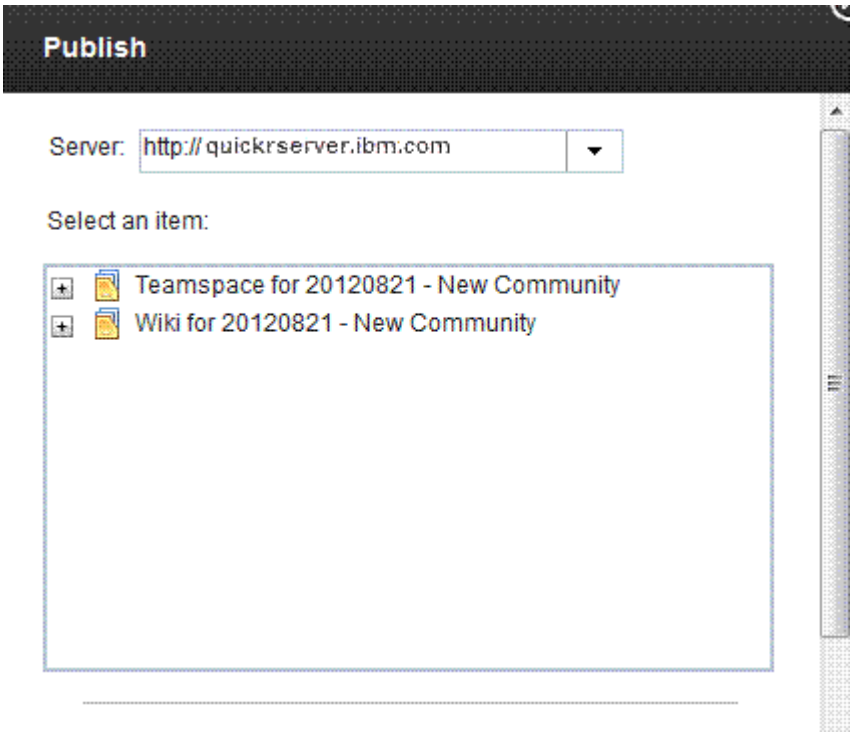


Figure 213. Published to Lotus Quickr

Enabling Connections Communities integration with Quickr

To enable integration between Communities and Quickr, the Connector must be installed. On the Deployment Manager computer, do the following steps:

__ 1. From the Lotus Connections Connectors for Quickr installation files, find the folder named `LC_Connectors_Quickr_Install`. From here, locate the IM folder and from within this folder select the folder appropriate for your operating system (Windows, Linux for System z, or Linux). From this folder, launch `install.exe`. Click **Install** to continue.

Figure 214. IBM Installation Manager: Install

__ 2. Select the packages which are required to be installed. Click **Next**.

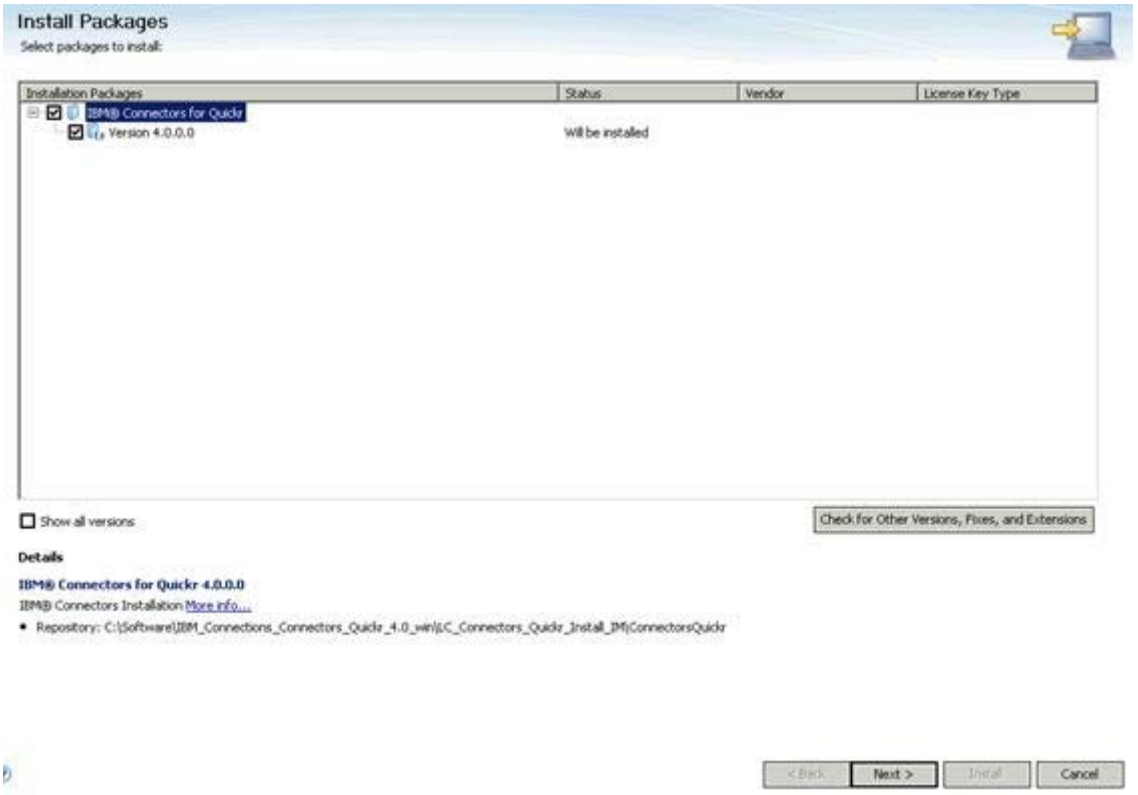


Figure 215. Selecting packages to install

__ 3. Accept the license agreement and click **Next** to continue.

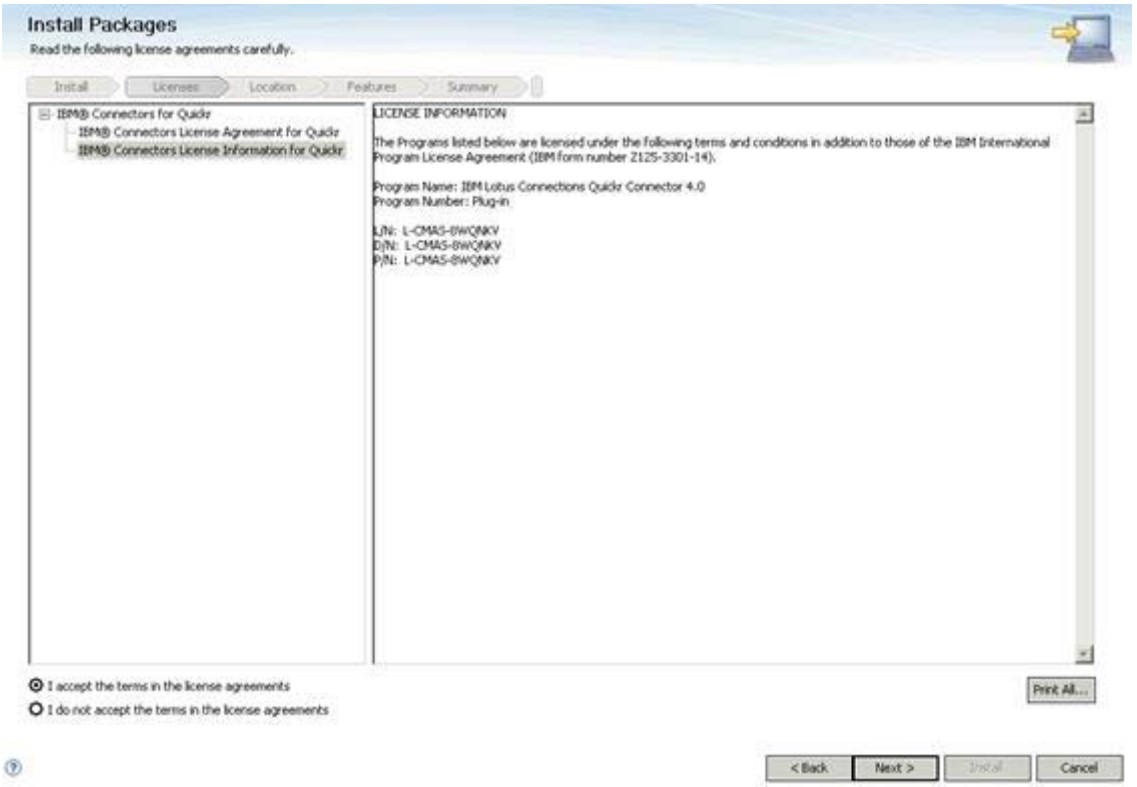


Figure 216. License agreement

__ 4. Browse to or type the installation directory path and click **Next** to continue.

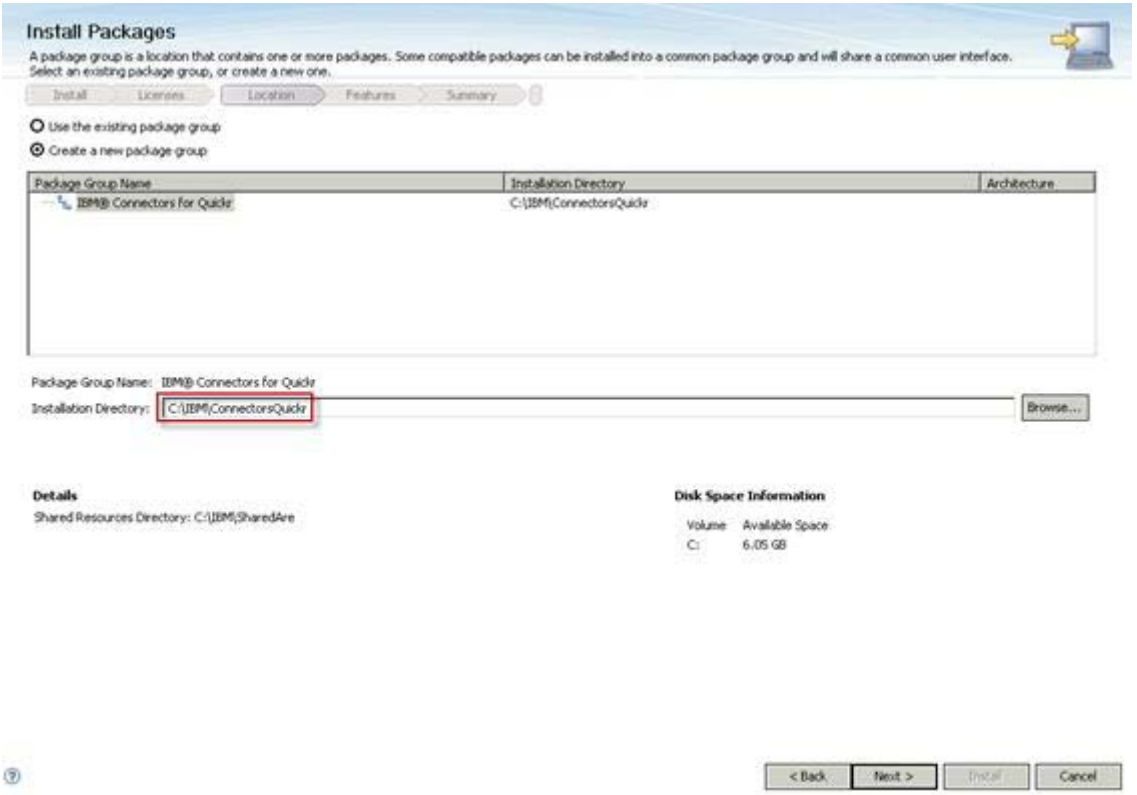


Figure 217. Installation directory

__ 5. Select the installation package and click **Next** to continue.

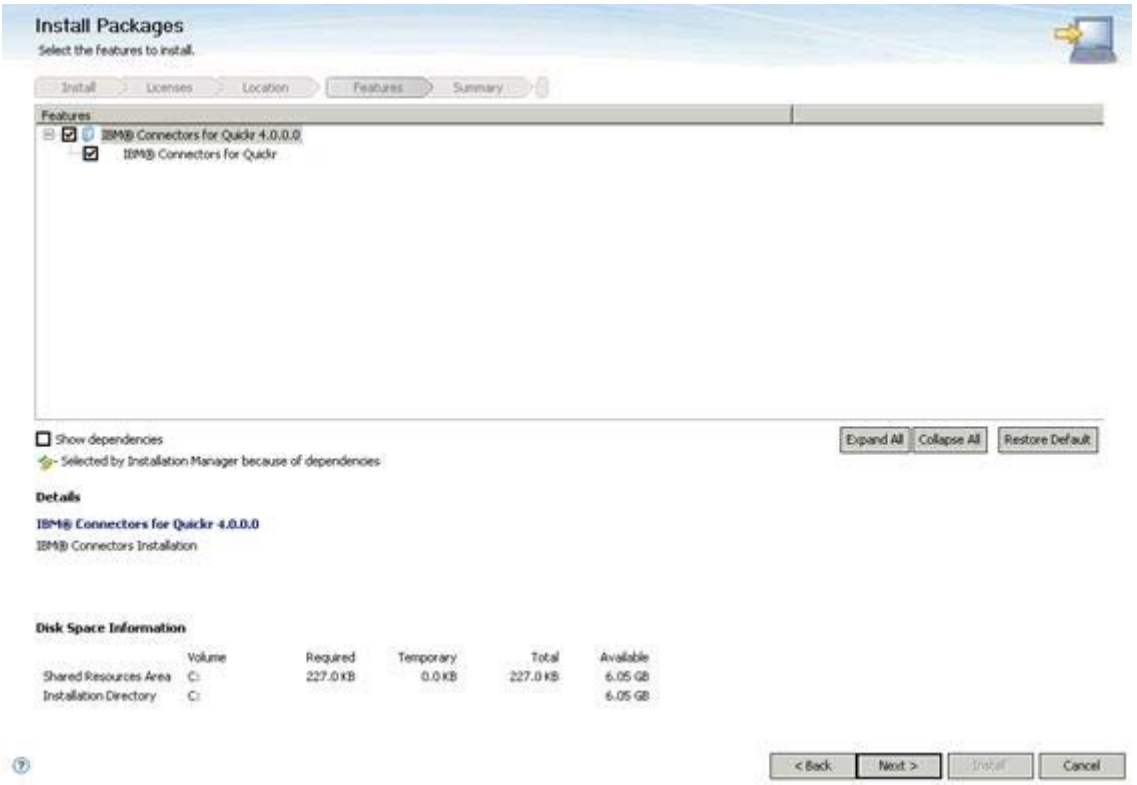


Figure 218. Selecting the features to install

__ 6. Select **Quickr type Quickr Domino** and then select **Quickr Domino Wiki** and **Quickr Domino Teamspace**. Then, click **Next** to continue.

