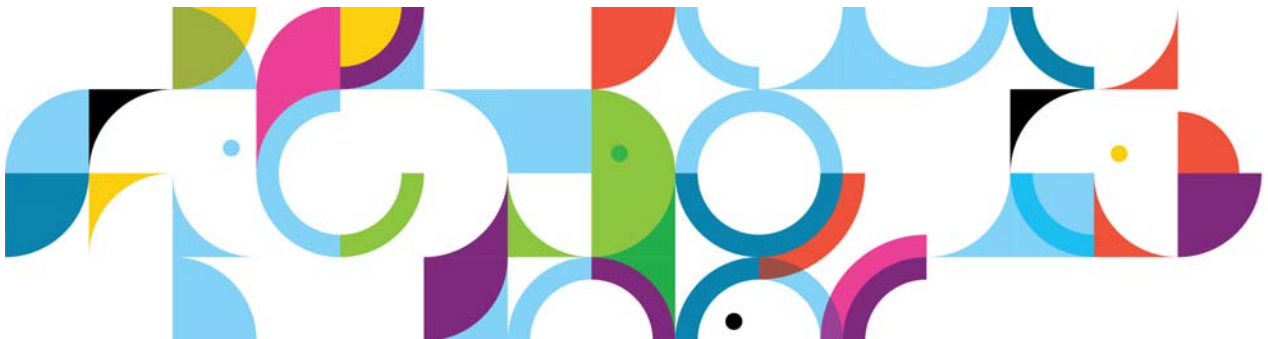




*IBM Connections 4 Public
Deployment Scenarios*

Deployment Scenarios

ERC 1.0



Trademarks

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

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

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

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

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

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

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

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

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

January 2013 edition

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

© Copyright International Business Machines Corporation 2013.

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

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

IBM Connections 4: PDS SUSE SiteMinder

About the author

Ravisanka Pangulur is a software engineer for the IBM Collaboration Solutions system verification test team.

Overview

This scenario explains how to deploy IBM Connections 4.0 in a network deployment that involves multiple computers, that is, 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.

Deployment topology

Installing IBM® Connections 4.0 in a network deployment to achieve optimum scaling, load balancing, and failover:

A network deployment can consist of a single server with all applications installed, or two or more sets of servers that are grouped to share the workload. You must also configure an additional system with WebSphere® Application Server Network Deployment Manager, which enables you to build, manage, and tune the clustered servers.

A network deployment provides the administrator with a central management facility, and it ensures that users have constant access to data. It balances the workload between servers, improves server performance, and facilitates the maintenance of performance when the number of users increases. The added reliability also requires a larger number of systems and the experienced administrative personnel who can manage them.

When you are installing IBM Connections 4.0, you have three deployment options. This author's deployment uses Medium Topology.

Medium deployment

Install a subset of applications in separate clusters. IBM Connections provides three predefined cluster names that are shared among all 12 applications. Use this option to distribute applications according to your usage expectations. For instance, you might anticipate higher loads for the Profiles application and install it in its own cluster, while other applications might be installed in a different cluster. This option allows you to maximize the use of available hardware and system resources to suit your needs.

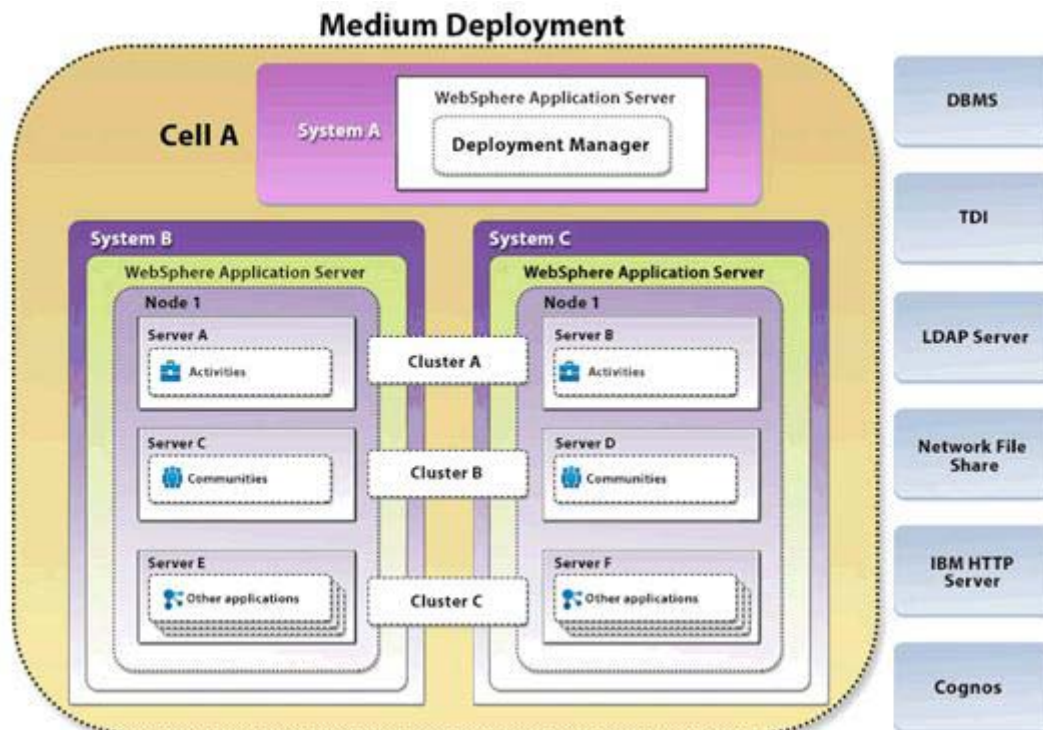


Figure 1. Medium deployment

- In a multi-node cluster, you must configure network share directories for content stores. When using NFS, use NFS v4 because NFS v3 lacks advanced locking capability. When using Microsoft SMB Protocol for file-sharing, use the UNC file-naming convention; for example: \\<machine-name>\<share-name>.
- You can assign various combinations of applications to clusters in many different ways, depending on your usage and expectations.
- The number of JVMs that you need for each cluster depends on the user population and workload. For failover, you must have two JVMs per application, or two nodes for each cluster, scaled horizontally. Horizontal scaling refers to having multiple JVMs per application with each JVM running on a WebSphere Application Server instance. Vertical scaling refers to running multiple JVMs for the same application on a single WebSphere Application Server instance. Vertical scaling is not officially supported in IBM Connections. However, it is typically not needed unless your server has several processors.
- For performance and security reasons, consider use of a proxy server in your deployment.

Systems and naming conventions that are used in this document

Computer host name	Applications	Version#	OS/version	RAM/ CPU	VM or HW
dm&IBM HTTP Server.machine.com	WebSphere Application Server Deployment Manager IBM HTTP Server	WebSphere Application Server v7.0.0.21 (64 bit) IBM HTTP Server v7.0.0.21 (32 bit)	SLES 10 SP4 64 bit	8 G / 2 CPUs	VM
node1.machine.com	Node1 (WebSphere Application Server)	WebSphere Application Server v7.0.0.21	SUSE 10 Linux	8 G / 2 CPUs	
node2.machine.com	Node2 (WebSphere Application Server)	WebSphere Application Server v7.0.0.21		8 G / 2 CPUs	
db2server.machine.com	DB2 Tivoli Directory Integrator)	DB2 v9.7+FP6 Tivoli Directory Integrator v9.1+FP5		8 G / 2 CPUs	

Contents

1. IBM WebSphere Deployment Manager: 7.0.0.0
2. IBM WebSphere Application Server: 7.0.0.0
3. Set up IBM HTTP Server v7.0 and plug-ins
4. Install WebSphere Application Server 7.0 Update Installer
5. Update Deployment Manager, Application Server, IBM HTTP Server, IBM HTTP Server plug-ins, and SDKs to WebSphere Application Server 7.0.0.21 FixPack
6. Federate Application Server into Deployment Manager
7. Enable security on your Deployment Manager
8. Federate LDAP repositories
9. Installation of DB2 9.7 Server
10. Installing DB2 9.7 client on your Deployment Manager and Application Server nodes
11. Installation of DB2 9.7: FixPack 6: Server + Client
12. Apply the DB2 license to your server
13. Create Connections databases on DB2 server
14. Configuring Tivoli Directory Integrator
15. Installation of Connections 4.0
16. Post-installation tasks

1. IBM WebSphere Deployment Manager: 7.0.0.0

1. Copy the WebSphere Application Server 7.0 setup image C1G35ML.tar.gz to your dm&IBM HTTP Server.machine.com and start the Deployment Manager installer by running the installation from within the WebSphere Application Server folder... you should see the following. Click **Next** to continue.