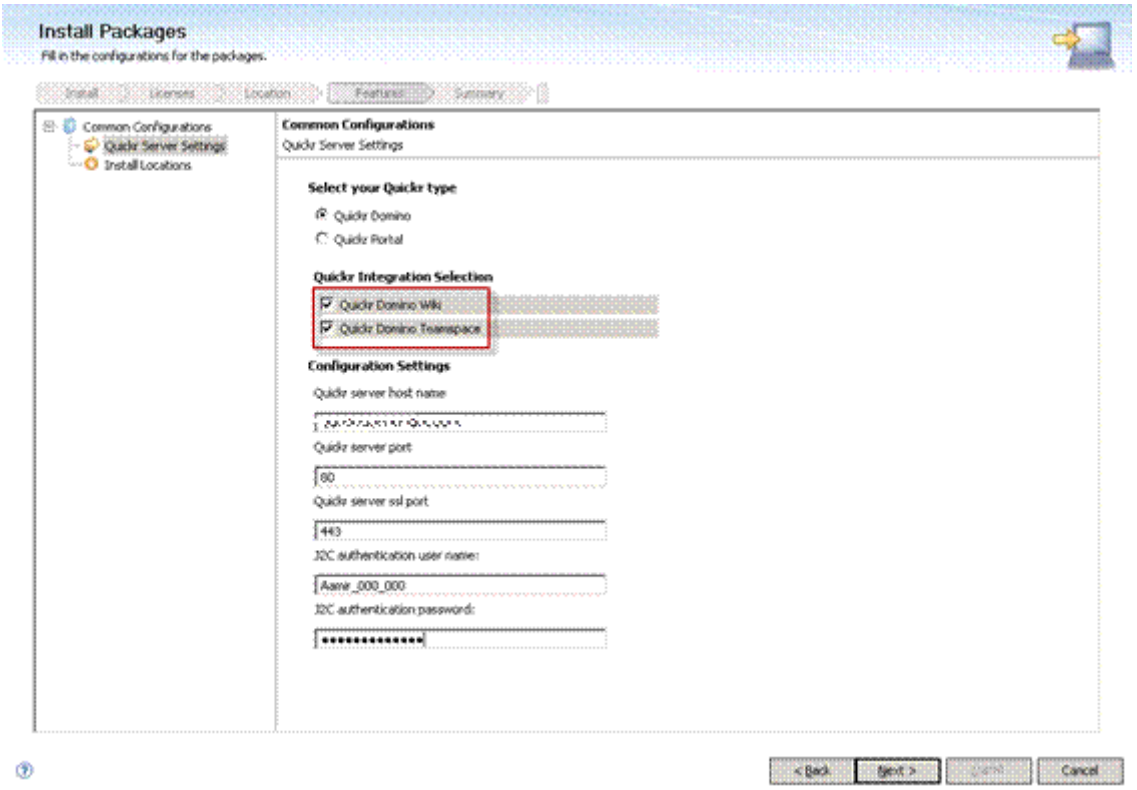


Figure 219. Configuration for the packages

__ 7. Enter the installation locations of the Quickr Connectors and click **Validate**. If the validation is successful, click **Next** to continue.

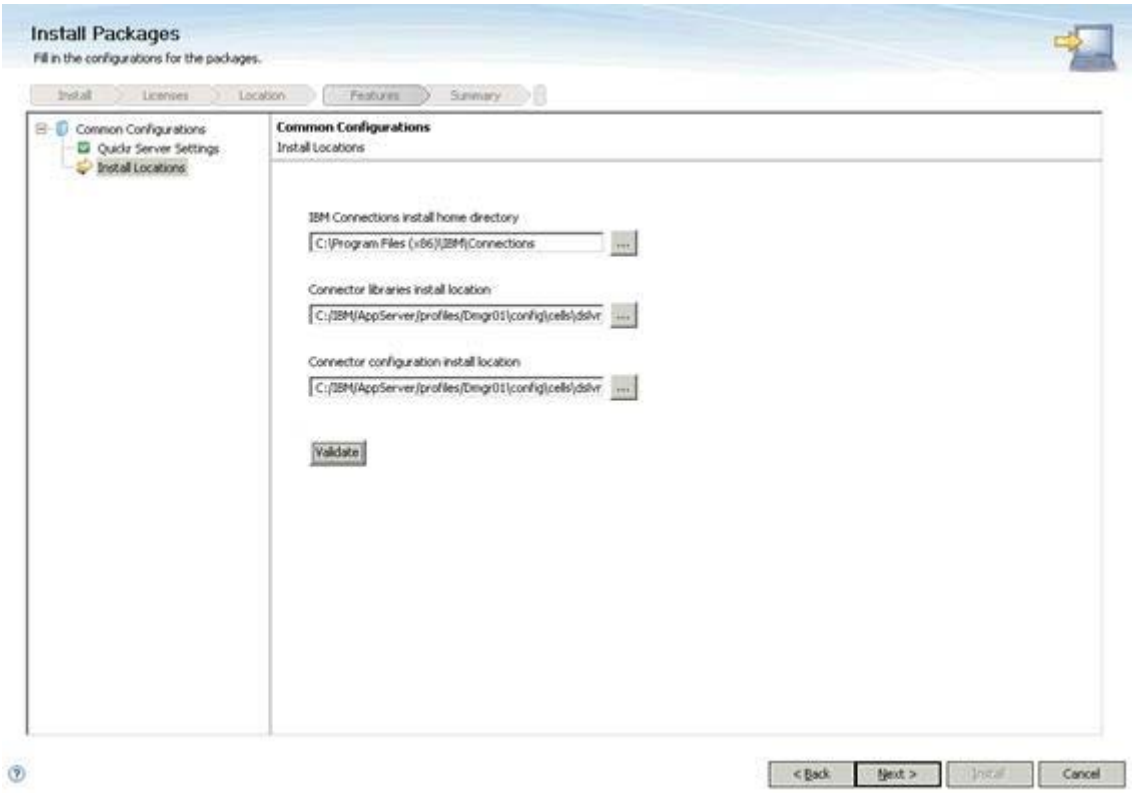


Figure 220. Install locations: Validation

__ 8. Now click **Install** to start the installation of Quickr Connectors.

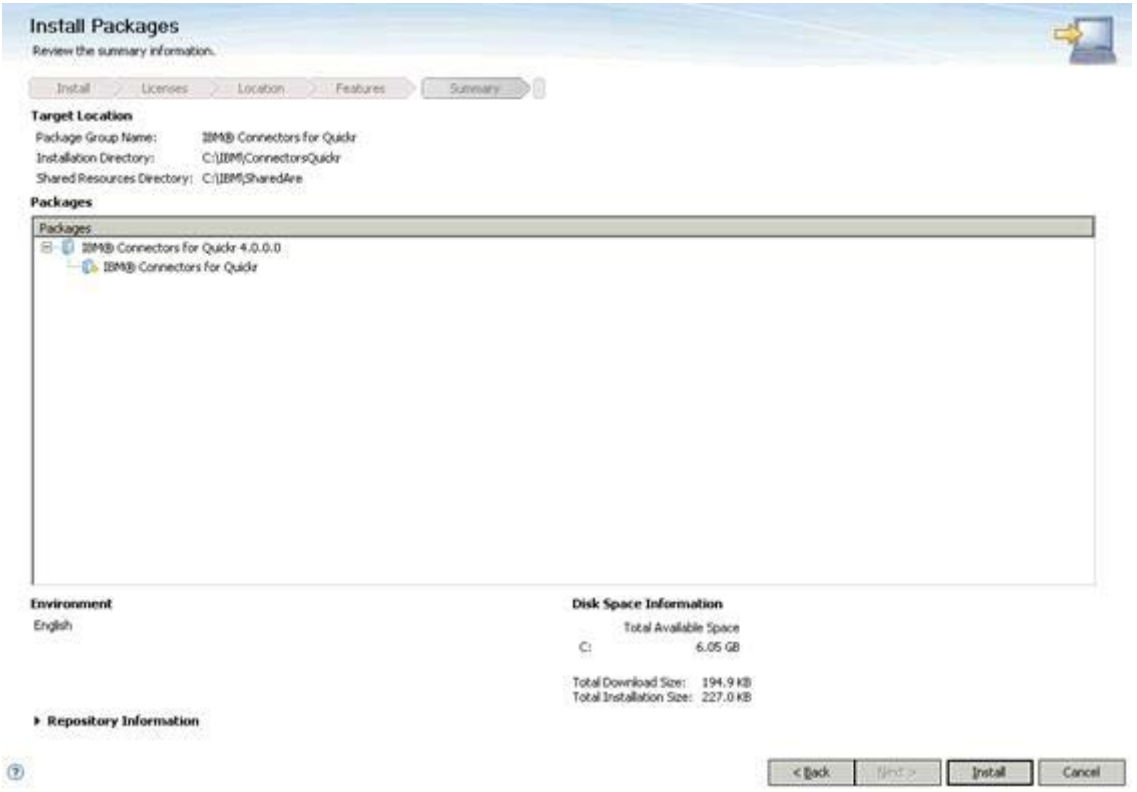


Figure 221. Summary information: Start installation

The installation of Quickr Connectors is now in progress, and takes several minutes to complete.

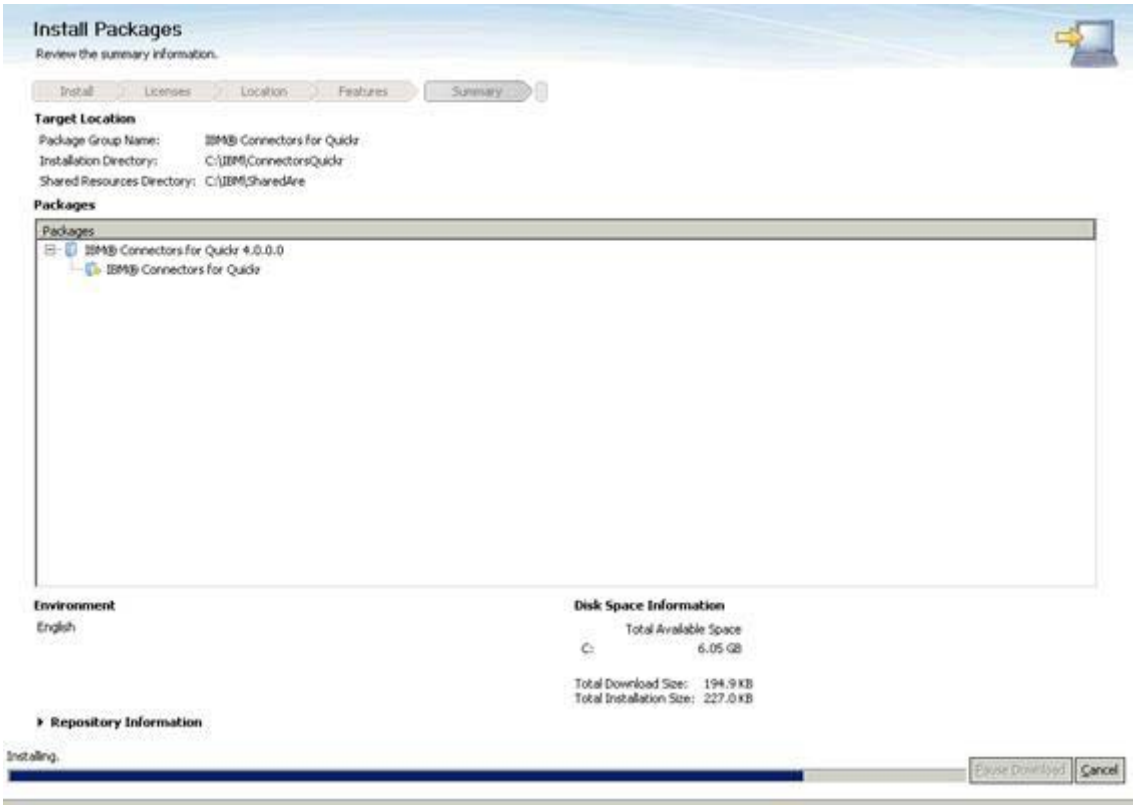


Figure 222. Installation in progress

__ 9. When the installation is successfully completed, click **Finish**.

Figure 223. Installation completion

__ 10. Restart IBM Connections and resynchronize the nodes for all changes to take effect.

__ 11. Now you can log in to IBM Connections as an authenticated user, create a Community and you should now see the Quickr applications in the Associated Applications section of the Community.

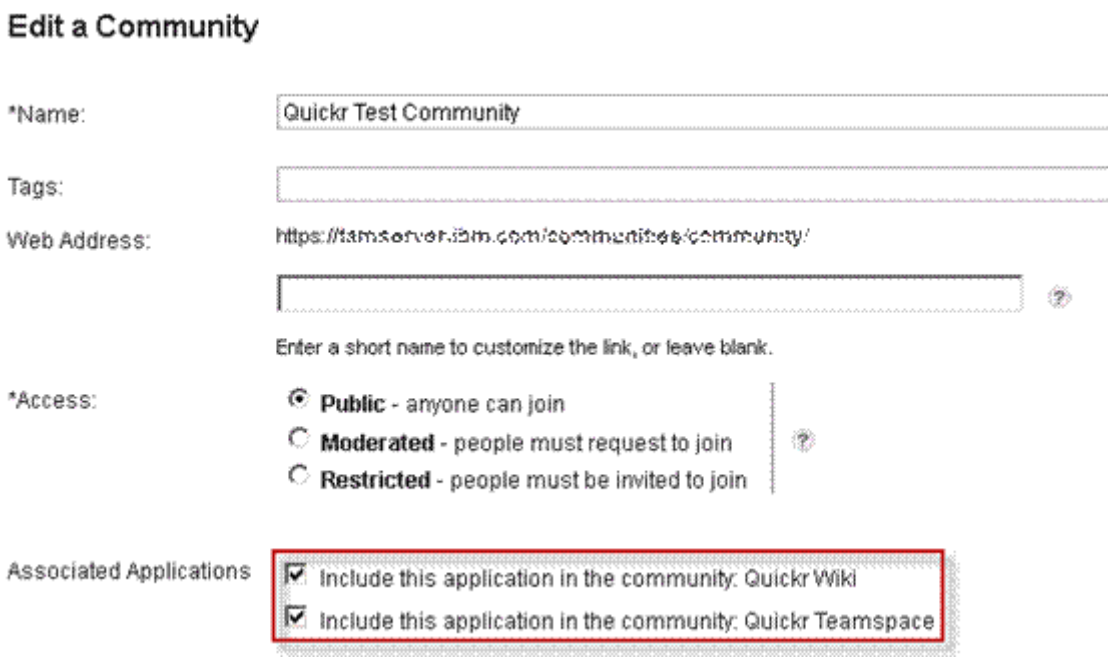


Figure 224. Editing a community

5. SharePoint 2010 Server installation

__ 1. Run the SharePoint 2010 Server .exe file from where it was downloaded. Click **Install software prerequisites**. All the software prerequisites for SharePoint are installed. On completion, click **Install SharePoint Server**

Figure 225. SharePoint Server 2010

__ 2. Enter the product key that is provided and click **Continue**.

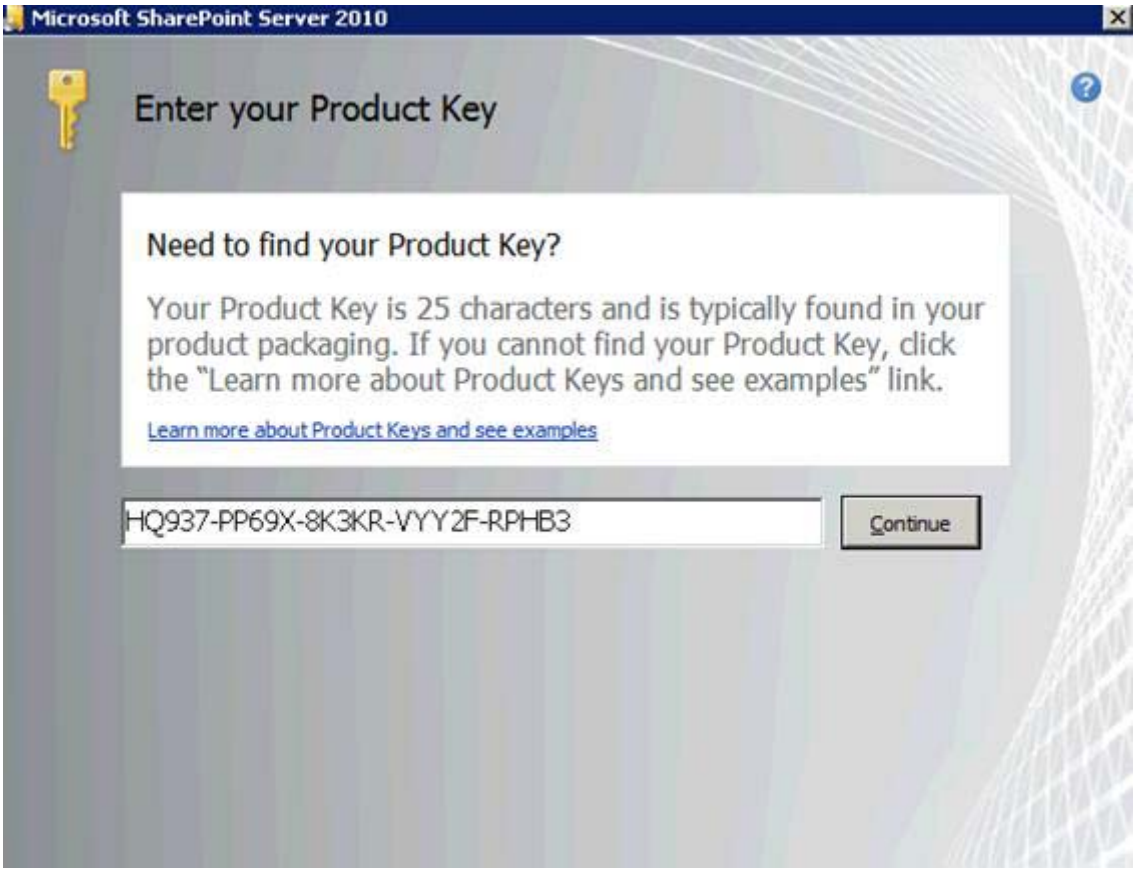


Figure 226. Enter your Product Key

__ 3. Select the box to accept the terms of agreement. Then, click **Continue**.

Figure 227. Read the Microsoft Software License Terms

__ 4. Click **Standalone** to continue.

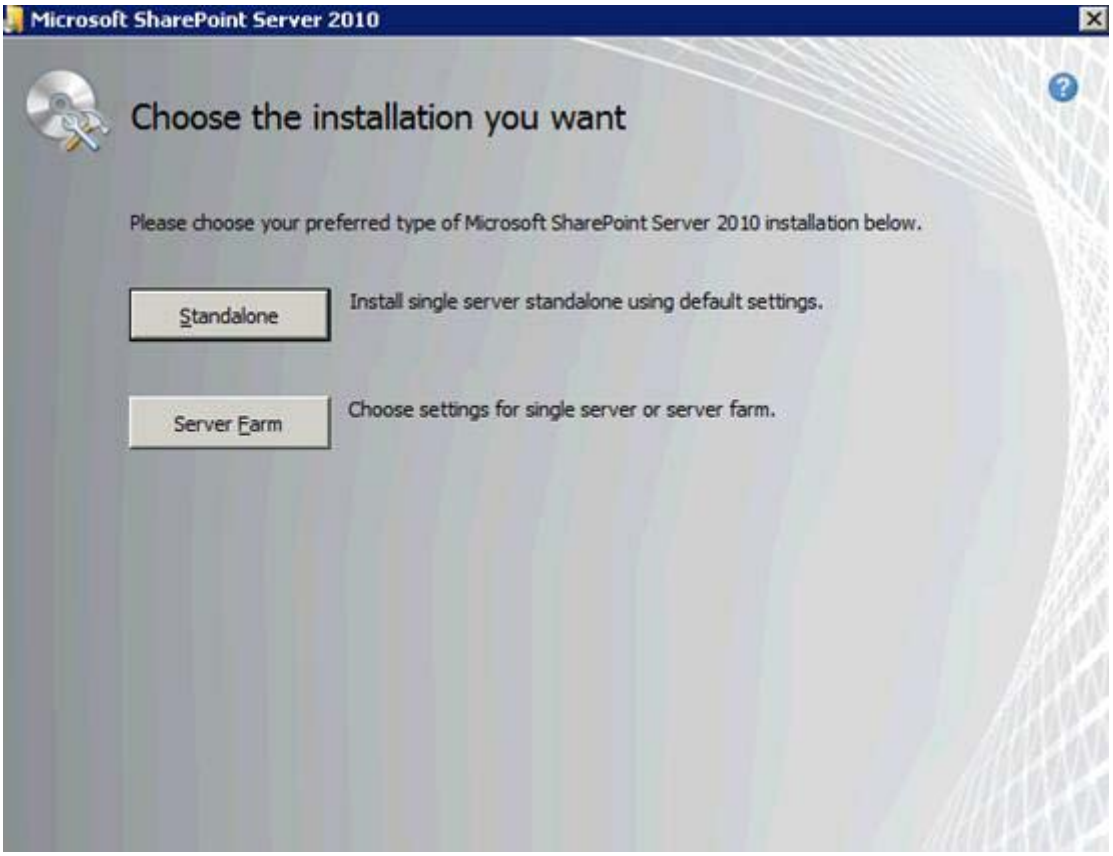


Figure 228. Choose the installation that you want

The installation of the SharePoint Server 2010 begins, and might take several minutes to complete.

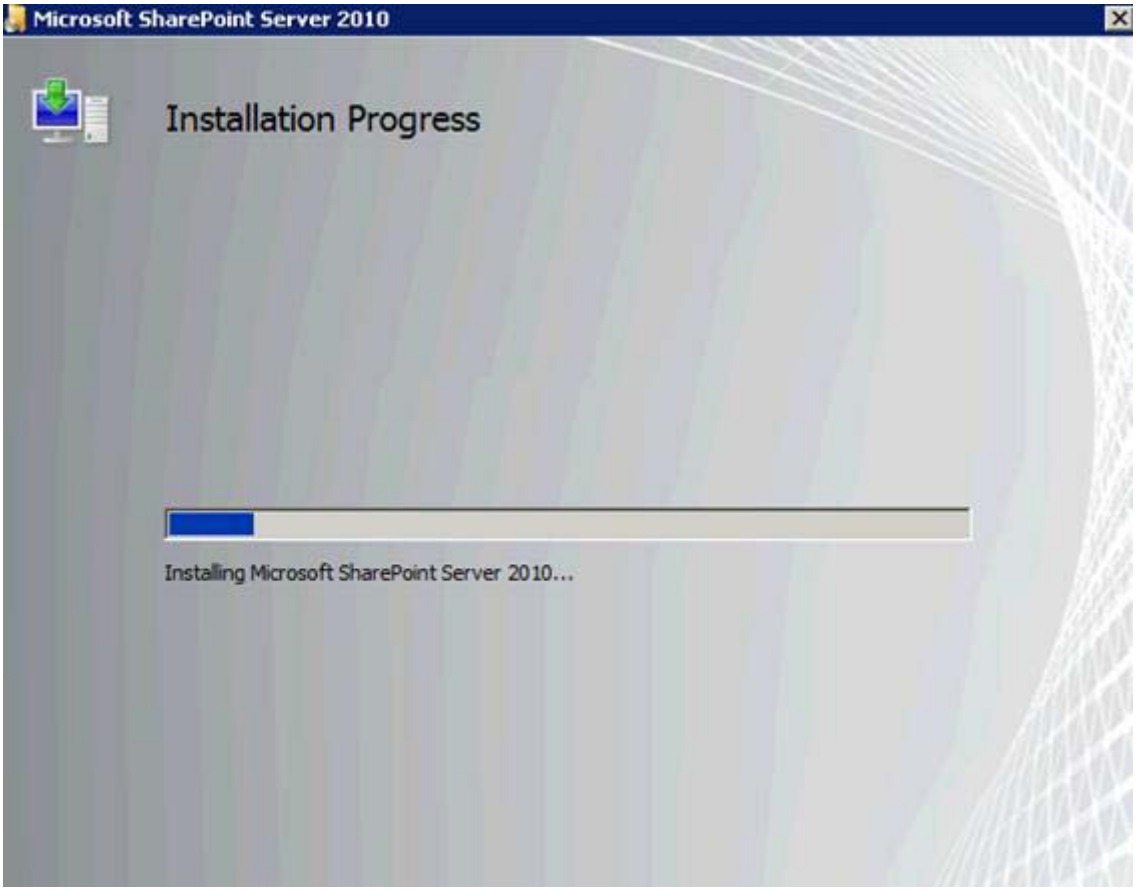


Figure 229. Installation progress

__ 5. Click **Next** to start the configuration of SharePoint Server.

Figure 230. SharePoint Products Configuration Wizard: Welcome

__ 6. Click **Yes** to start the SharePoint services and continue.

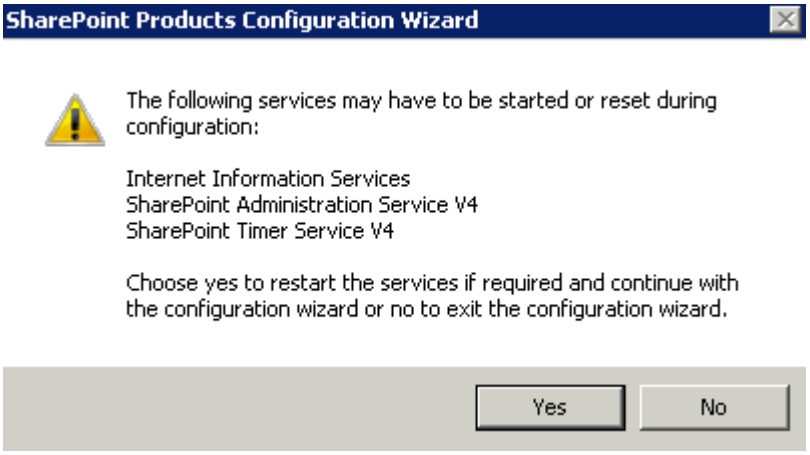


Figure 231. SharePoint Products Configuration Wizard: Warning message

The SharePoint configuration tool begins. It might take several minutes to complete. When completed, a web browser opens on the SharePoint home page.