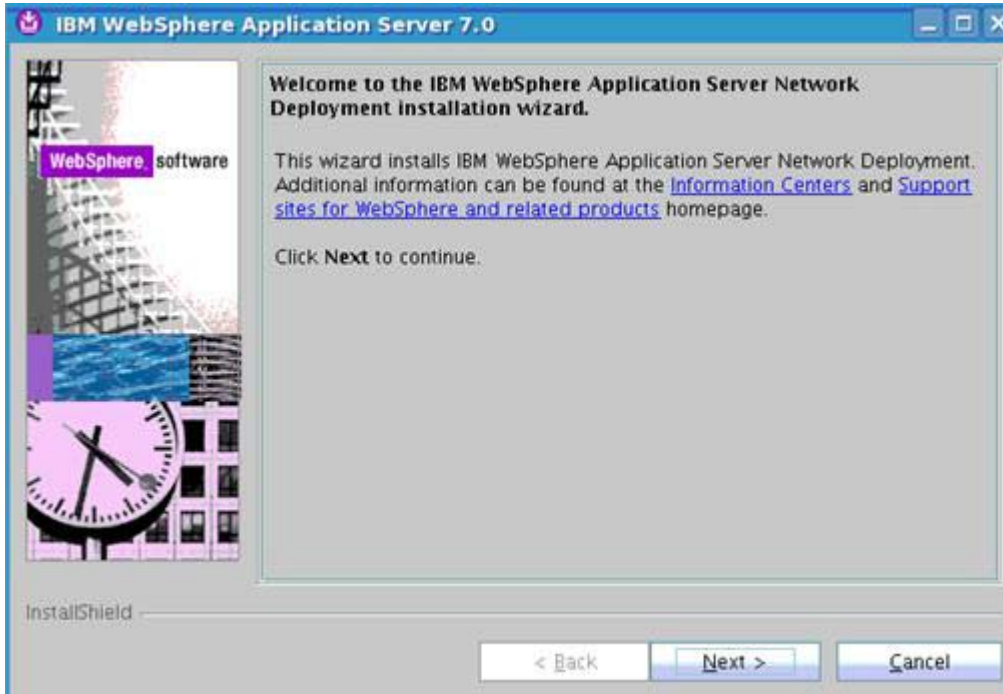


Figure 2. IBM WebSphere Application Server 7.0

___ 2. Accept the license agreement and click **Next** to continue.

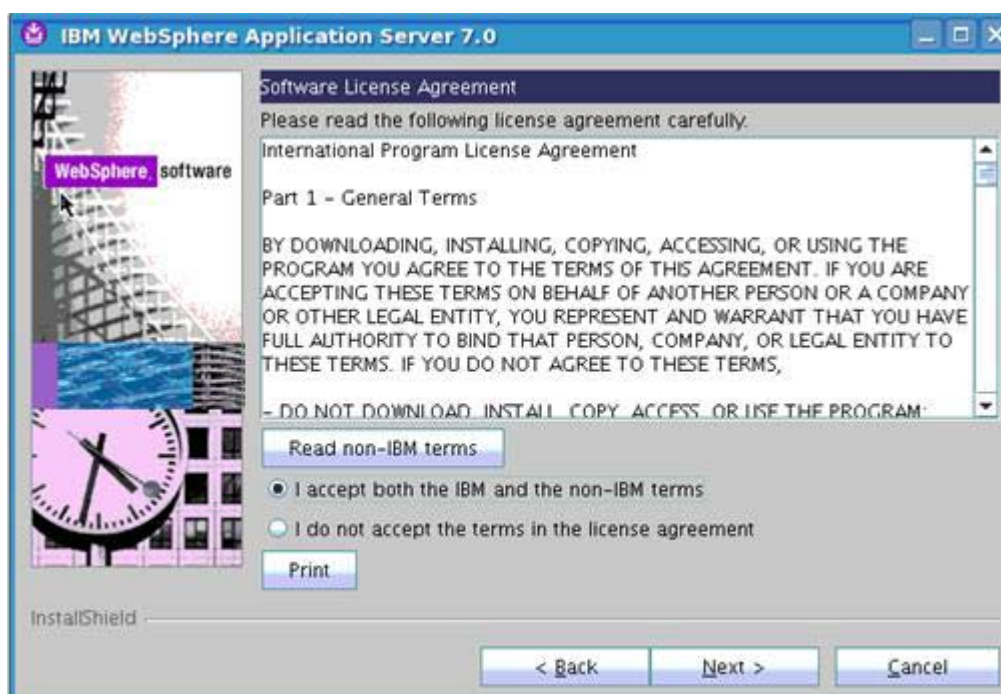


Figure 3. IBM WebSphere Application Server 7.0: License agreement

___ 3. Click **Next** at the system prerequisites check.

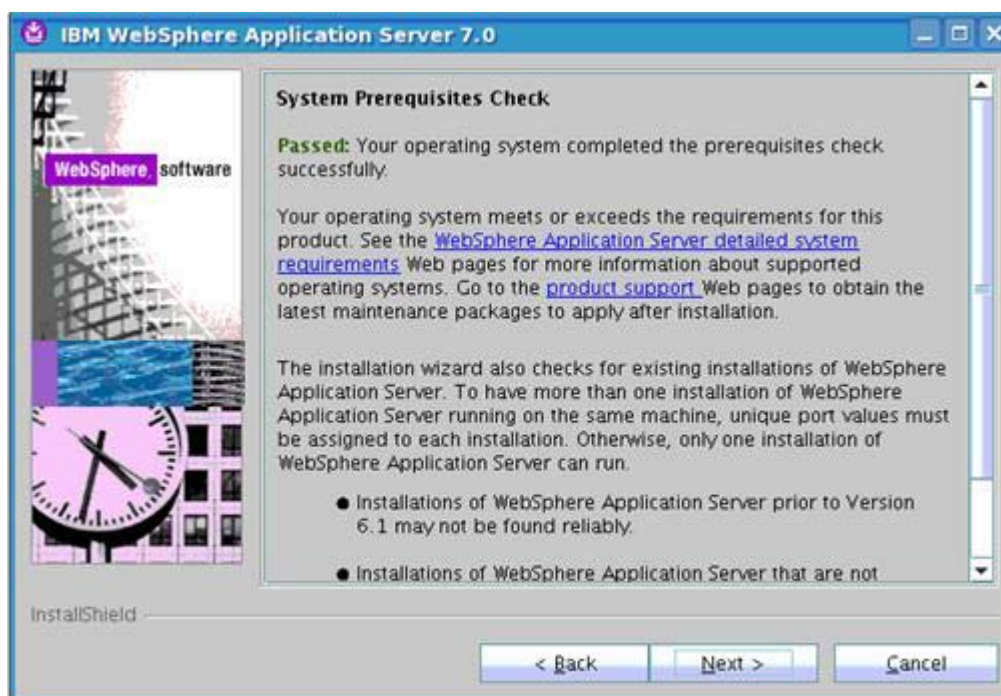


Figure 4. IBM WebSphere Application Server 7.0: System Prerequisites Check

4. Do not select anything from the optional features and click **Next** to continue.

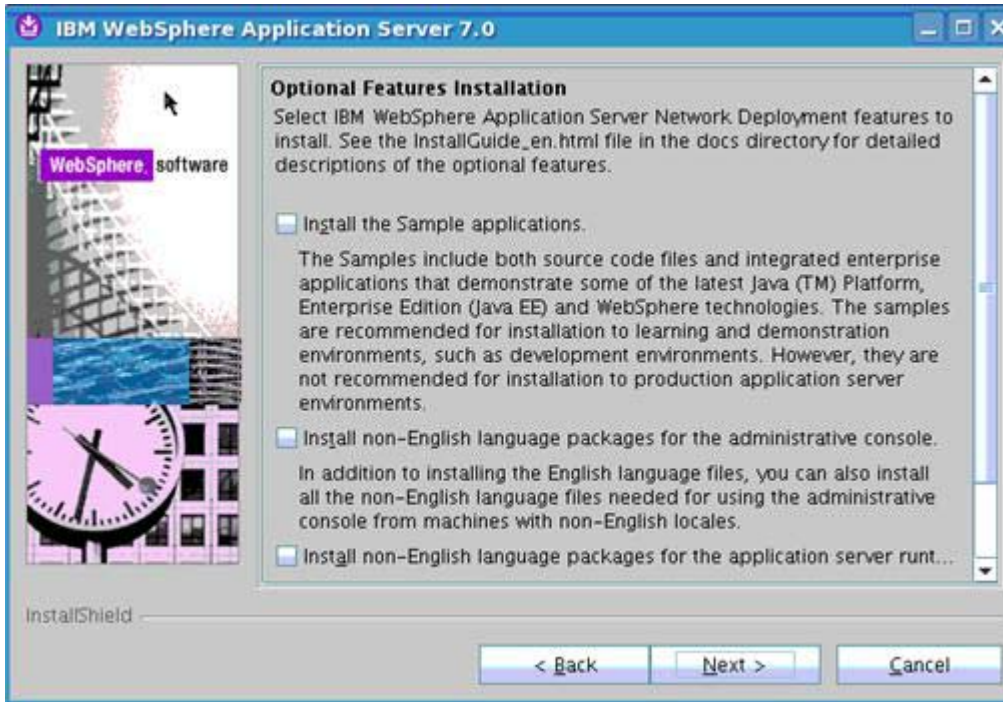


Figure 5. IBM WebSphere Application Server 7.0: Optional Features Installation

5. Change the default installation path if needed and click **Next** to continue.

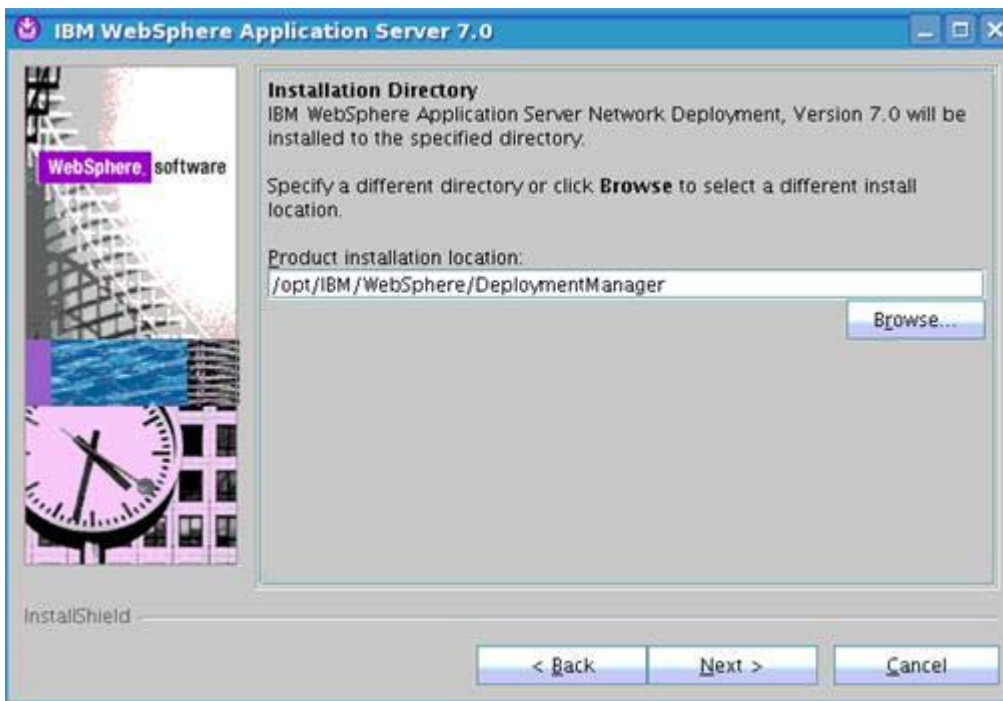


Figure 6. IBM WebSphere Application Server 7.0: Installation Directory

- ___ 6. Click **Management**, to install the Deployment Manager. Then, click **Next** to continue.

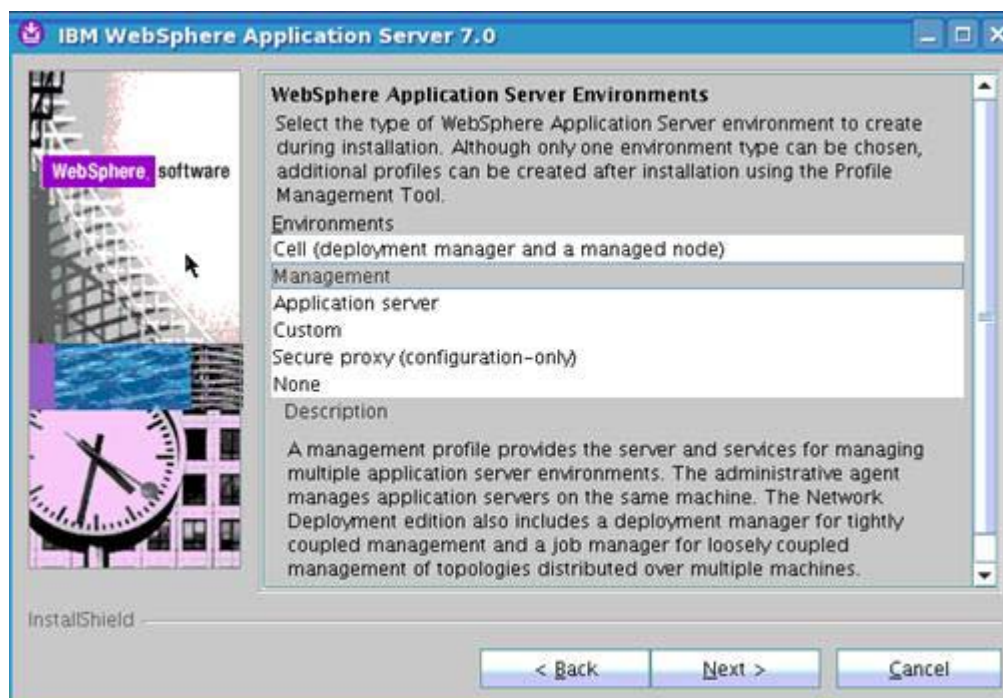


Figure 7. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments

- ___ 7. Click **Deployment Manager** and then **Next** to continue.

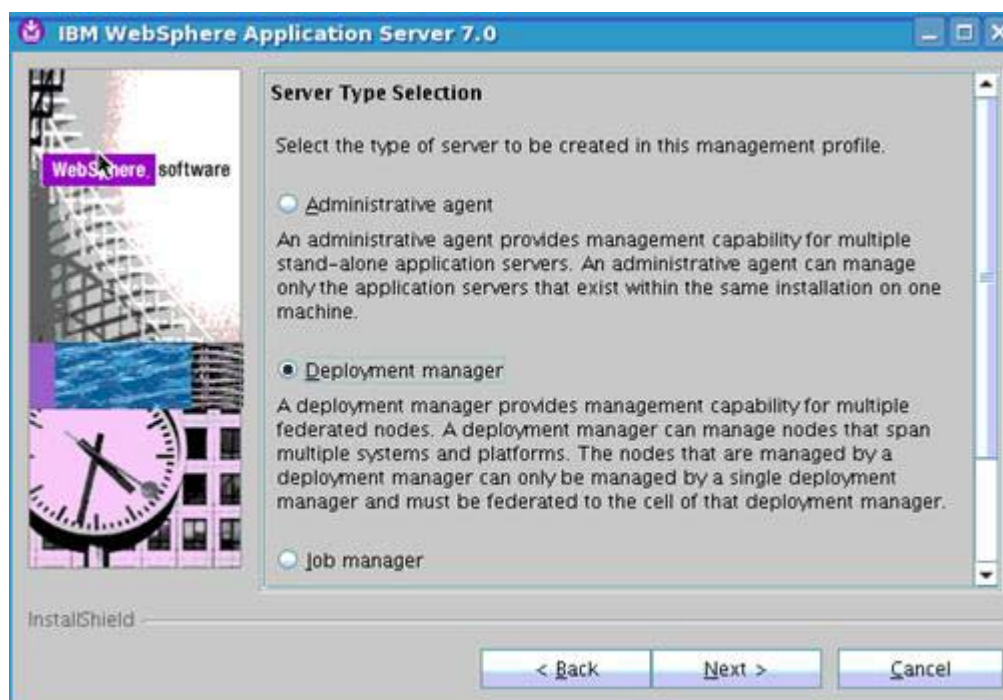


Figure 8. IBM WebSphere Application Server 7.0: Server Type Selection

8. Enter the user name and password and click **Next** to continue.

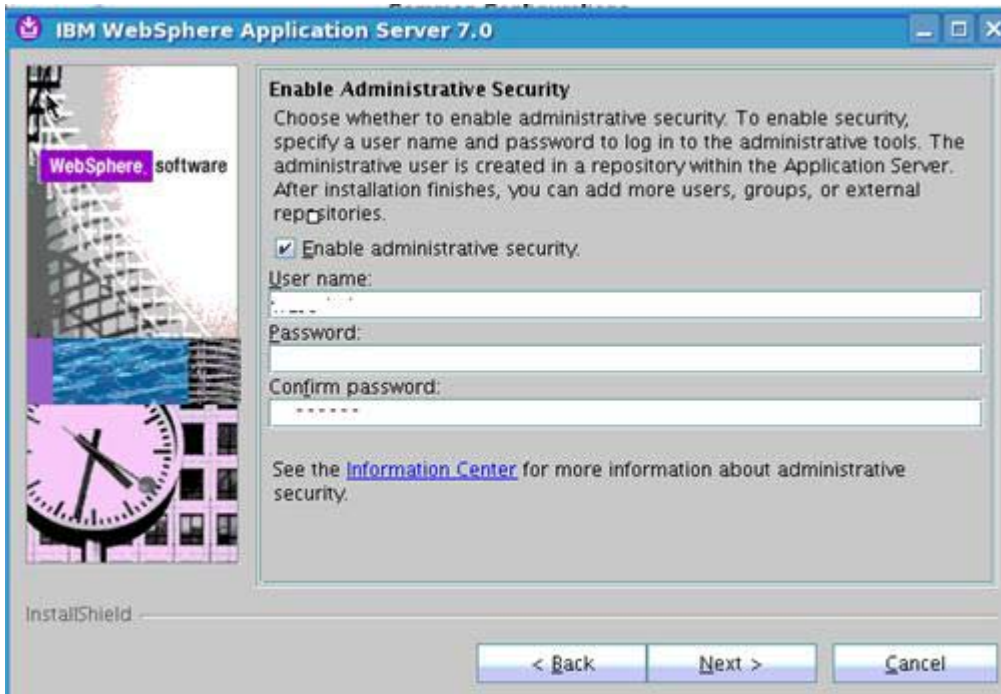


Figure 9. IBM WebSphere Application Server 7.0: Enable Administrative Security

9. Do not select "Create a repository". Click **Next** to continue.

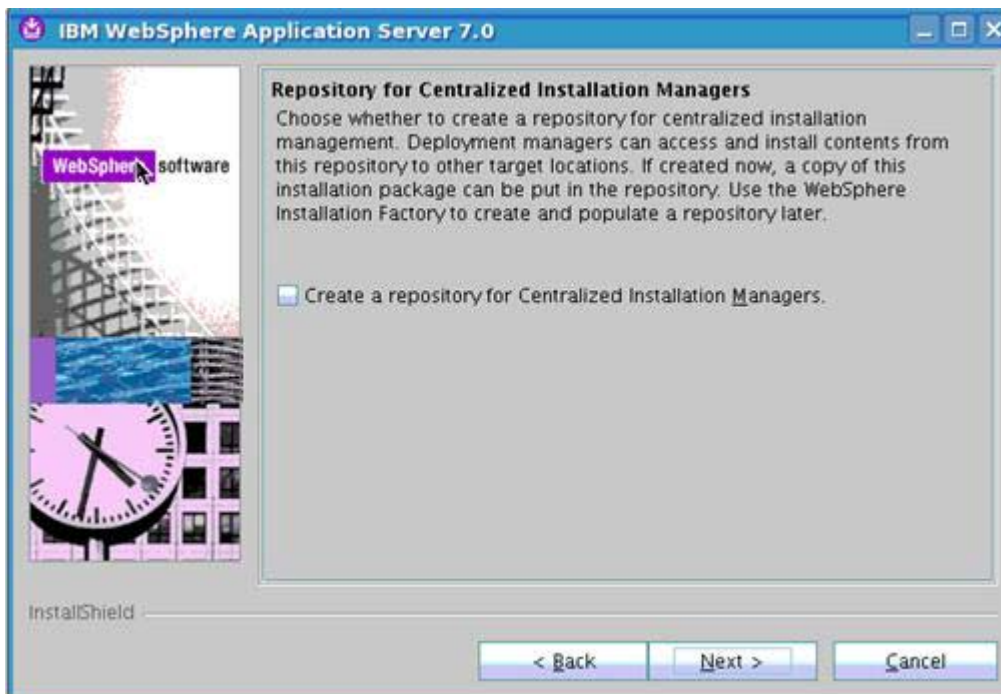


Figure 10. IBM WebSphere Application Server 7.0: Repository for Centralized Installation Managers

___ 10. Verify the permissions and click **Next**.

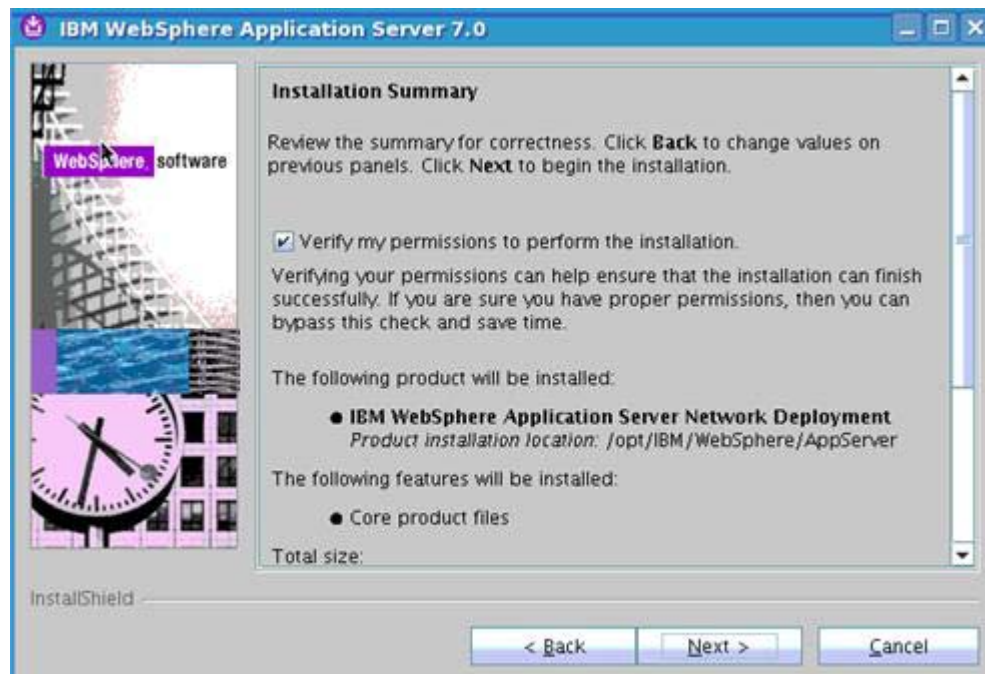


Figure 11. IBM WebSphere Application Server 7.0: Installation Summary: Verification

___ 11. Review the installation summary and click **Next**.

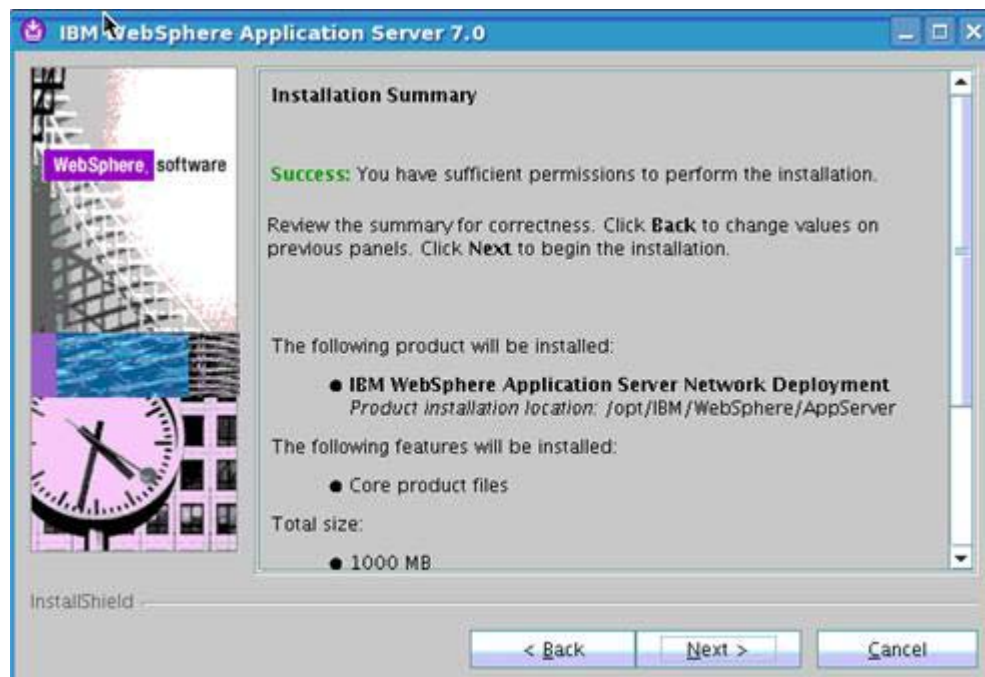


Figure 12. IBM WebSphere Application Server 7.0: Installation Summary

The installation starts to copy files.

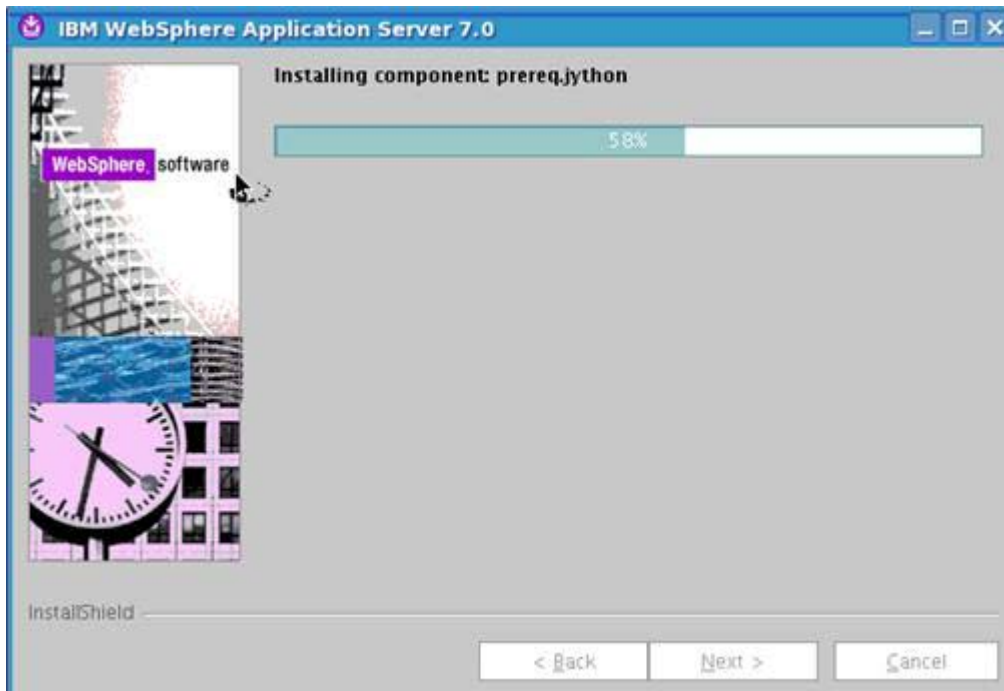


Figure 13. IBM WebSphere Application Server 7.0: Component installation in progress

___ 12. After some time the installation finishes. Click **Finish** to exit the installer.

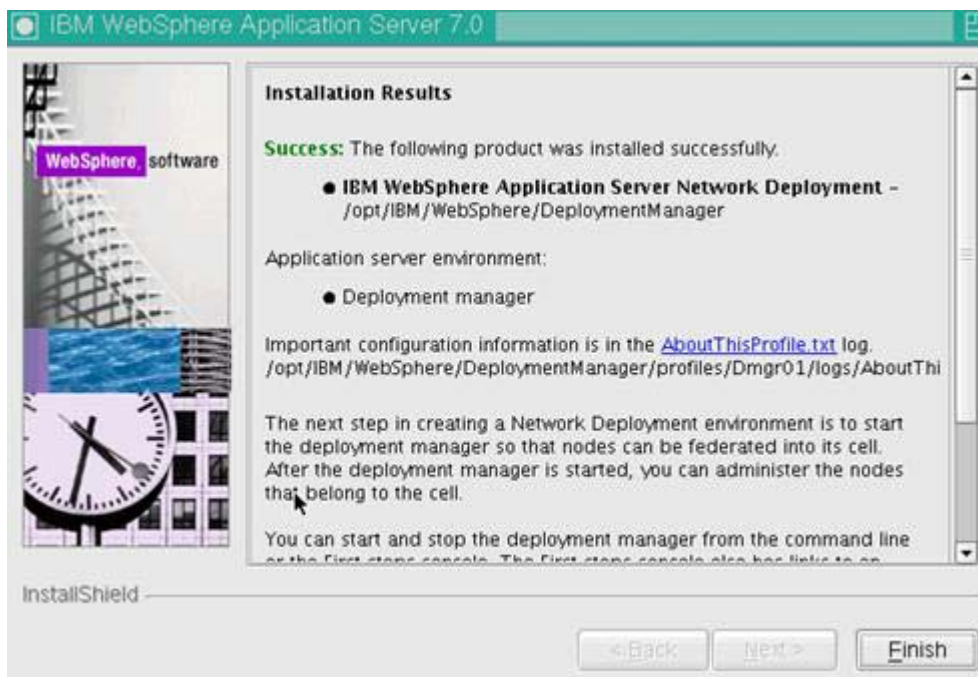


Figure 14. IBM WebSphere Application Server 7.0: Installation Results

13. In the First steps screen, click **Installation verification**.



Figure 15. WebSphere Application Server: First steps

The installation verification tool succeeded, as shown in the following figure.

```

First steps output - Installation verification
Server name is: dmgr
Profile name is: Dmgr01
Profile home is: /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01
Profile type is: management
Cell name is: dm & ihs. Cell01
Node name is: dm & ihs - CellManager01
Current encoding is: UTF-8
Start running the following command: /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin/startServer.sh dmgr -profileName Dmgr01
>ADMU0116I: Tool information is being logged in file
> /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/startServer.log
>ADMU0128I: Starting tool with the Dmgr01 profile
>ADMU3100I: Reading configuration for server: dmgr
>ADMU3200I: Server launched. Waiting for initialization status.
>ADMU3000I: Server dmgr open for e-business; process id is 10146
Server port number is: 9060
VTL0010I: Connecting to the dm&ihs.machine.com WebSphere Application Server on port: 9060
VTL0015I: WebSphere Application Server dm&ihs.machine.com is running on port: 9060 for profile Dmgr01
VTL0035I: The Installation Verification Tool is scanning the /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/SystemOut.log file
[10/5/11 12:35:01:144 IST] 00000000 WSKeyStore W CWPY0041W: One or more key stores are using the default password.
[10/5/11 12:35:05:185 IST] 00000000 ThreadPoolMgr W WSVR0626W: The ThreadPool setting on the ObjectRequestBroker service is deprecated
[10/5/11 12:35:33:851 IST] 00000000 TcpTransport W ADMDO025W: In process discovery, the 127.0.0.1 IP address is used to advertise an end
VTL0040I: 3 errors/warnings are detected in the /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/SystemOut.log file
VTL0070I: The Installation Verification Tool verification succeeded.
  
```

Figure 16. First steps output: Installation verification

2. IBM WebSphere Application Server: 7.0.0.0



Note

Do this step on each node of your Connections cluster.

1. Copy the WebSphere Application Server 7.0 setup image `C1G35ML.tar.gz` to your `node1.machine.com` and `node2.machine.com` and start the Application Server installer by running installation from within the WebSphere Application Server folder. Click **Next** to continue.

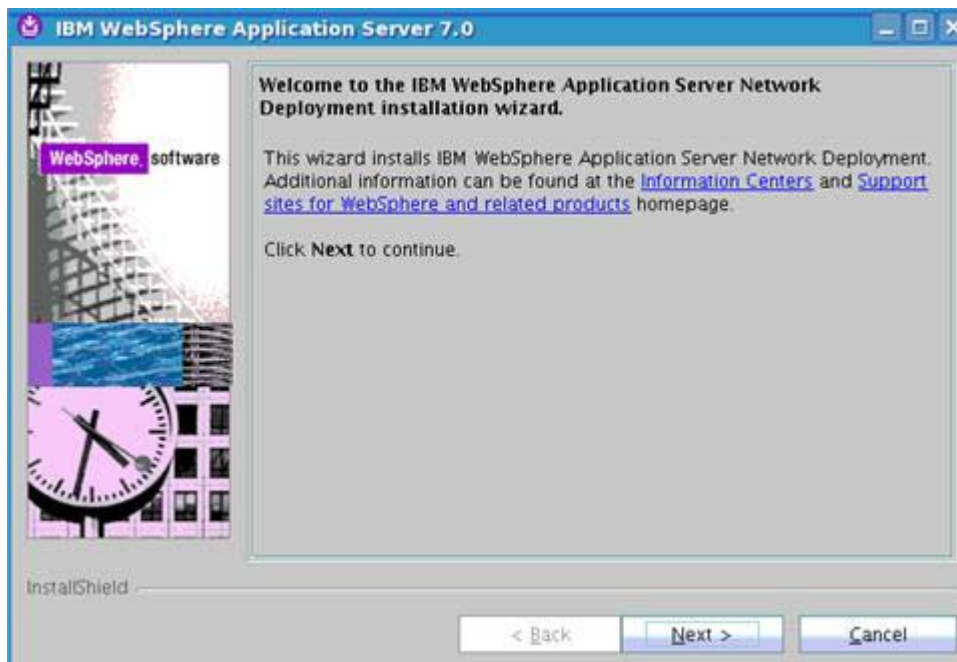


Figure 17. IBM WebSphere Application Server 7.0: Welcome

- ___ 2. Accept the license agreement and click **Next** to continue.

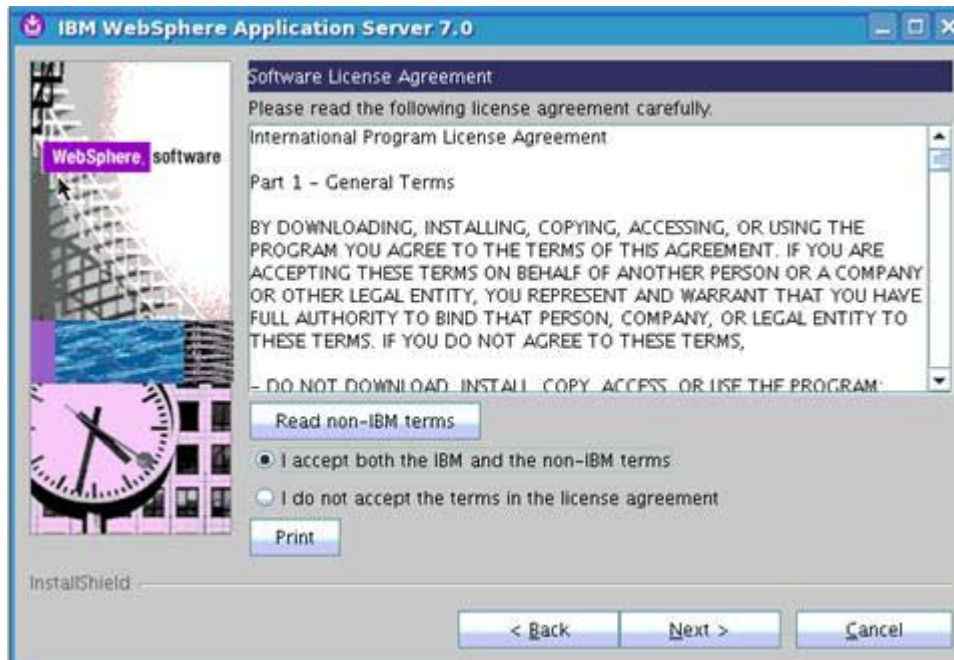


Figure 18. IBM WebSphere Application Server 7.0: Software License Agreement

- ___ 3. Click **Next** in the system prerequisites check panel.