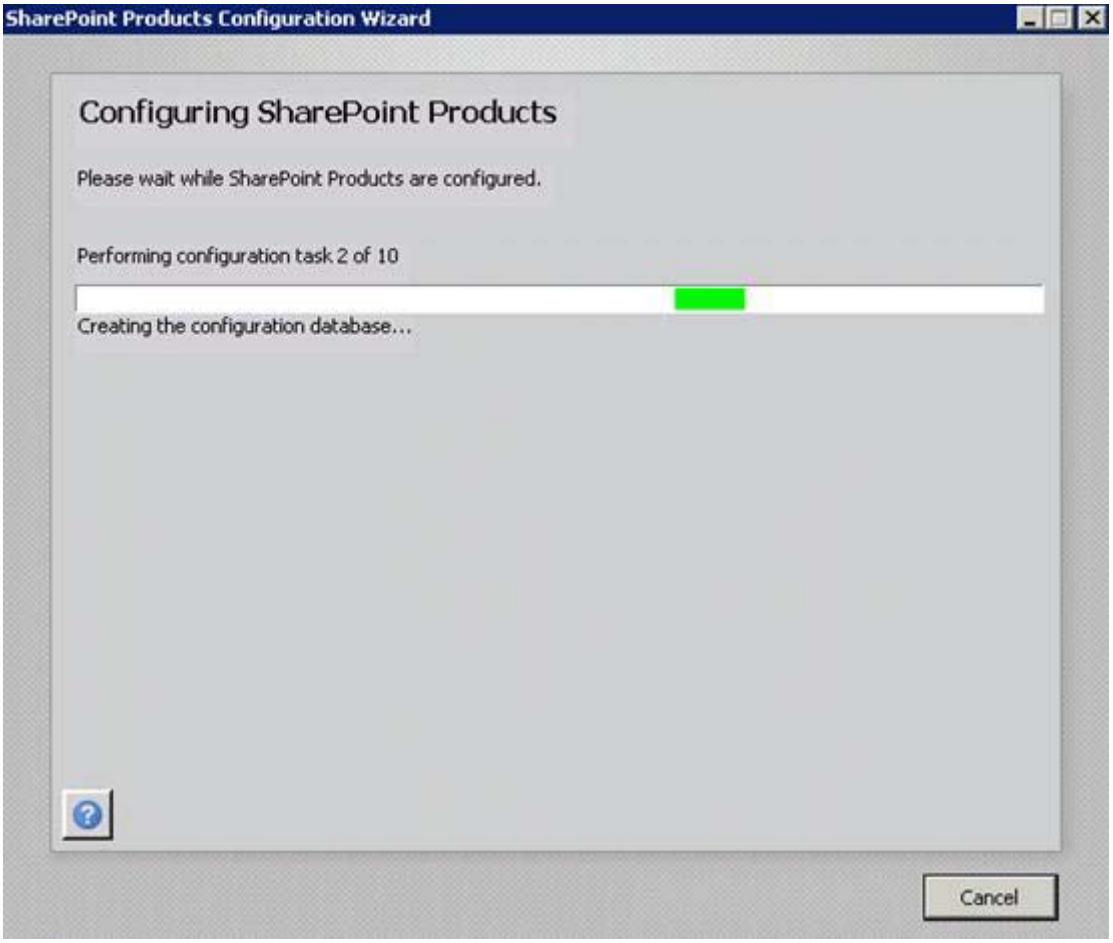


Figure 232. SharePoint Products Configuration Wizard: Configuration SharePoint Products

__ 7. Click **Site Actions > New Site** to create a site.

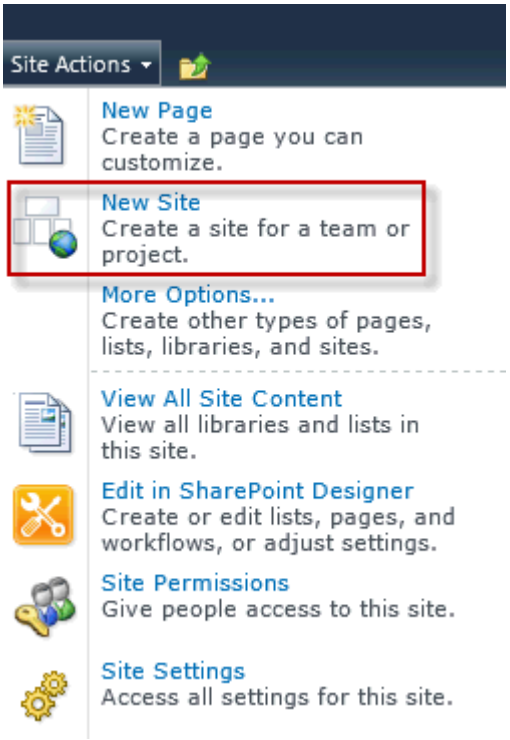


Figure 233. Site Actions: New Site

__ 8. Ensure that the Team Site is selected, and then click **OK** to continue.

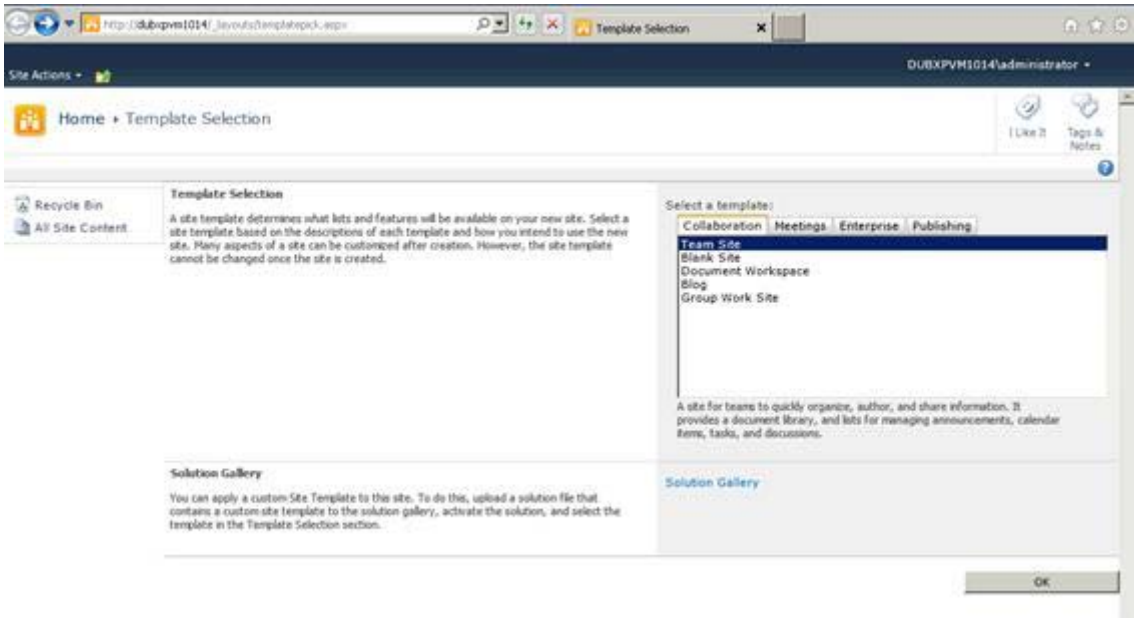


Figure 234. Home: Template Selection

__ 9. Enter a title for the site name and a description. Select **Team Site** as a template and click **Create** to continue creating the site.

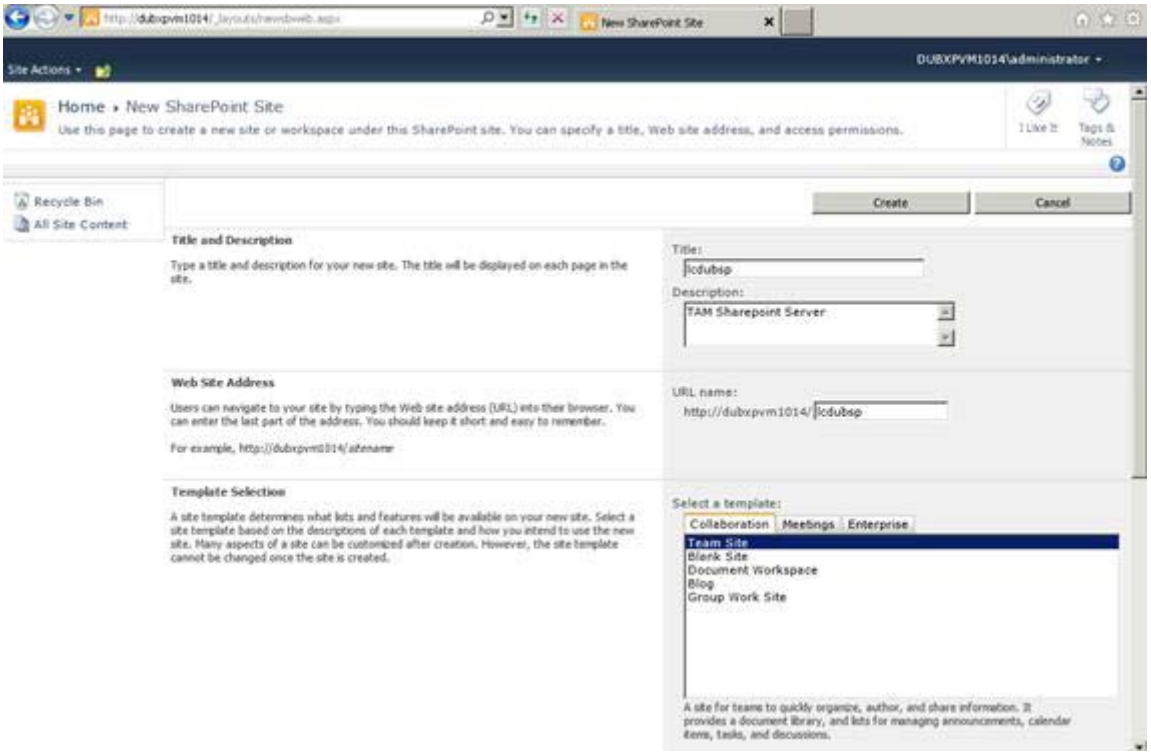


Figure 235. Home: New SharePoint Site

6. Install and deploy IBM Connections plug-in for SharePoint

Information

Before installing the IBM Connections plug-in, the SharePoint Language Pack must be installed.

Installing SharePoint Language Pack

__ 1. Browse Windows Explorer to where the ServerLanguagePack installation file was downloaded.

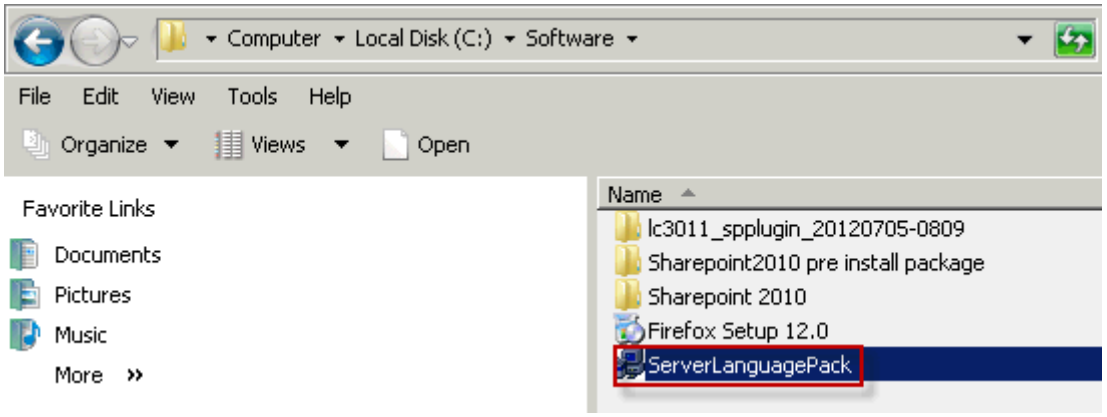


Figure 236. ServerLanguagePack

__ 2. Click **Run** to start the installation program.

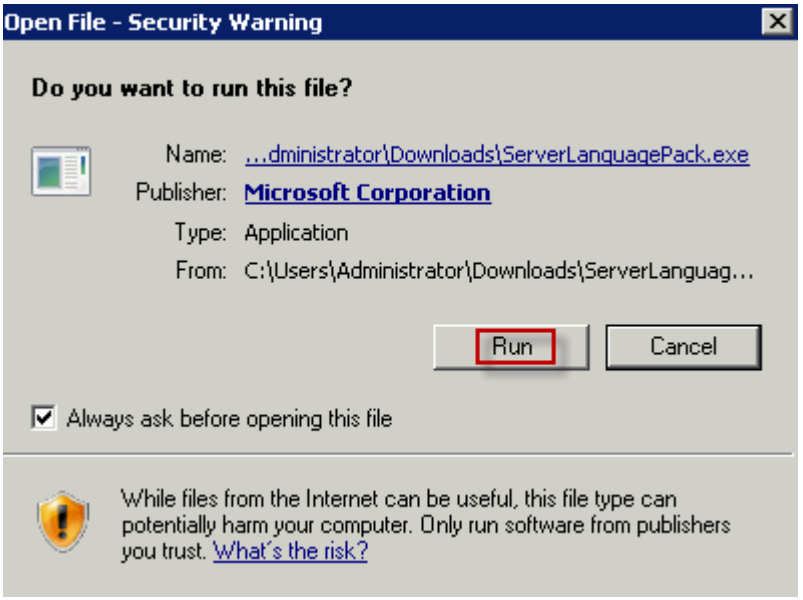


Figure 237. Open File: Security Warning

__ 3. Accept terms of agreement and click **Continue**.

Figure 238. Read the Microsoft Software License Terms

The installation of the Language pack is now in progress.

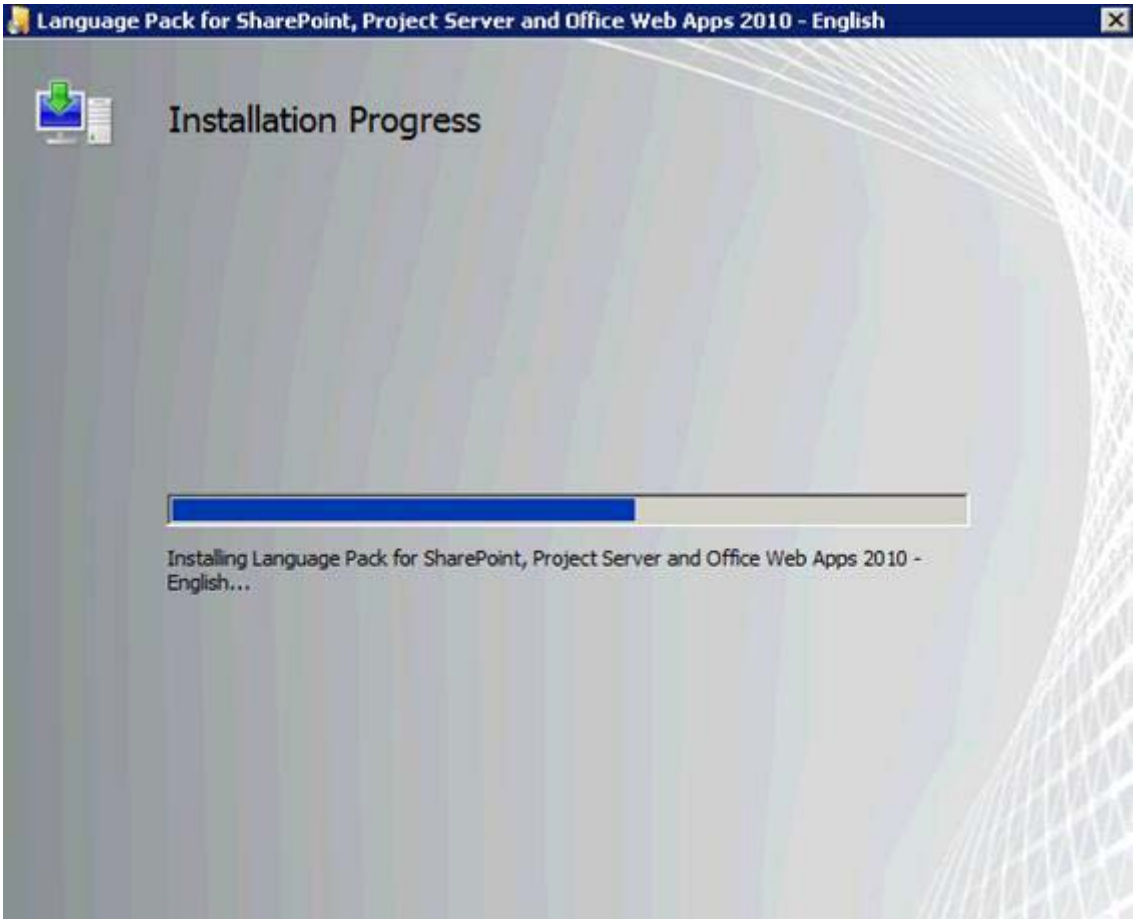


Figure 239. Installation progress

__ 4. Ensure that the Run the SharePoint Products Configuration Wizard now box is checked and click **Close** to continue.

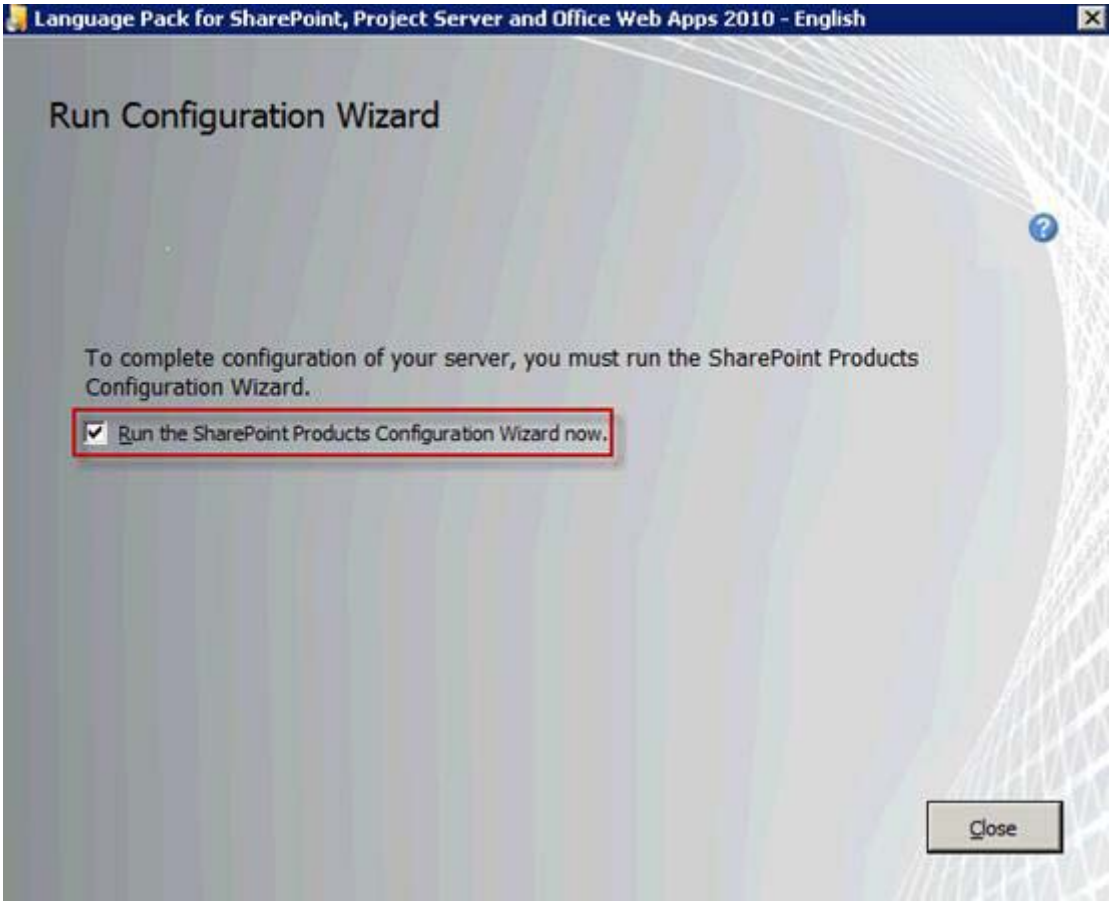


Figure 240. Run Configuration Wizard

__ 5. Click **Next** to continue the configuration process.

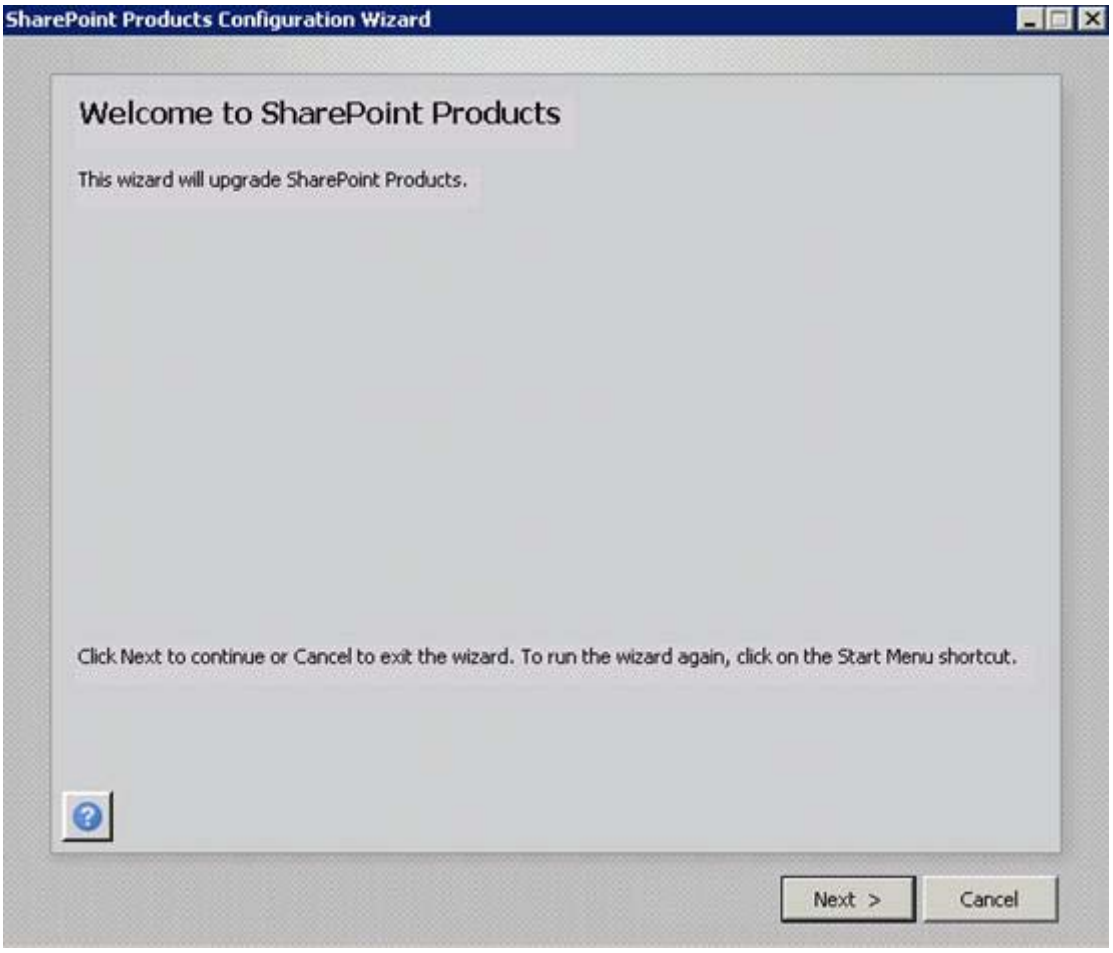


Figure 241. SharePoint Products Configuration Wizard: Welcome

__ 6. Click **Yes** to start the services and continue.

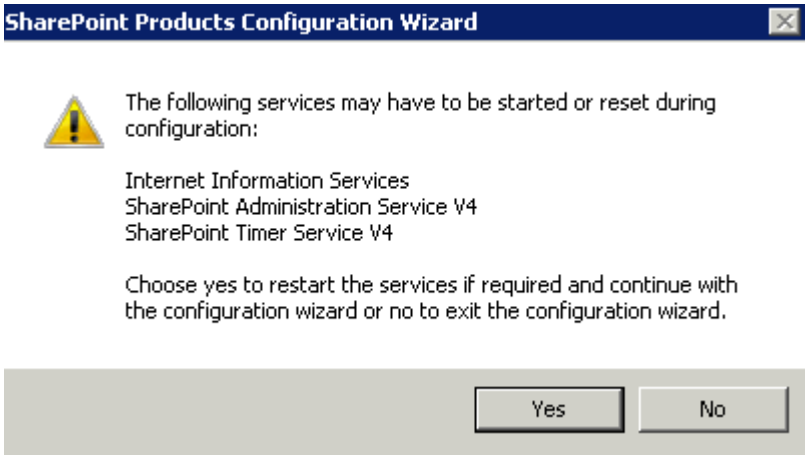


Figure 242. SharePoint Products Configuration Wizard: Warning message

The configuration of the Language Pack is now in progress.

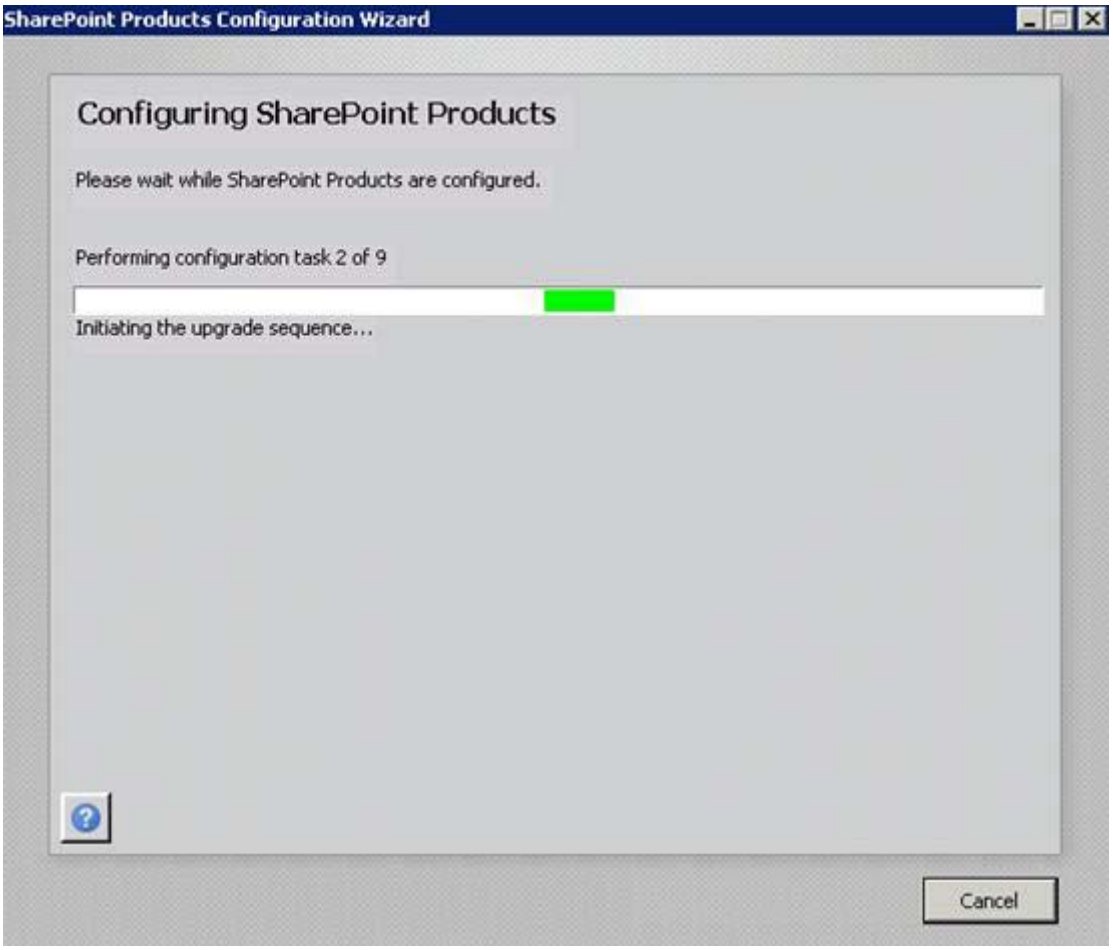


Figure 243. LanguagePack installation in progress

__ 7. Click **Finish** to complete the configuration.

Figure 244. Configuration Successful

Installing IBM Connections plug-in for SharePoint

Note

If you do not have a Lotus Greenhouse account, you must create one before you are able to download any of the IBM software.