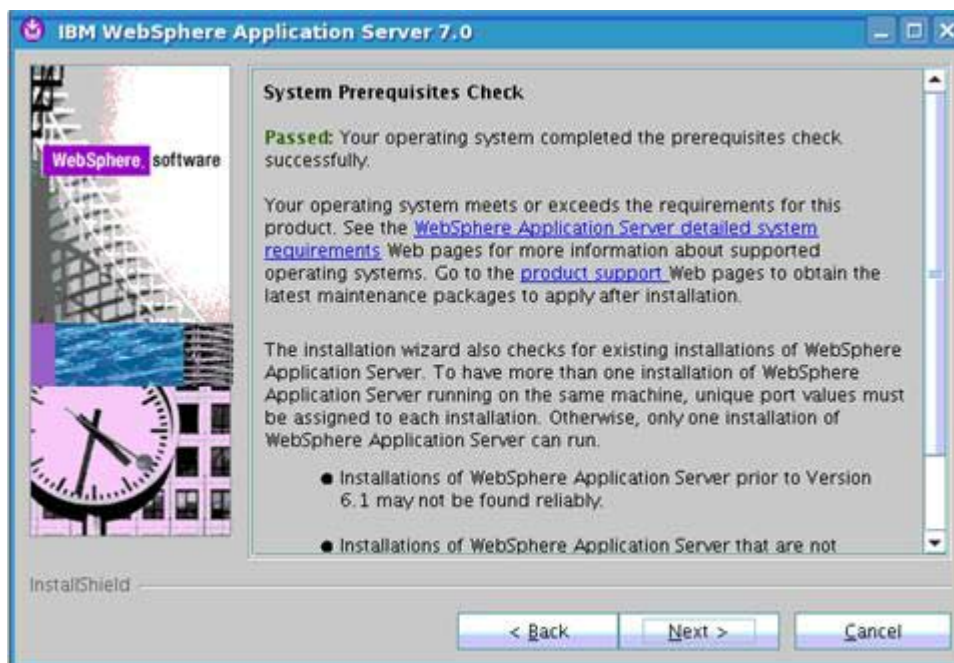


Figure 19. IBM WebSphere Application Server 7.0: System Prerequisites Check

- 4. Select **Install a new copy of IBM WebSphere Application Server Network Deployment** (it shows only if the Deployment Manager and Application Server are installed on the same computer).

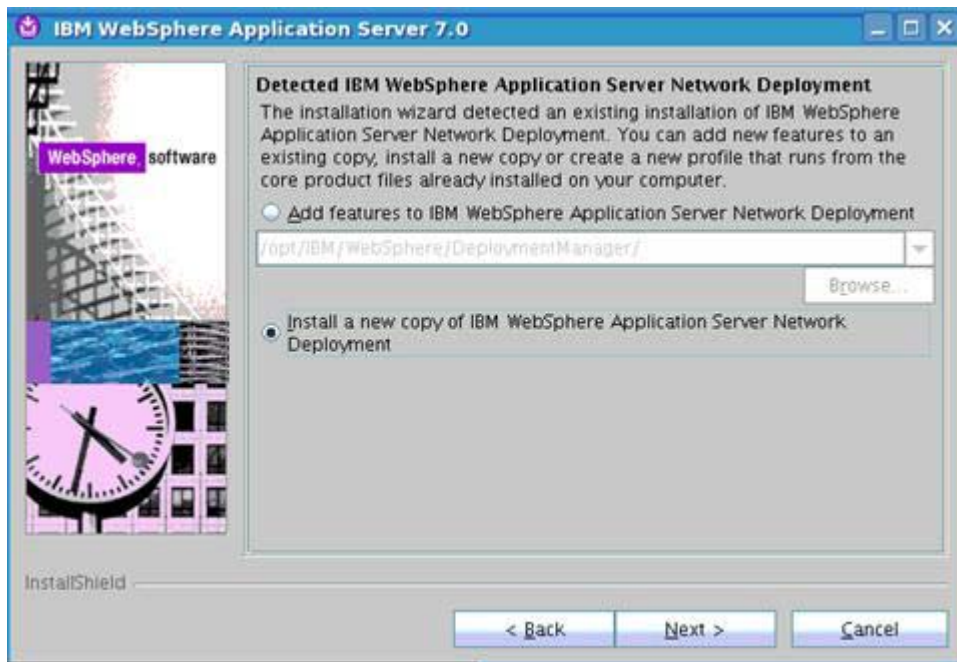


Figure 20. IBM WebSphere Application Server 7.0: Detected IBM WebSphere Application Server Network Deployment

- 5. Do not select anything from the optional features and click **Next** to continue.

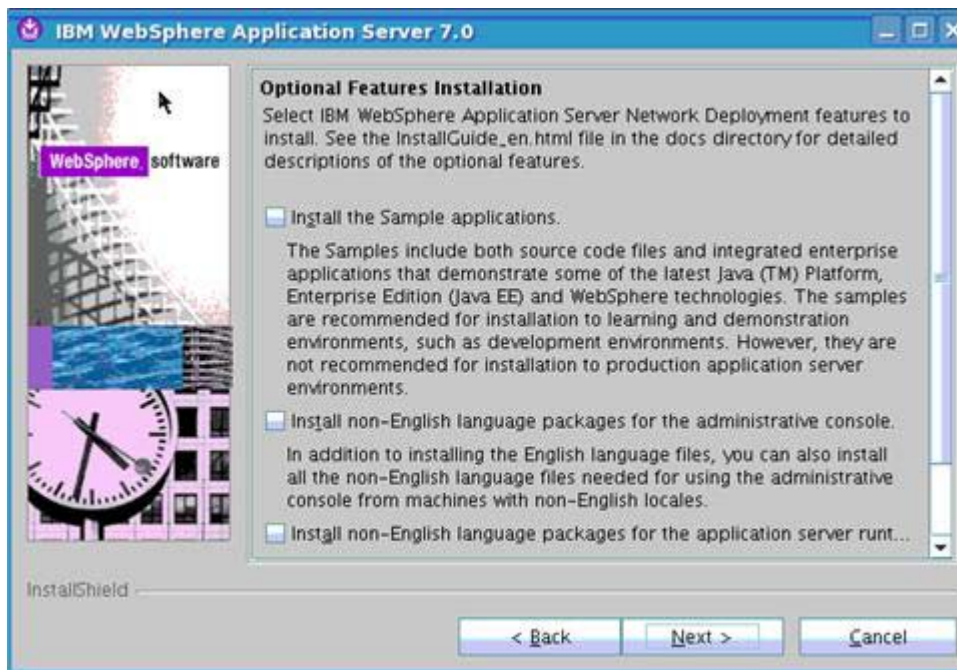


Figure 21. IBM WebSphere Application Server 7.0: Optional Features Installation

- ___ 6. Change the default installation path if needed and click **Next** to continue.

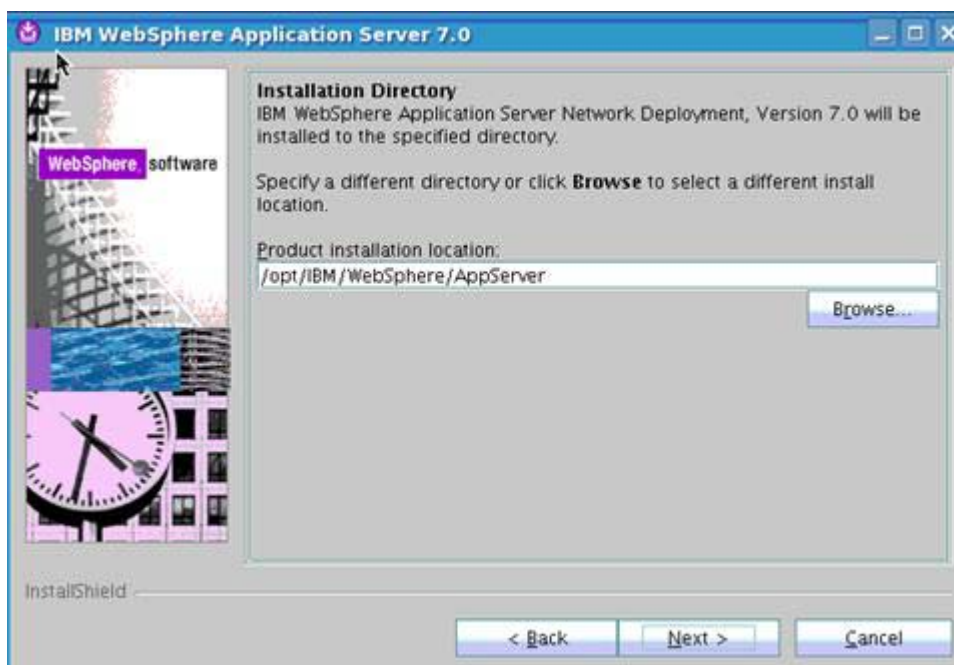


Figure 22. IBM WebSphere Application Server 7.0: Installation Directory

- ___ 7. Select **Application Server** and click **Next** to continue.

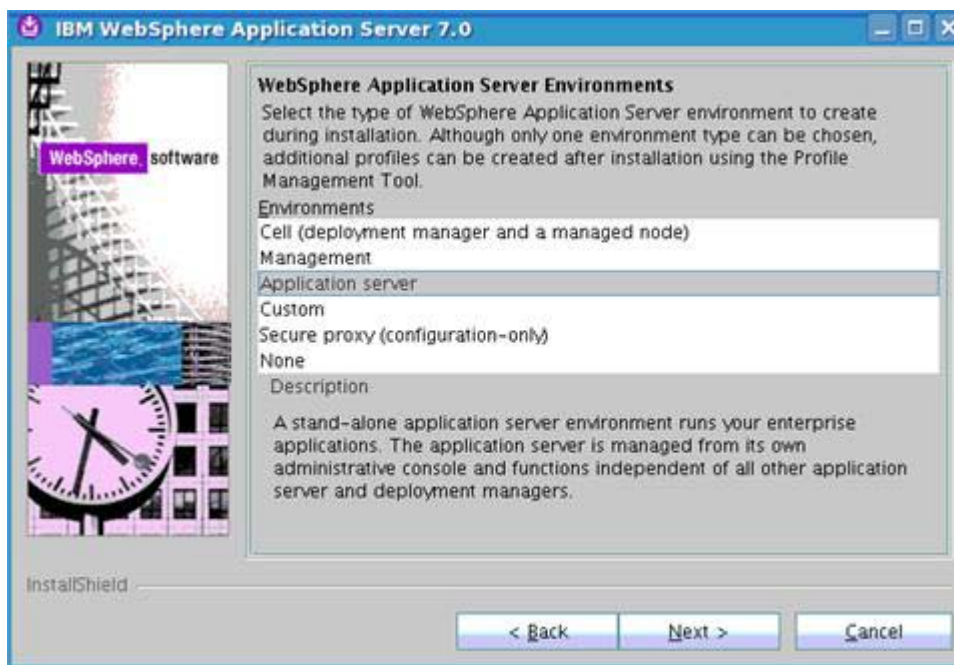


Figure 23. IBM WebSphere Application Server 7.0: WebSphere Application Server Environments

___ 8. Enter an admin name and password and click **Next** to continue.



Figure 24. IBM WebSphere Application Server 7.0: Enable Administrative Security

___ 9. Verify the permissions and click **Next** to continue.

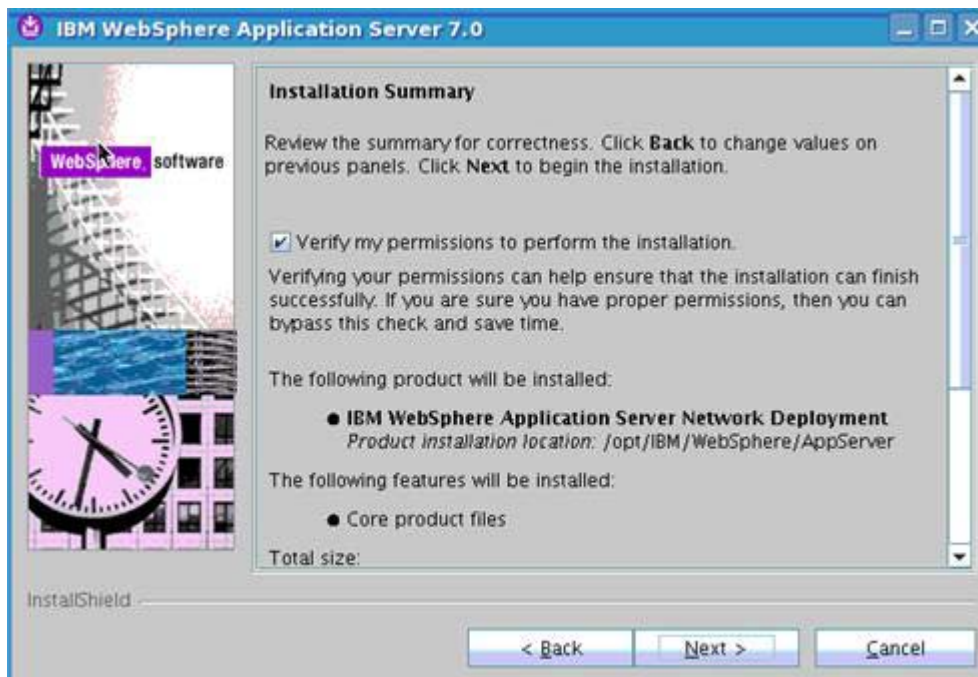


Figure 25. IBM WebSphere Application Server 7.0: Installation Summary: Verification

___ 10. Review the Installation Summary and click **Next** to continue.

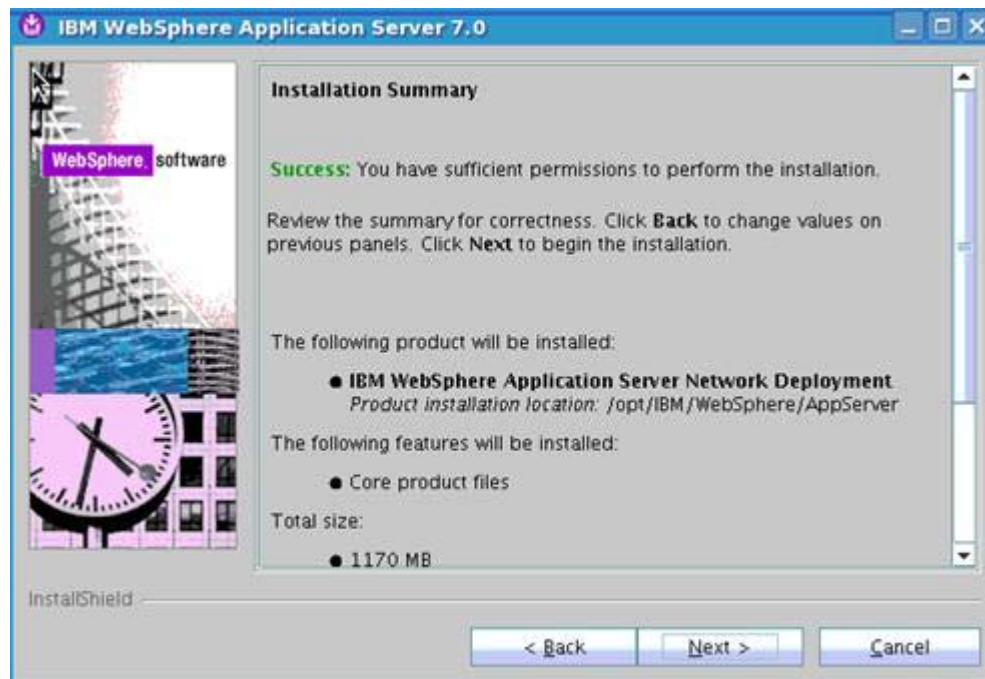


Figure 26. IBM WebSphere Application Server 7.0: Installation Summary

The installation starts to copy files.