__ 1. Ensure that the correct plug-in is installed for your SharePoint deployment as it might be a Server Farm or Standalone. Browse Windows Explorer to where the plug-in installation files were downloaded. Click `Install.bat` to start the installation program.

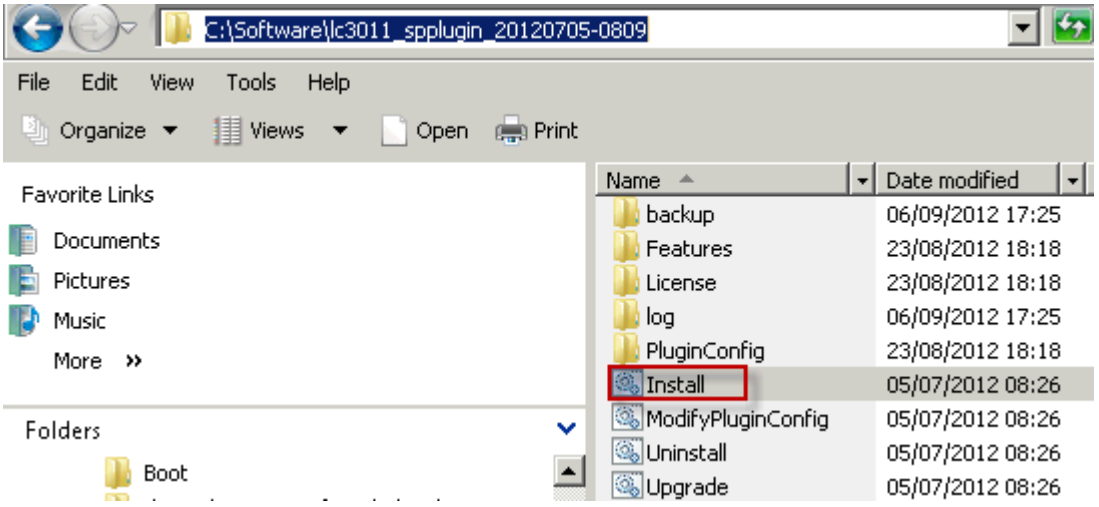


Figure 245. Installing IBM Connections plug-in for SharePoint

__ 2. Click **Run** to start the IBM Connections plug-in configuration.

Figure 246. Open File: Security Warning

__ 3. Enter the Profiles and Federated Search URLs in the fields provided. Then, click **OK** to complete the IBM Connections plug-in installation. When completed, the configuration dialog box closes automatically.

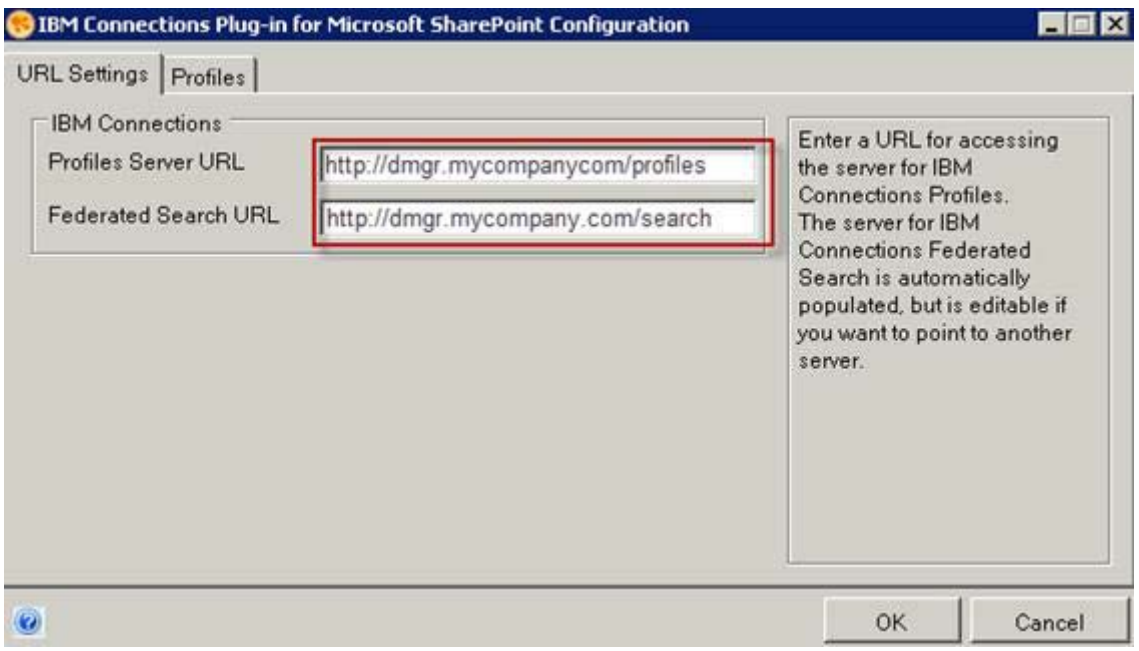


Figure 247. IBM Connections plug-in for SharePoint: Profiles Server URL

Deploying IBM Connections plug-in for SharePoint

If the installation of the IBM Connections plug-in for SharePoint is successful, the IBM Connections Tag Cloud, Search IBM Connections Profiles, and Business Card features are installed when their solutions are deployed. They must be activated before the Web Parts display within the Web Parts Gallery when user is logged on to a site.

To deploy the Web Parts display, do the following steps:

__ 1. Enter the site URL in browser (`http://myserver.mycompany.com:7812`) and select **Forms Based Authentication**. The port number might not be the same on your deployment. Select **Forms Authentication**.

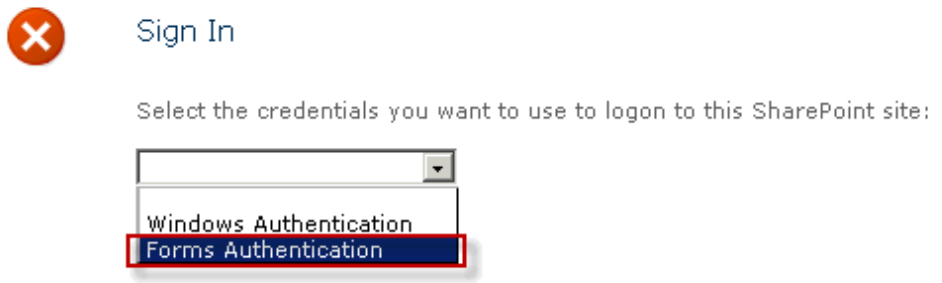


Figure 248. Forms Authentication

__ 2. Log in to site as authenticated user.

Figure 249. Sign in to the site

__ 3. Click the down arrow for **Site Actions** and select **Site Settings** to continue.

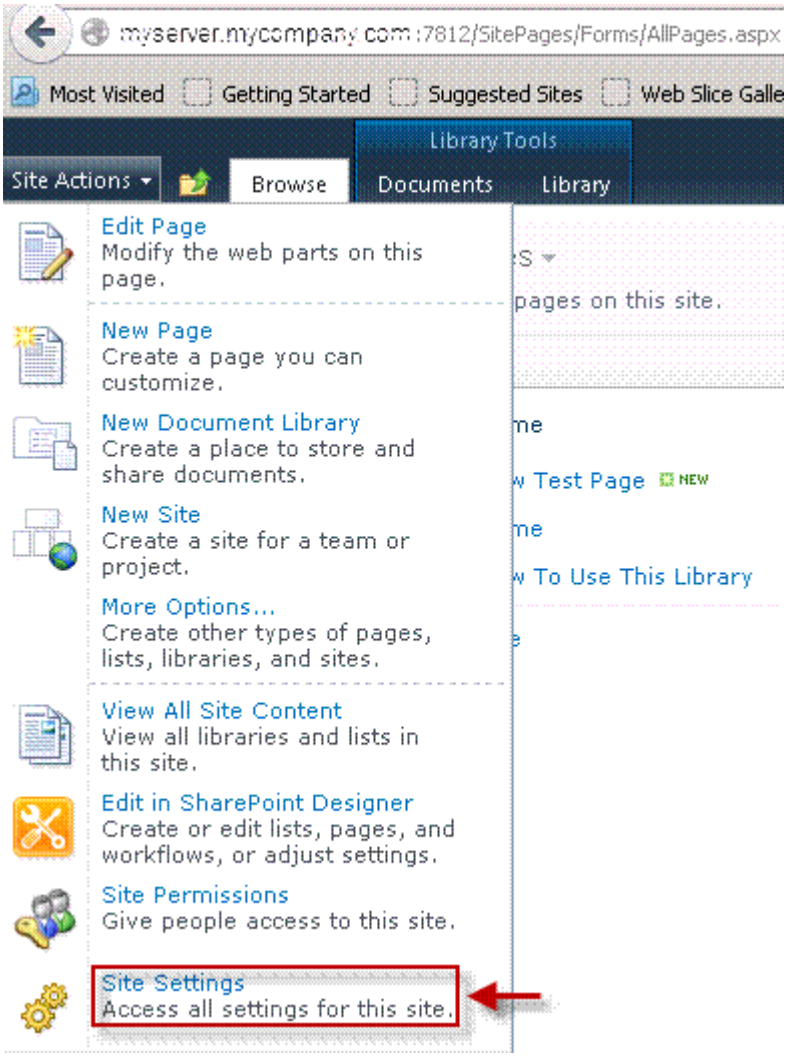


Figure 250. Site Settings

__ 4. In the Site Collection Administration section click **Site Collection Features** to continue.

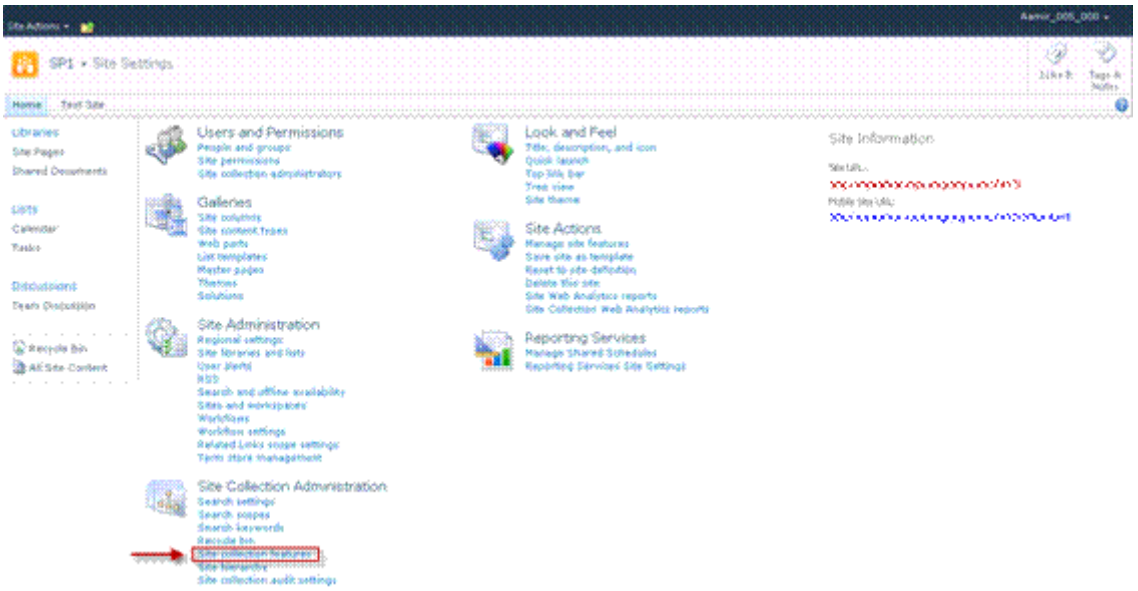


Figure 251. Site Settings: Site collection features

__ 5. Now for ProfilesSearchWebPart and TagCloudWebPart click **Activate** to activate the web parts to take place. Then click **OK**.

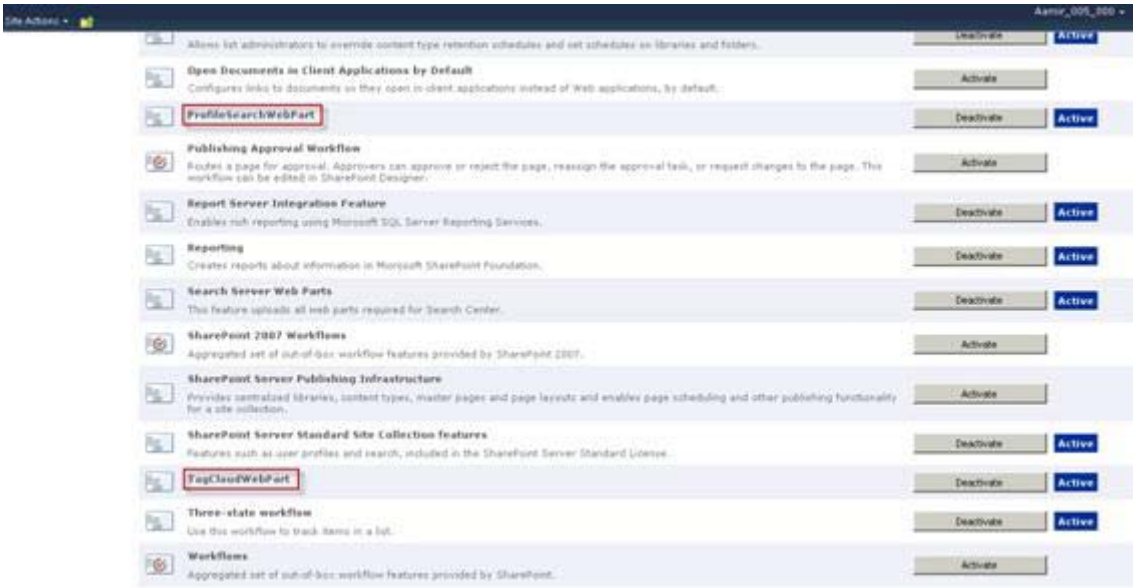


Figure 252. Site Actions

The deployment of the IBM Connections plug-in is now completed.

7. Configuring SharePoint SSO/security

Configuring the LDAP Web.Config files

Configure forms-based authentication for a claims-based web application

The following procedure in the URL provided shows how to configure a forms-based web application to use an LDAP provider:

`http://technet.microsoft.com/en-us/library/ee806890.aspx.`

Add LDAP users to SharePoint site

__ 1. Log on to the SharePoint server and from the start menu click SharePoint 2010 Central Administration.

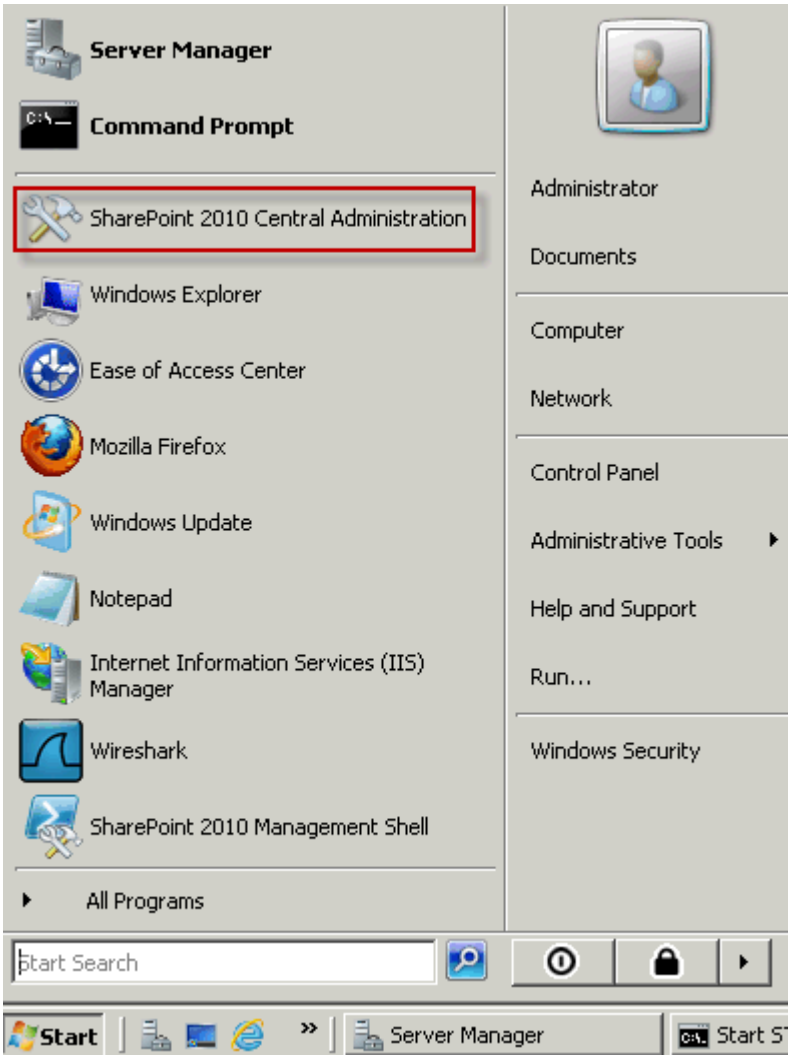


Figure 253. SharePoint 2010 Central Administration

__ 2. Under Application Management, click **Manage web applications**.

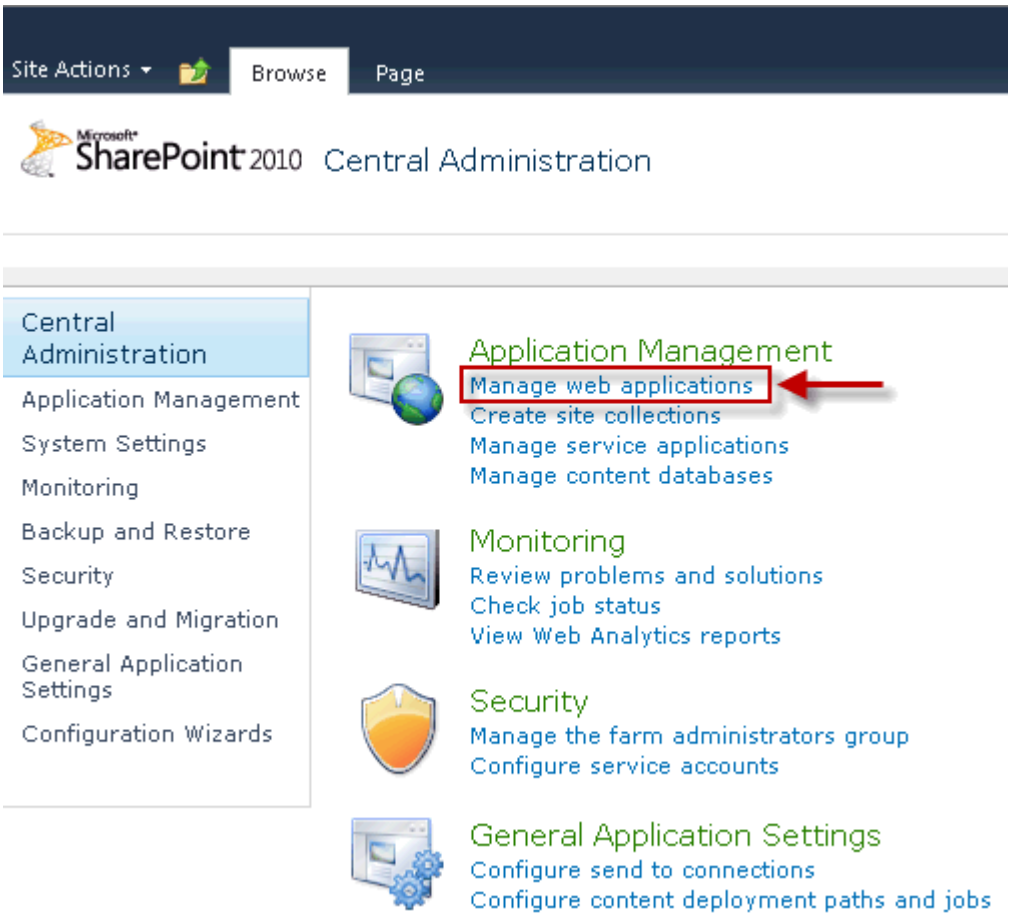


Figure 254. Application Management: Manage web applications

__ 3. Now highlight the SharePoint site and from the menu ribbon click **Authentication Providers**.

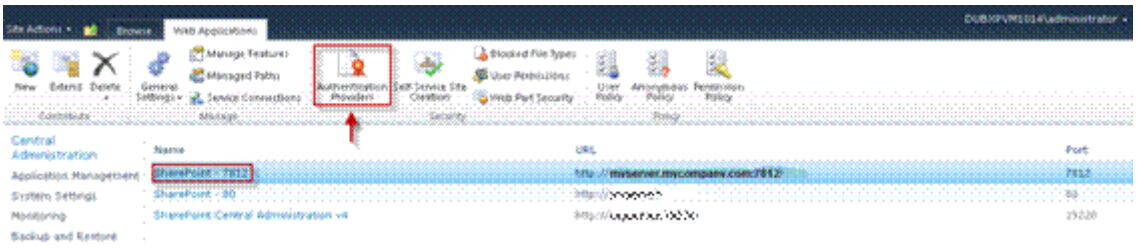


Figure 255. Authentication Providers

__ 4. Click **Default** for Claims Based Authentication.

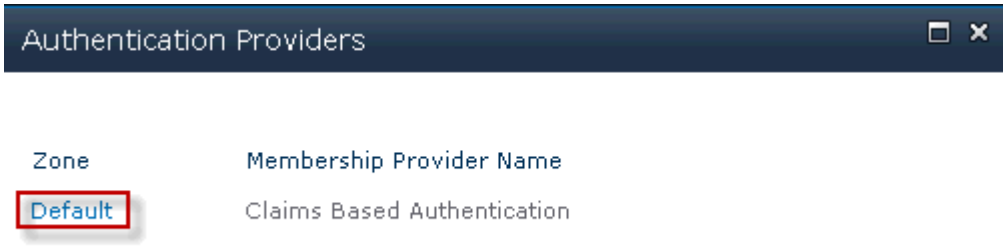


Figure 256. Authentication Providers: Default

__ 5. In section Claims Authentication Types, select **Enable Forms Based Authentication (FBA)**, and then enter the ASP.NET Membership provider name and ASP.NET Role manager name. Then, click **Save** to continue.