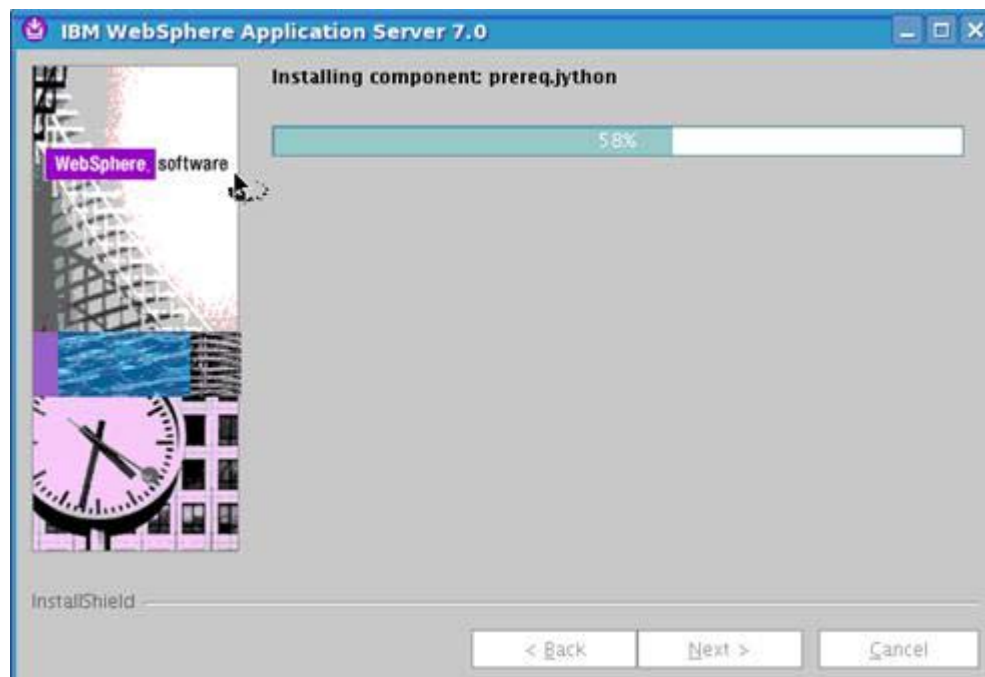


Figure 27. IBM WebSphere Application Server 7.0: Component installation in progress

___ 11. After some time the installation finishes. Click **Finish** to exit the installer.

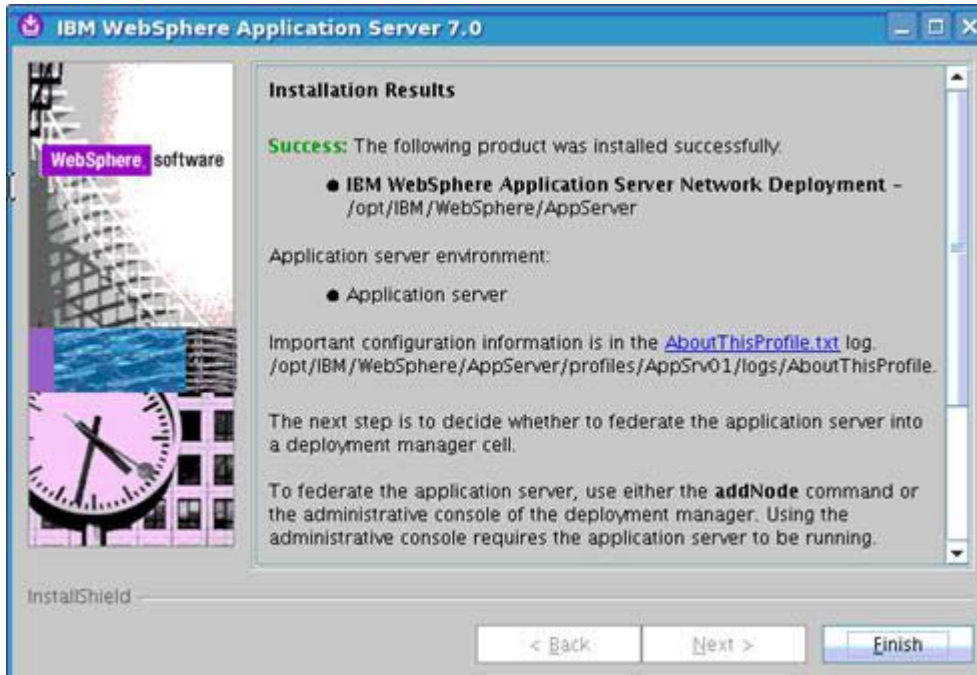


Figure 28. IBM WebSphere Application Server 7.0: Installation Results

12. In the WebSphere Application Server, click **Installation Verification**.

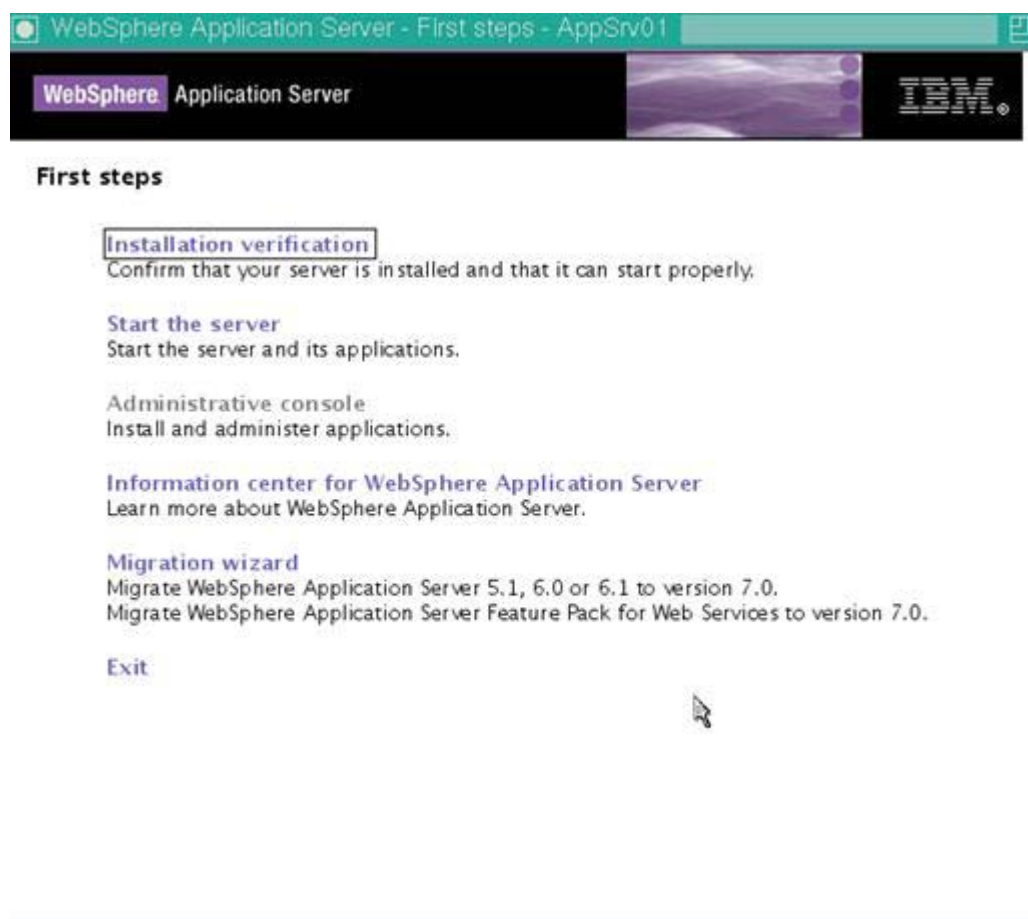


Figure 29. WebSphere Application Server: First steps

The installation verification tool succeeded, as shown in the following figure.

```

First steps output - Installation verification
Server name is: server1
Profile name is: AppSrv01
Profile home is: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01
Profile type is: default
Cell name is: "node1 Node01Cell"
Node name is: "node1 .Node01"
Current encoding is: UTF-8
Start running the following command: /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin/startServer.sh server1 -profileName AppSrv01
>ADMU0116: Tool information is being logged in file
> /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/server1/startServer.log
>ADMU0128: Starting tool with the AppSrv01 profile
>ADMU3100: Reading configuration for server: server1
>ADMU3200: Server launched, waiting for initialization status.
>ADMU3000: Server server1 open for e-business; process id is 10453
Server port number is: 9080
IVTL0010: Connecting to the node1.machine.com --- WebSphere Application Server on port: 9080
IVTL0015: WebSphere Application Server node1.machine.com is running on port: 9080 for profile AppSrv01
Testing server using the following URL: http://node1.machine.com:9080/iv/ivserver?parm2=ivserver
IVTL0050: Servlet engine verification status: Passed
Testing server using the following URL: http://node1.machine.com:9080/iv/ivserver?parm2=ivAddition.jsp
IVTL0055: JavaServer Pages files verification status: Passed
Testing server using the following URL: http://node1.machine.com:9080/iv/ivserver?parm2=ivEjb
IVTL0060: Enterprise bean verification status: Passed
  
```

Figure 30. First steps output: Installation verification

3. Set up IBM HTTP Server v7.0 and plug-ins

1. Copy the installation files to your `dm\IBM HTTP Server.machine.com` and start the IBM HTTP Server installation from the WebSphere Application Server 7.0 Supplement CD Package. The IBM HTTP Server 7.0 installation wizard opens. Click **Next** to continue.

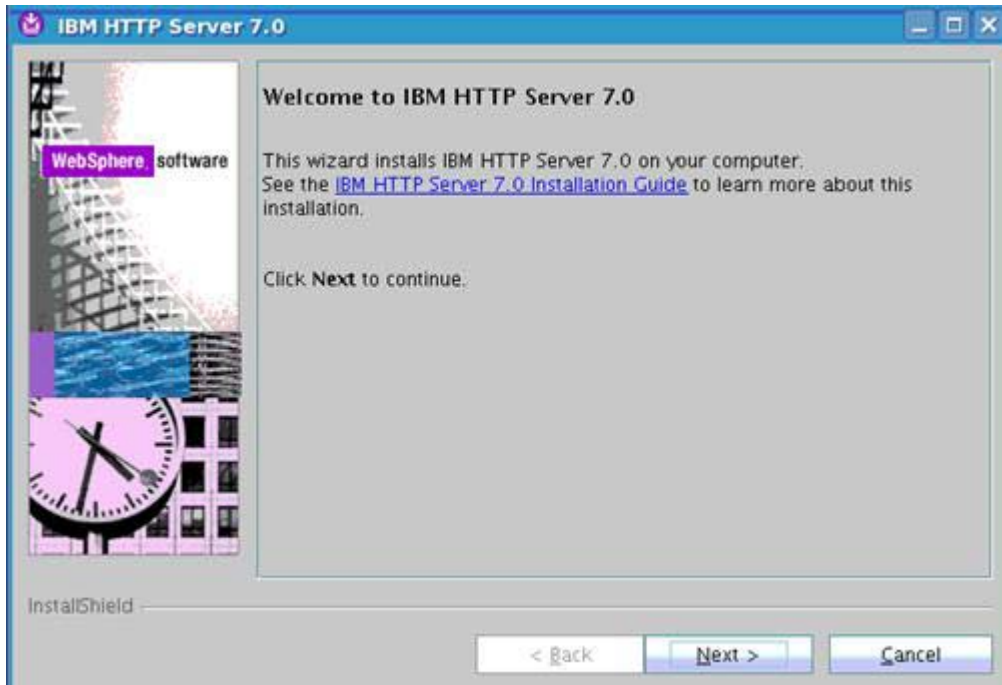


Figure 31. IBM HTTP Server 7.0: Welcome

- ___ 2. Accept the license agreement and click **Next**.