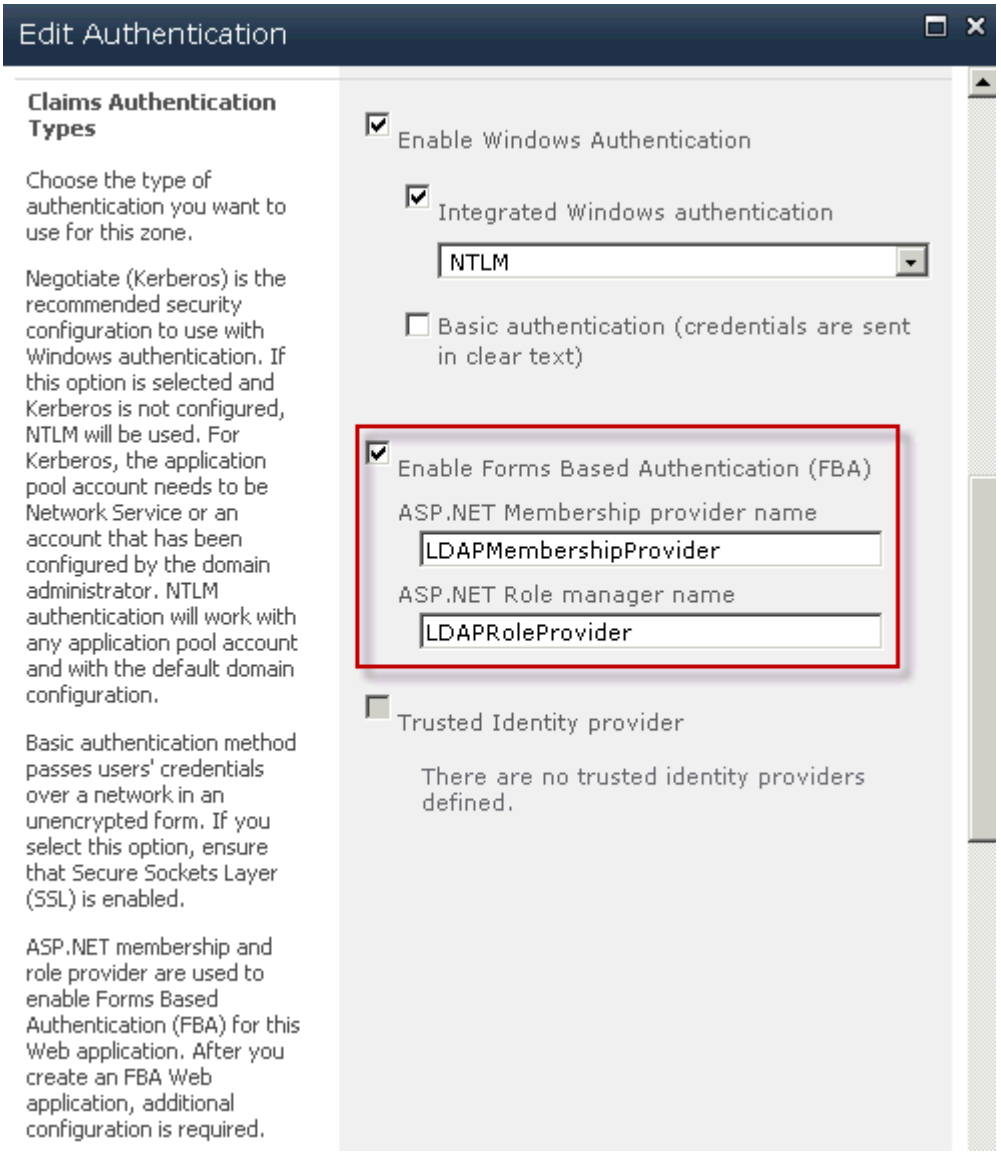


Figure 257. Edit authentication

__ 6. Select **Default Sign In Page**.

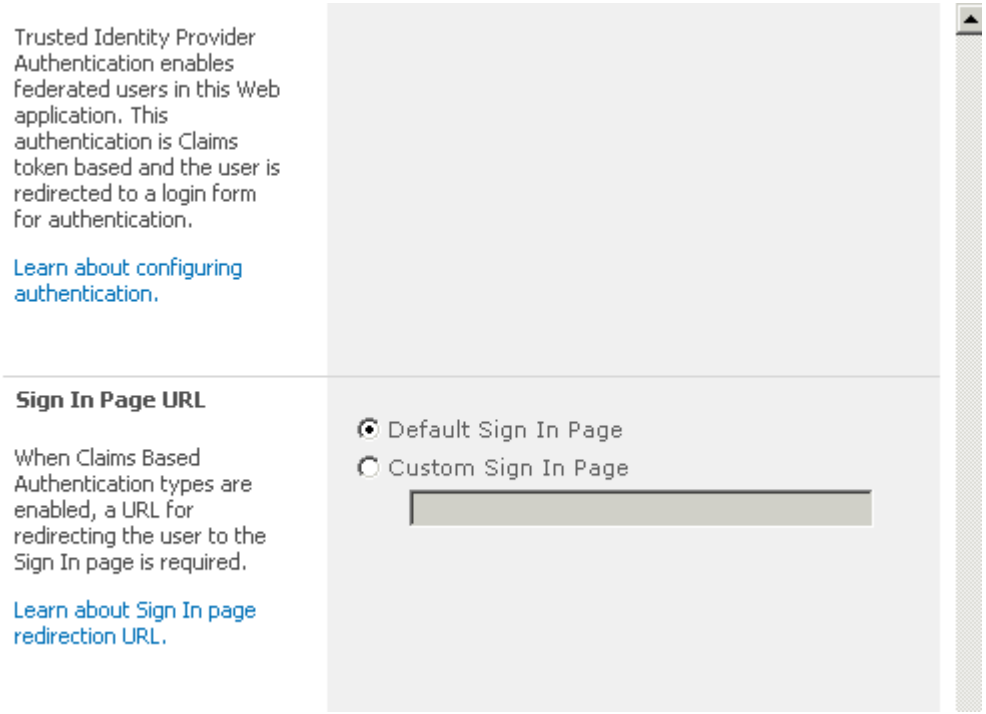


Figure 258. Sign In Page URL

__ 7. Click **Yes** to enable Client Integration, and then **Save**.

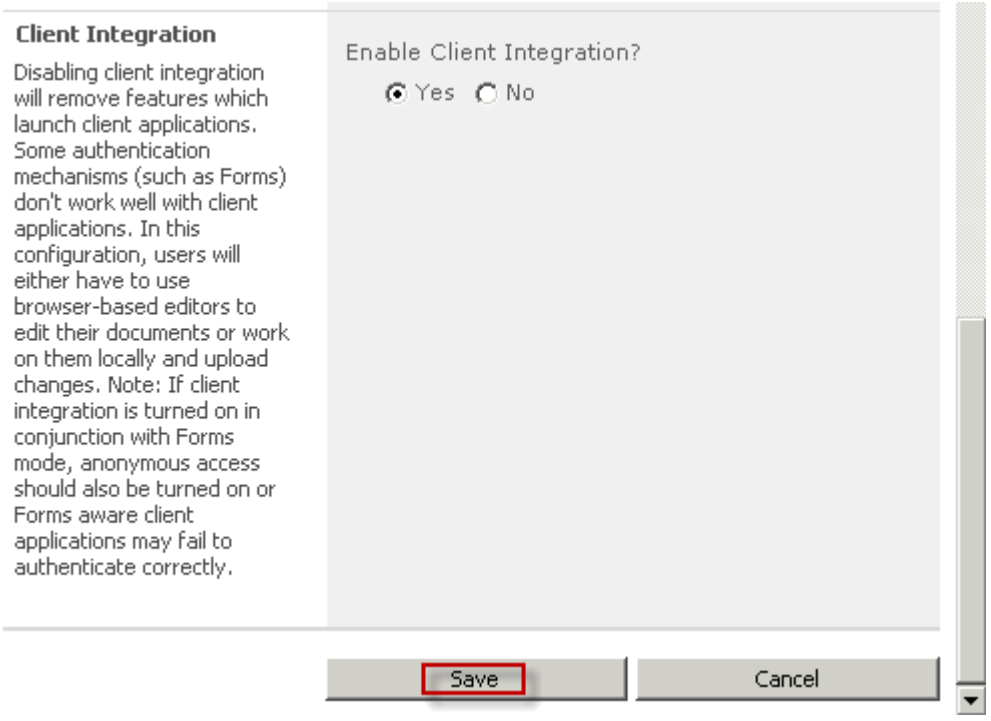


Figure 259. Enable Client Integration

__ 8. Now from the menu ribbon click **User Policy**.

Figure 260. User Policy

__ 9. Leave the default All zones to add users and click **Next** to continue.

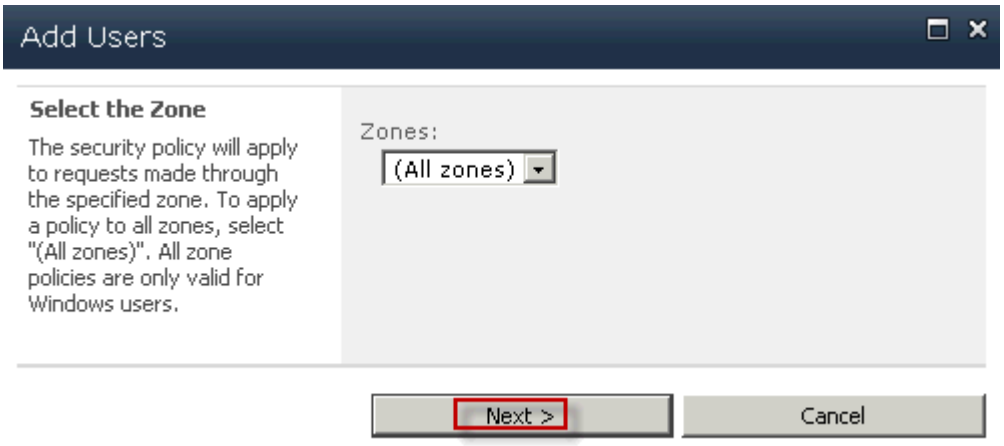


Figure 261. Select the Zone

__ 10. Click **Add Users**.

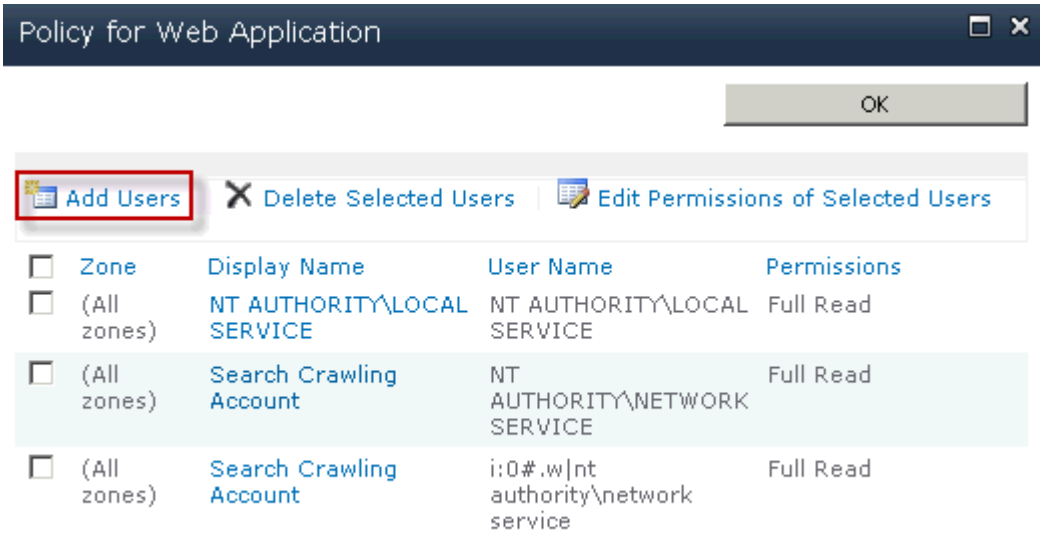


Figure 262. Policy for Web Application: Add Users

__ 11. Now type in the user names you want to add from the third-party LDAP server, and click the person/tick icon to search for and add the user. When you added all the users, click **Finish** to continue.

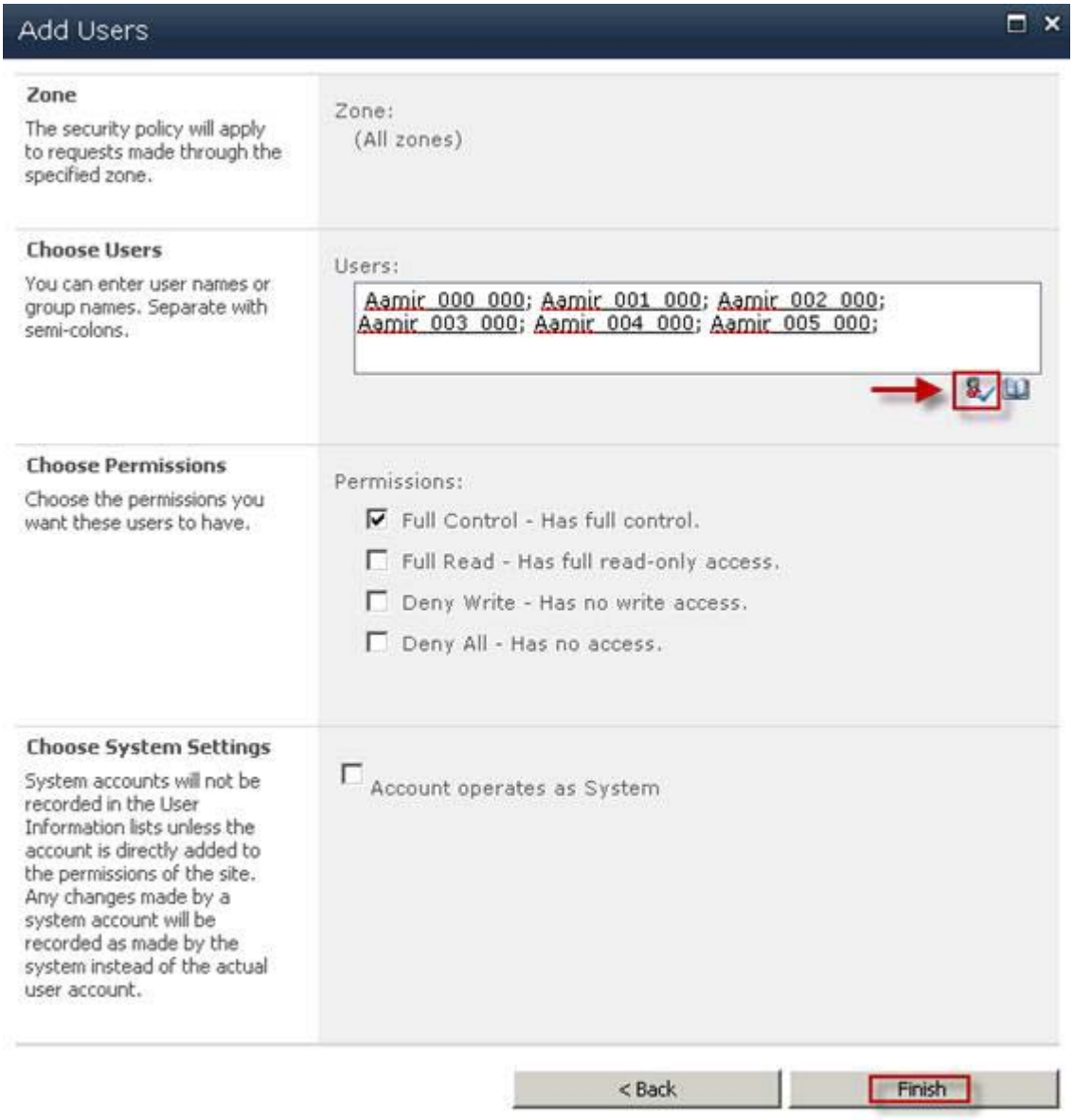


Figure 263. Adding users

__ 12. All users that were selected are now added. Click **OK** to complete the setup.

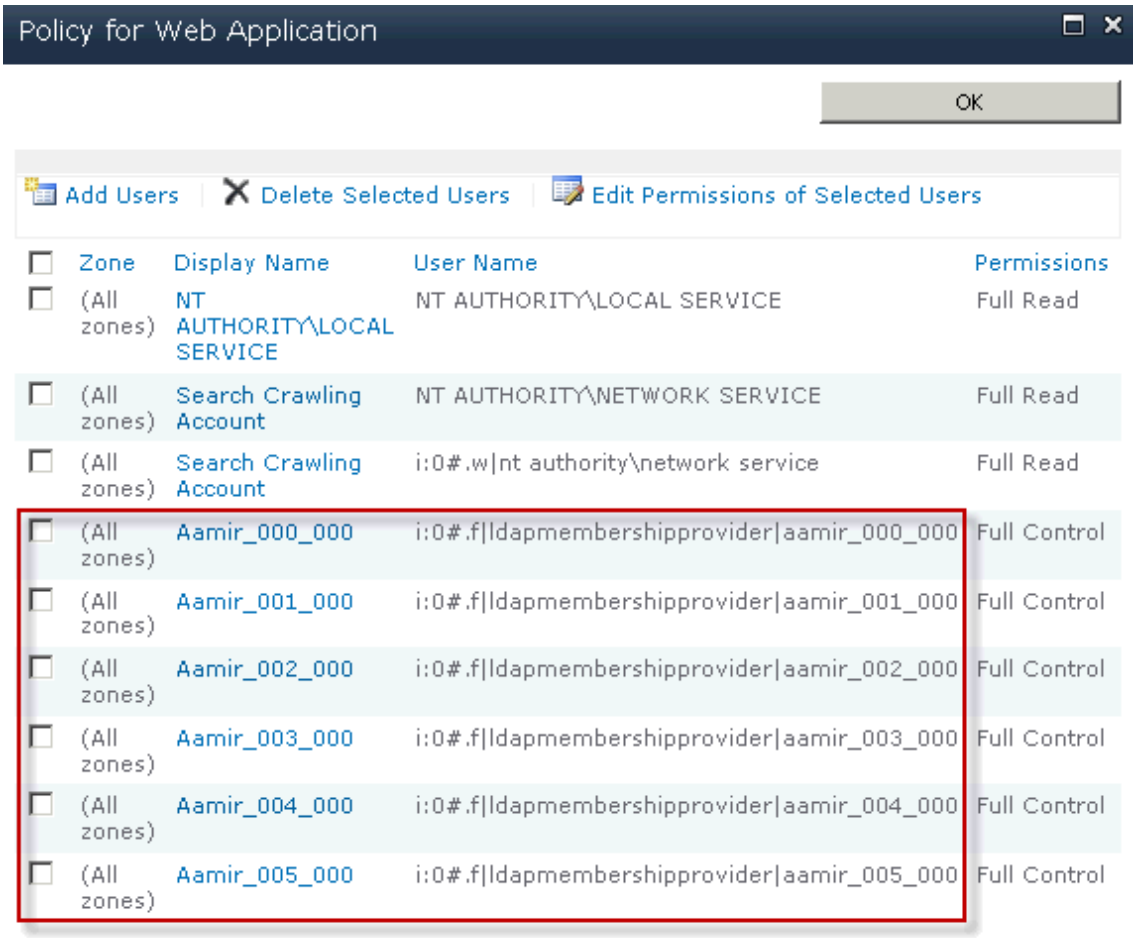


Figure 264. Users successfully added

IBM