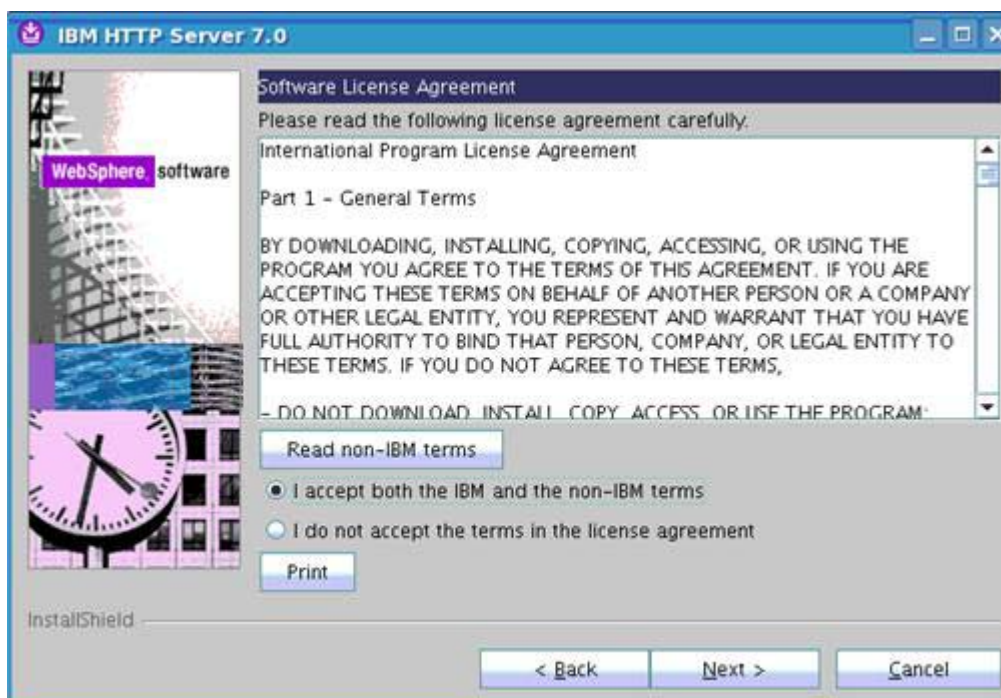


Figure 32. IBM HTTP Server 7.0: Software License Agreement

- ___ 3. In the System Prerequisites Check panel, click **Next** to continue.

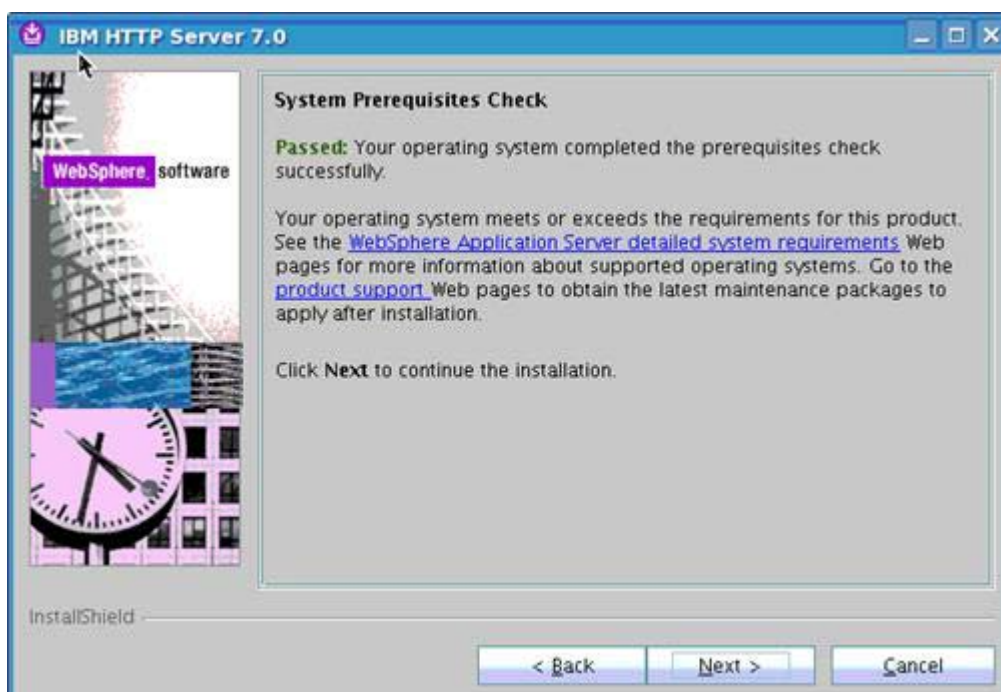


Figure 33. IBM HTTP Server 7.0: System Prerequisites Check

___ 4. Change the default installation path if needed and click **Next** to continue.

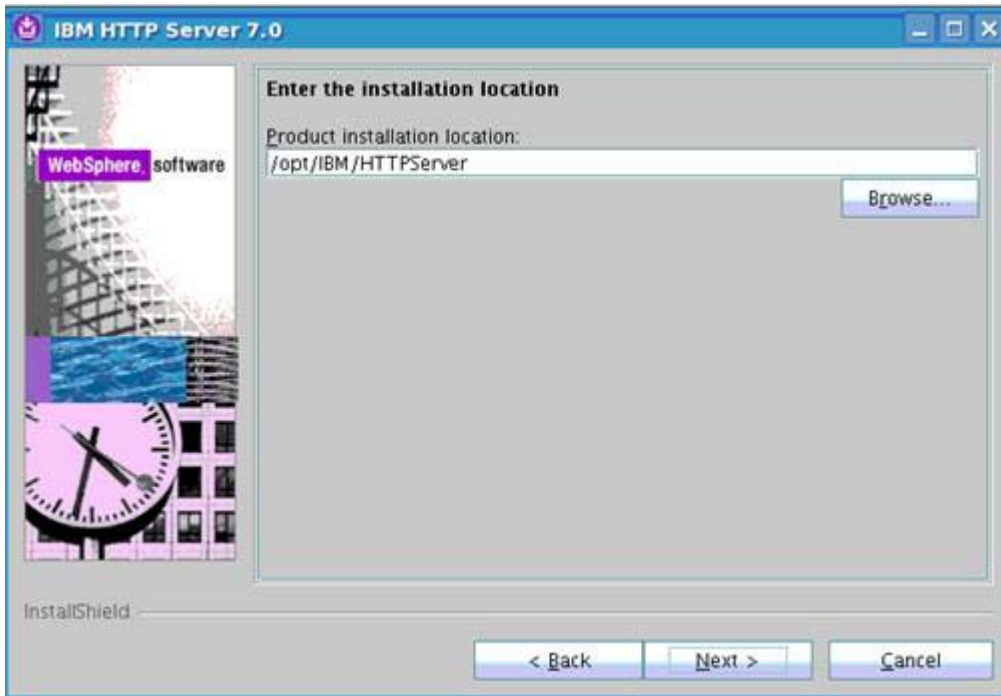


Figure 34. IBM HTTP Server 7.0: Enter the installation location

___ 5. The default port values should be fine. Click **Next** to continue.

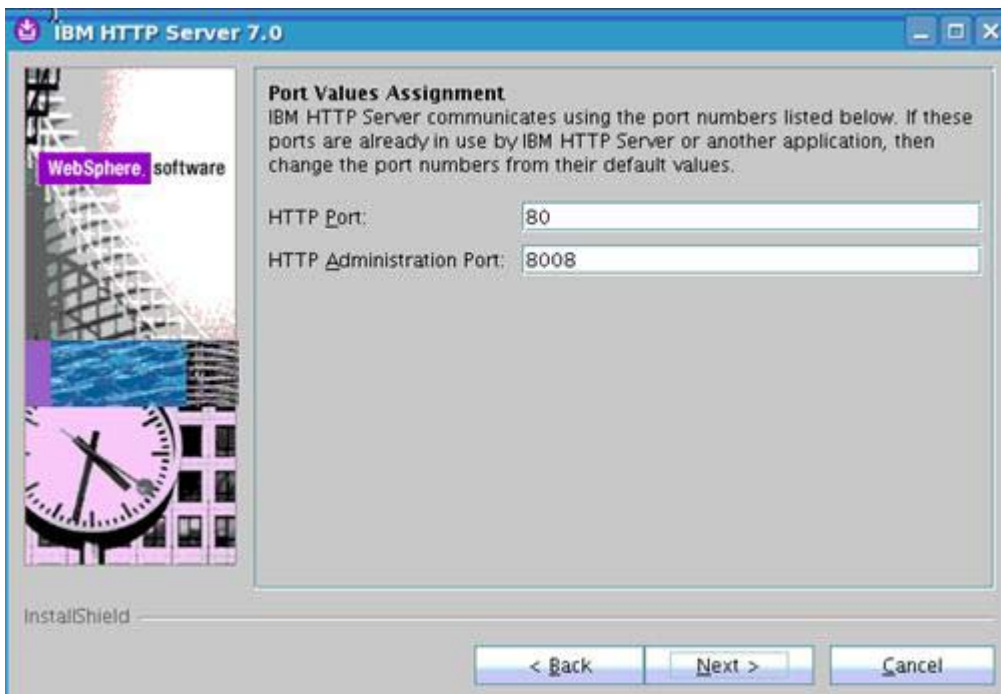


Figure 35. IBM HTTP Server 7.0: Port Values Assignment

- ___ 6. Specify and admin user (for example, IBM HTTP Serveradmin) and password and click **Next** to continue.

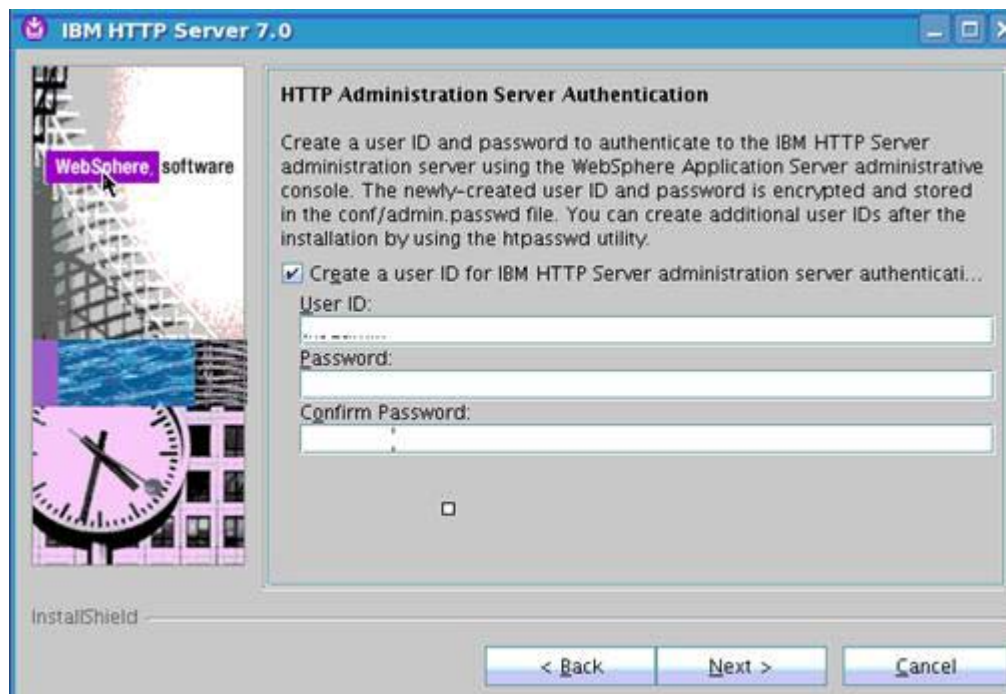


Figure 36. IBM HTTP Server 7.0: HTTP Administration Server Authentication

- ___ 7. For the administration server, enter a user ID and a group (for example, IBM HTTP Serveradmin for the user ID and IBM HTTP Serveradmins for the group). Click **Next** to continue.

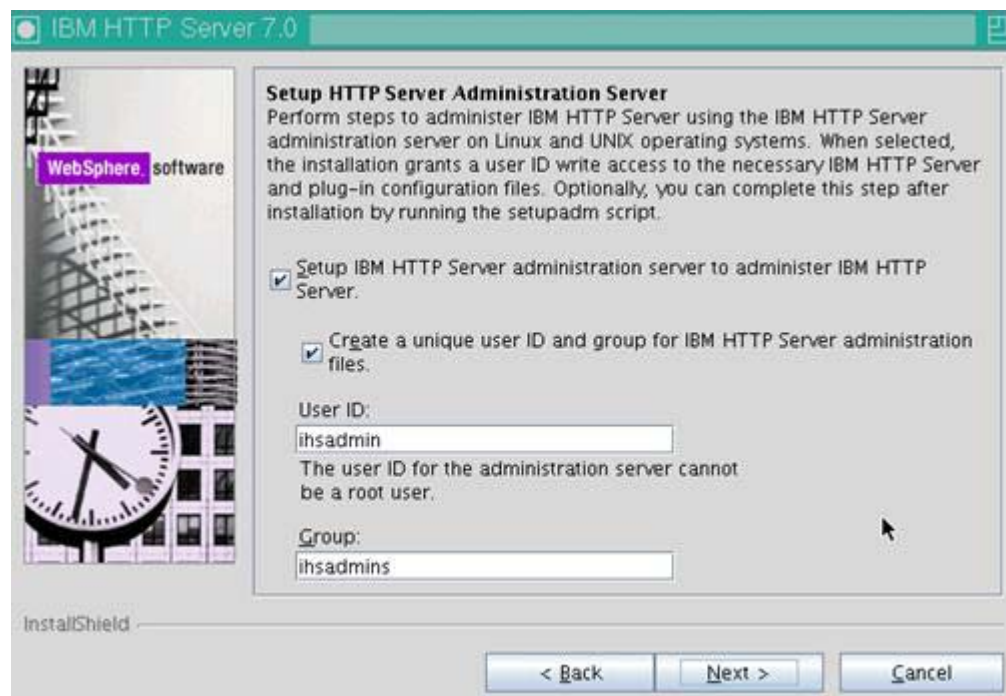


Figure 37. IBM HTTP Server 7.0: Setup HTTP Server Administration Server

8. Select Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server. Provide the web server definition and host name information, and click **Next** to continue.

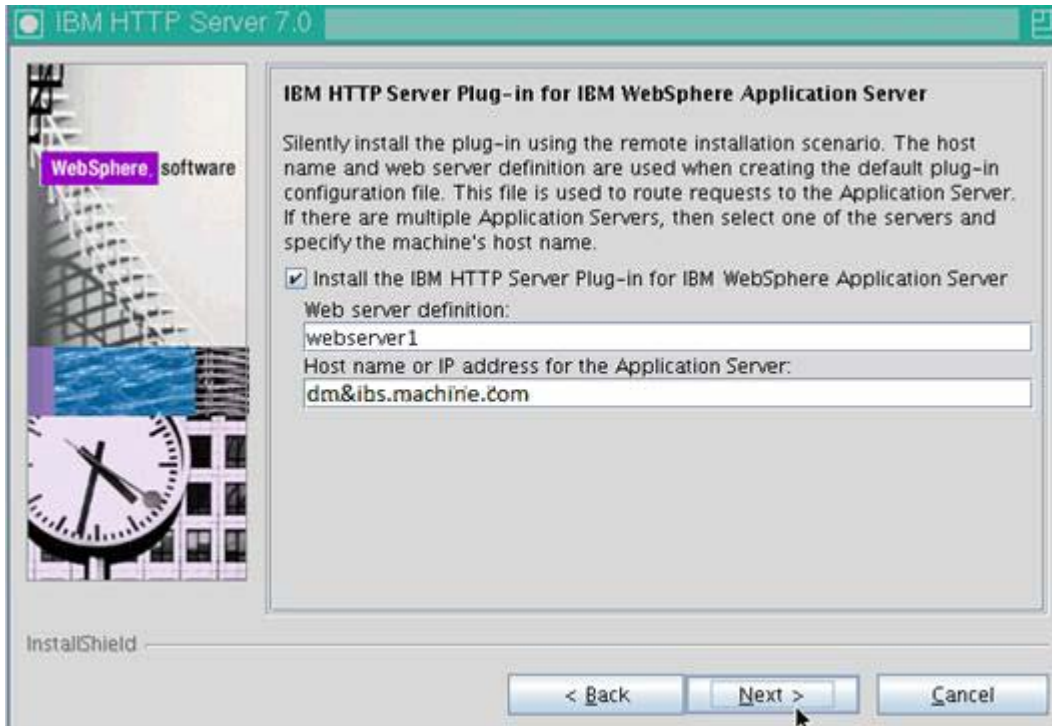


Figure 38. IBM HTTP Server 7.0: IBM HTTP plug-in for IBM WebSphere Application Server

9. In the Installation summary panel, click **Next** to start the installation of the files.

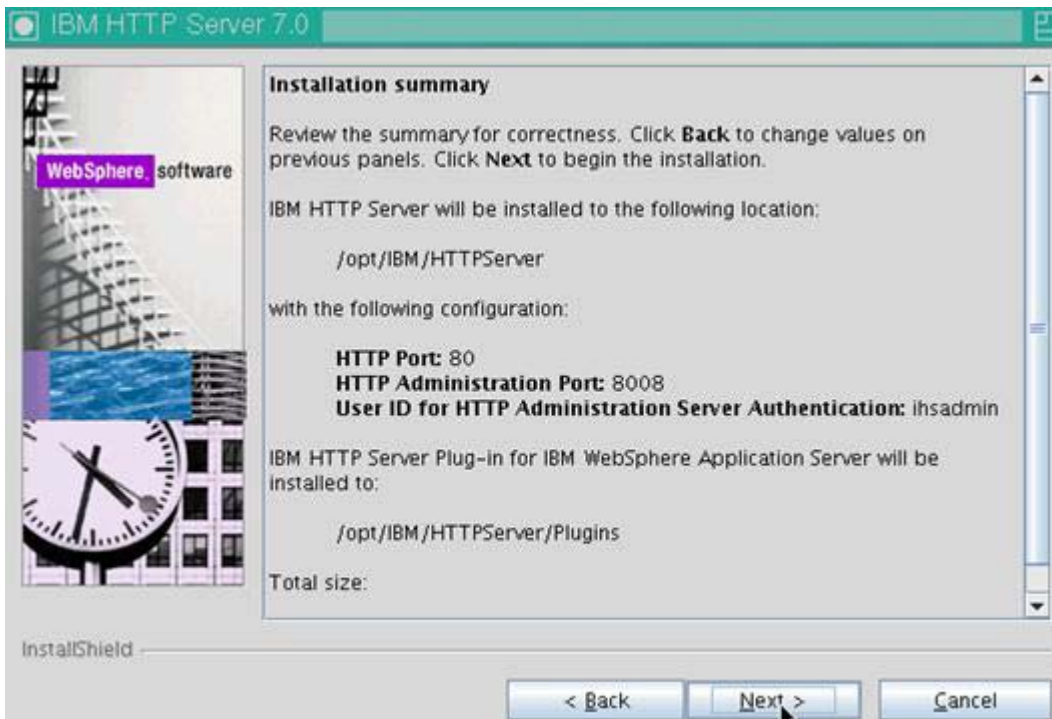


Figure 39. IBM HTTP Server 7.0: Installation summary

___ 10. After some time the installation completes. Click **Finish** to exit the wizard.

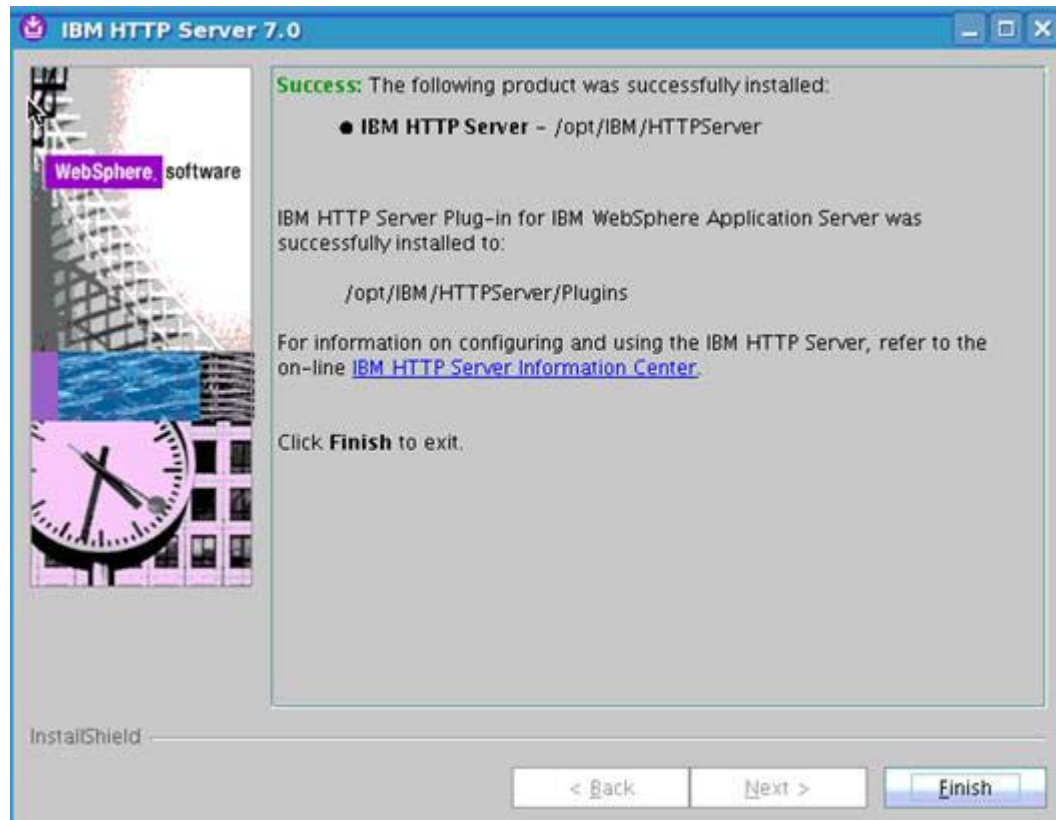


Figure 40. IBM HTTP Server 7.0: Installation complete

- ___ 11. IBM HTTP Server 7.0 is now installed. To start it, go to `/opt/IBM/HTTPServer/bin` and run `./apachectl start`. You can also start the admin by running `./adminctl start`. Then, go to `http://dm&IBM HTTP Server.machine.com`. The following page is displayed.

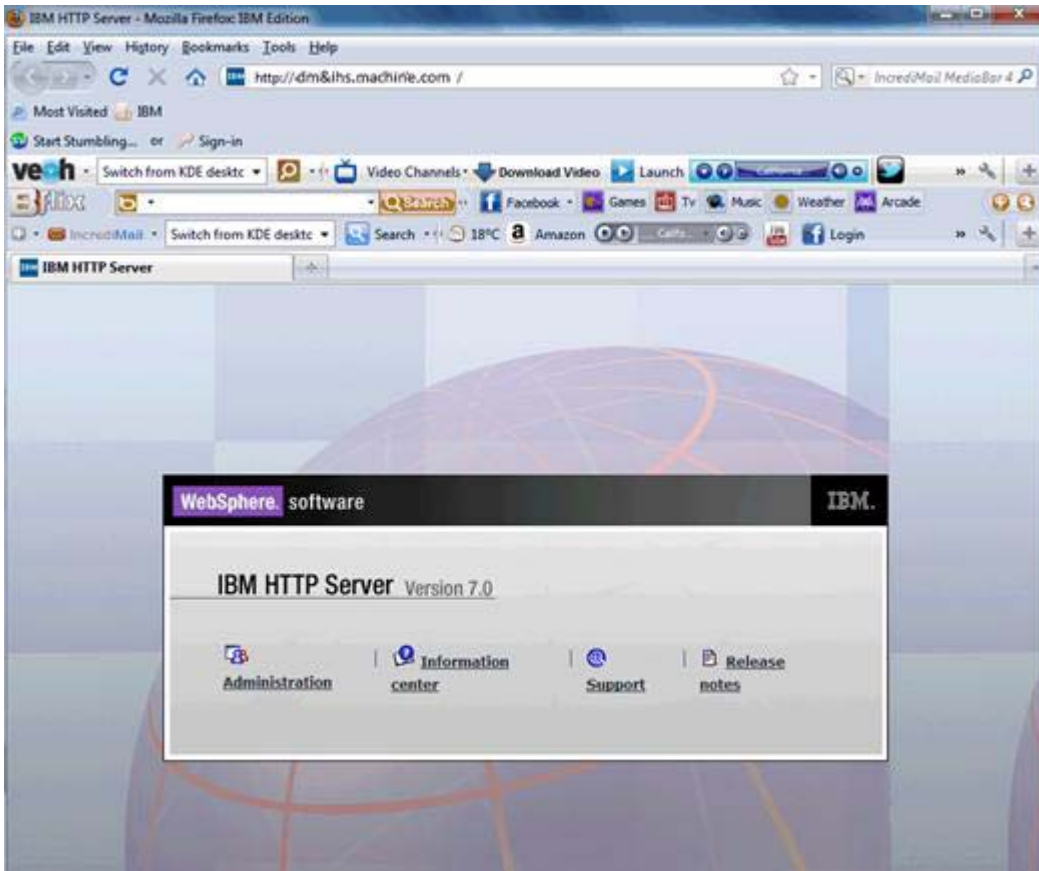


Figure 41. IBM HTTP Server Version 7.0

4. Install WebSphere Application Server 7.0 Update Installer

1. Copy the `7.0.0.9-WS-UPDI-LinuxAMD64.tar.gz` to your computers and uncompress the installation. Go into `UpdateInstaller` and run `install`. The installation wizard opens. Click **Next** to continue.

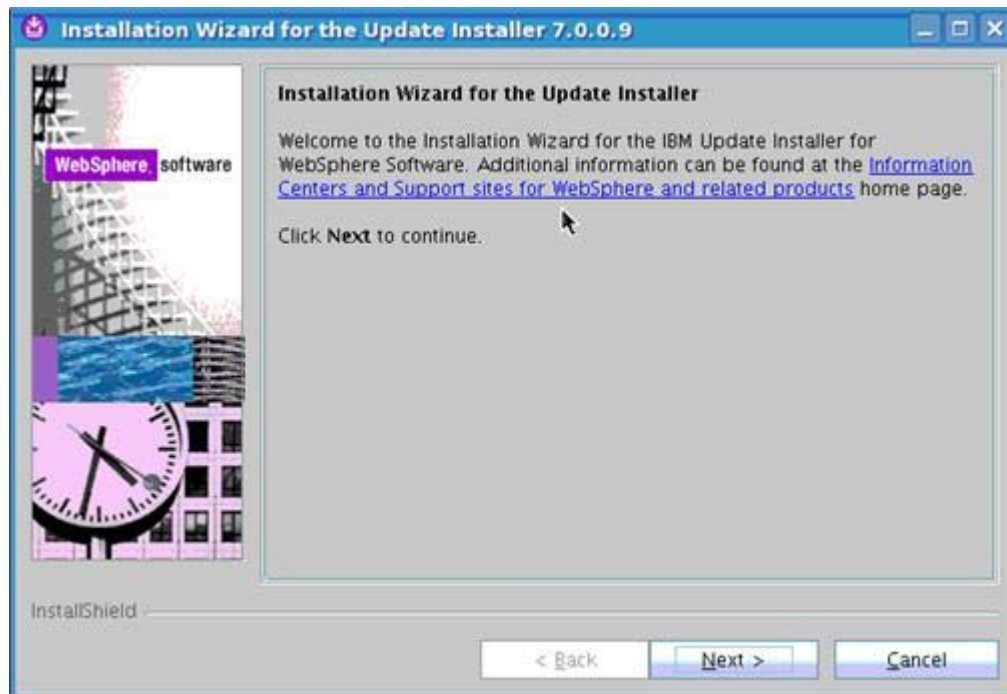


Figure 42. Installation wizard for the Update Installer 7.0.0.9: Welcome

___ 2. Accept the license agreement and click **Next** to continue.

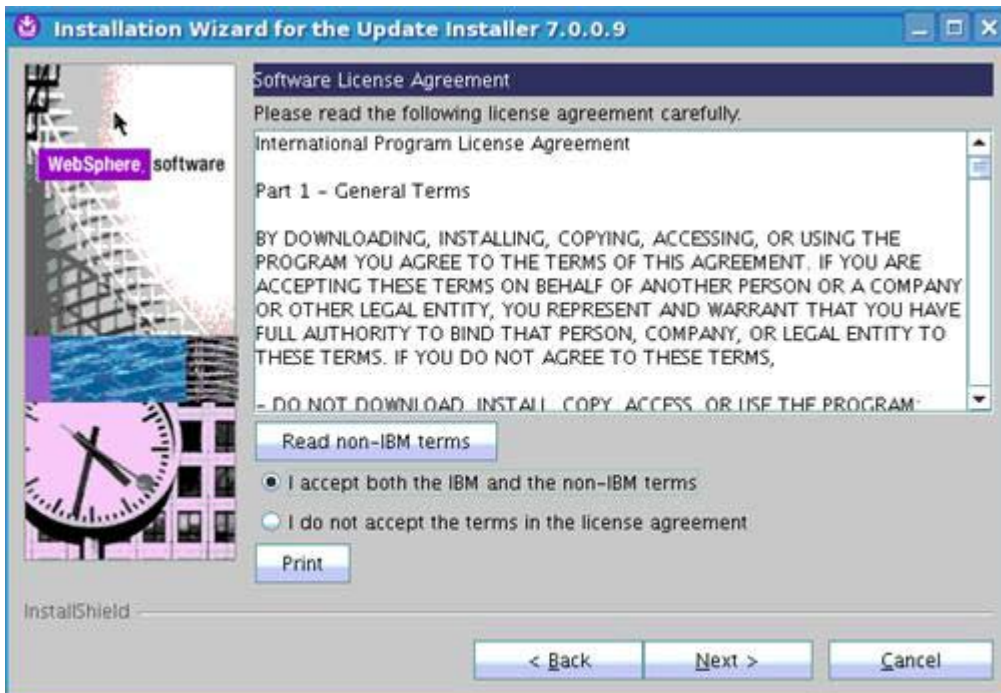


Figure 43. Installation wizard for the Update Installer 7.0.0.9: Software License Agreement

___ 3. In the System Prerequisites Check panel, click **Next** to continue.

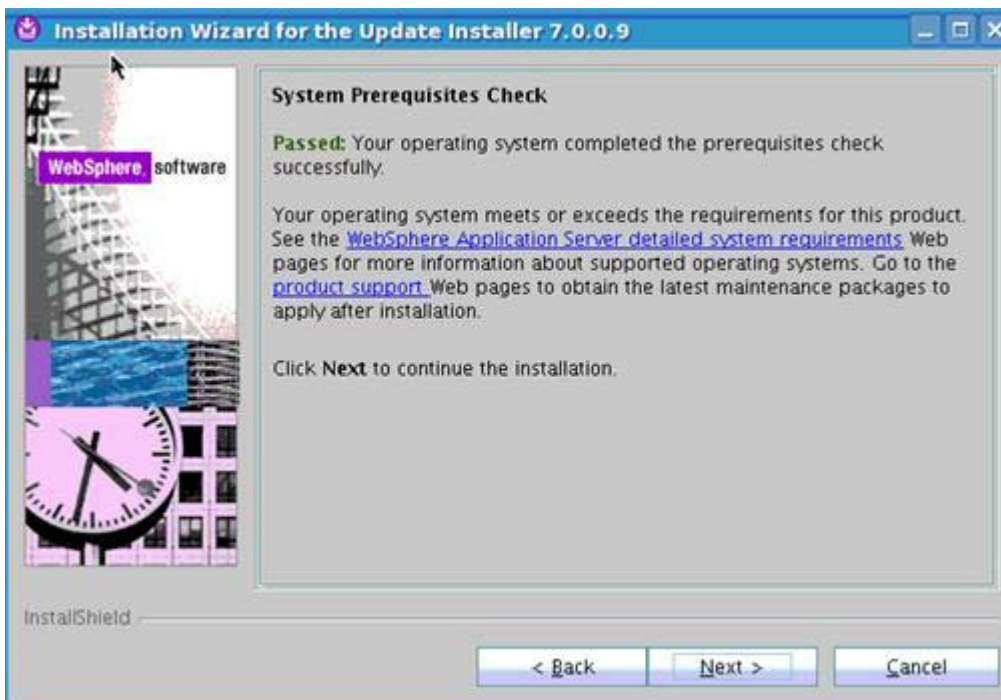


Figure 44. Installation wizard for the Update Installer 7.0.0.9: System Prerequisites Check

- ___ 4. Change the installation path location if needed and click **Next** to continue.

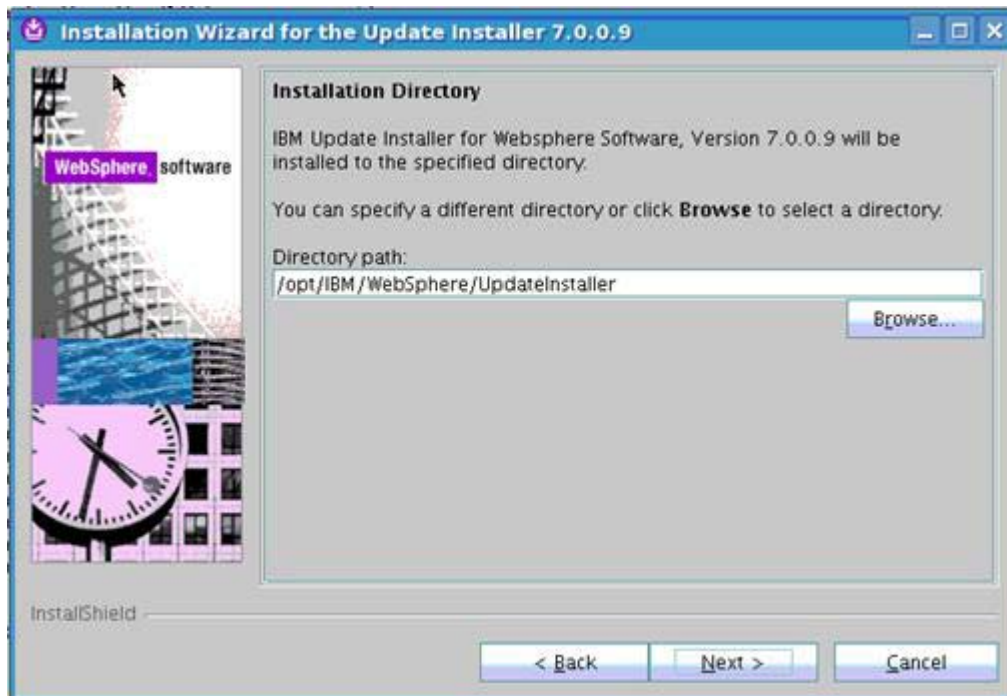


Figure 45. Installation wizard for the Update Installer 7.0.0.9: Installation Directory

- ___ 5. Check the installation summary and click **Next** to continue.

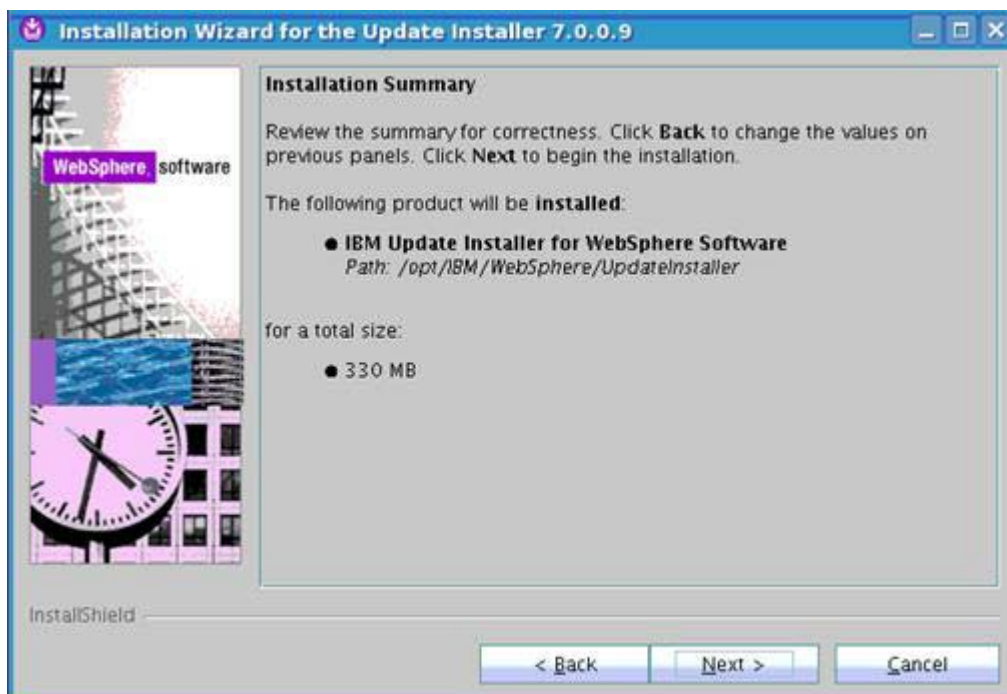


Figure 46. Installation wizard for the Update Installer 7.0.0.9: Installation Summary

The installation of the files starts.

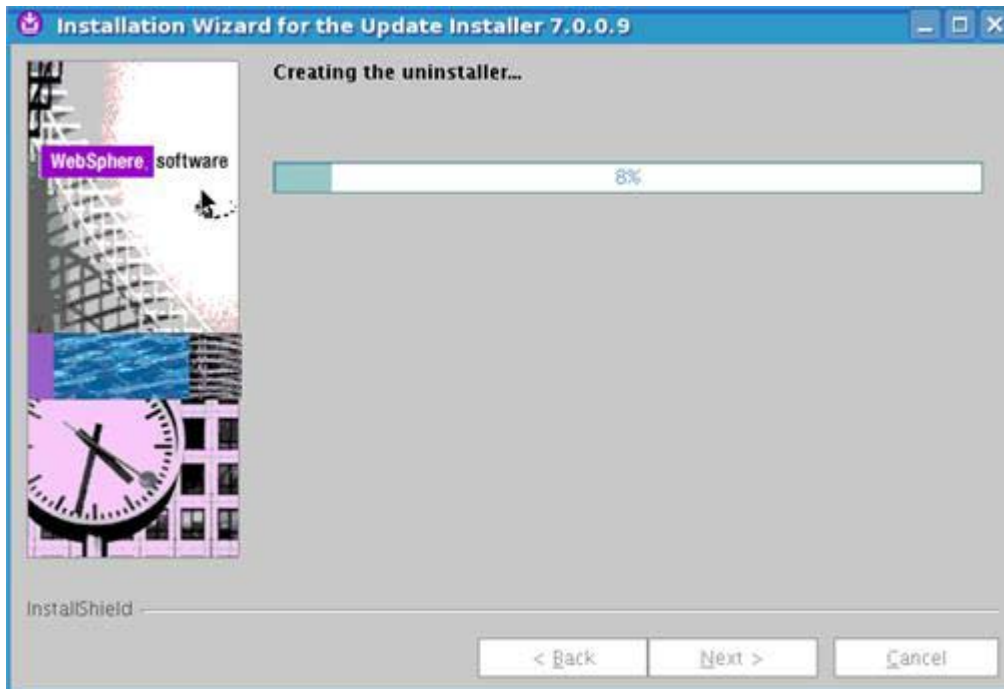


Figure 47. Installation wizard for the Update Installer 7.0.0.9: Installation in progress

- 6. After some time it completes. Click **Finish** to exit the installer. WebSphere Application Server Update Installer is now successfully installed. .

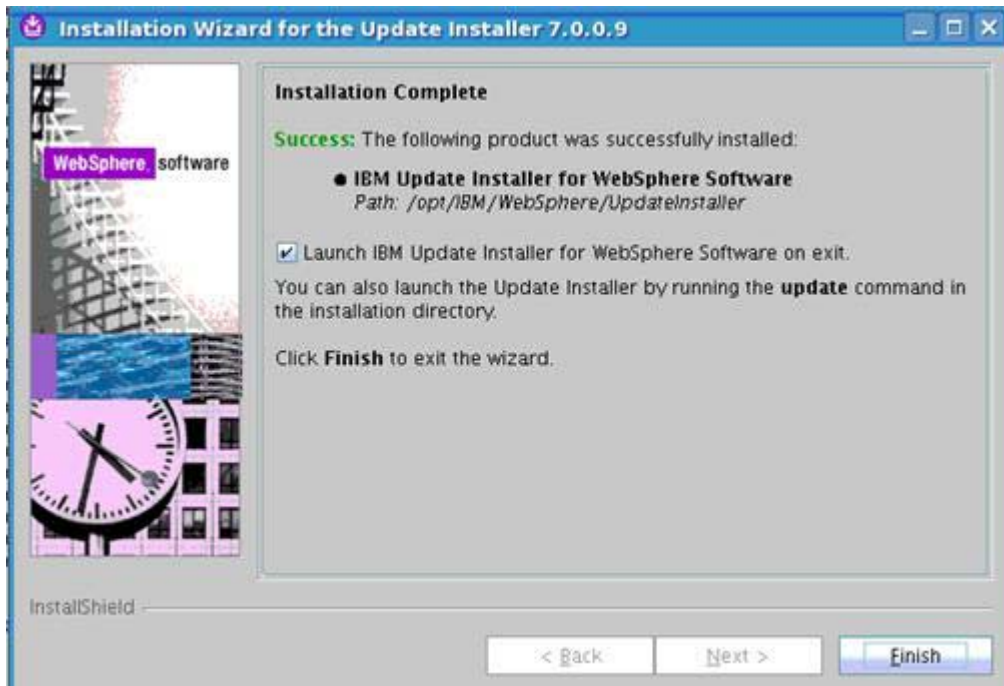


Figure 48. Installation wizard for the Update Installer 7.0.0.9: Installation Complete

5. Update Deployment Manager, Application Server, IBM HTTP Server, IBM HTTP Server plug-ins, and SDKs to WebSphere Application Server 7.0.0.21 FixPack

- ___ 1. Copy 7.0.0-WS-WAS-LinuxX64-FP0000021.pak, 7.0.0-WS-WASSDK-LinuxX64-FP0000021.pak, 7.0.0-WS-PLG-LinuxX64-FP0000021.pak, and 7.0.0-WS-IBM HTTP Server-LinuxX64-FP0000021.pak to some location on your Deployment Manager, Application Server, and IBM HTTP Server server.
- ___ 2. Stop your Deployment Manager, NodeAgent, Application Server, and IBM HTTP Server Servers.
- ___ 3. Start the WebSphere Application Server Update Installer by running `./update.sh` from under `/opt/IBM/WebSphere/UpdateInstaller/`. In the following installation wizard, click **Next** to continue.

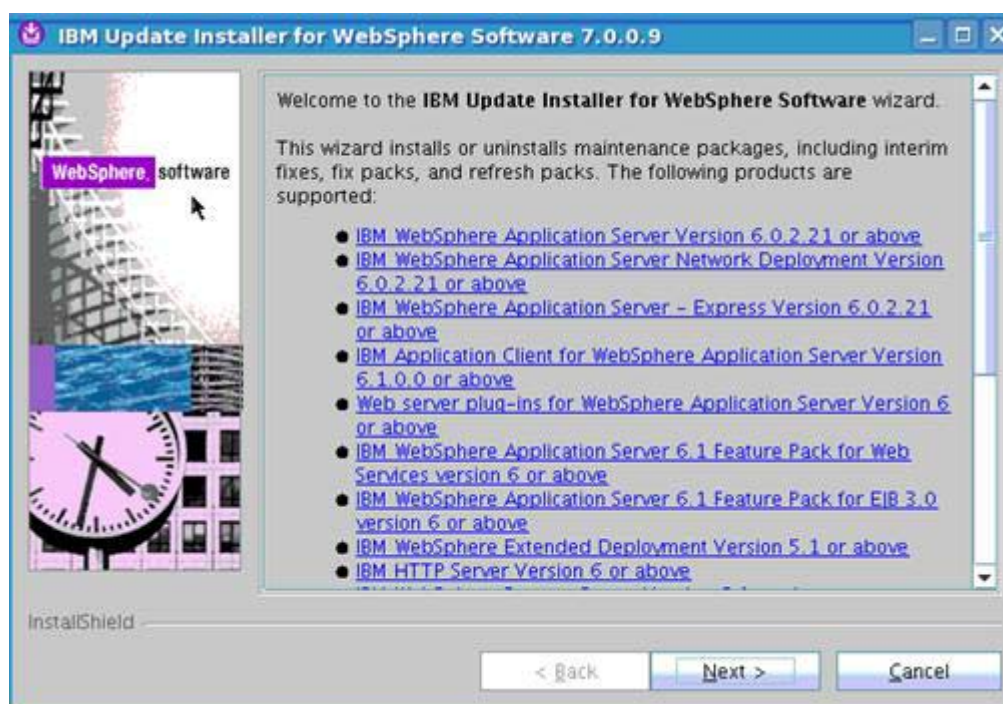


Figure 49. IBM Update Installer for WebSphere Software 7.0.0.9: Welcome

___ 4. Browse to the path of your Deployment Manager and select **Next**.

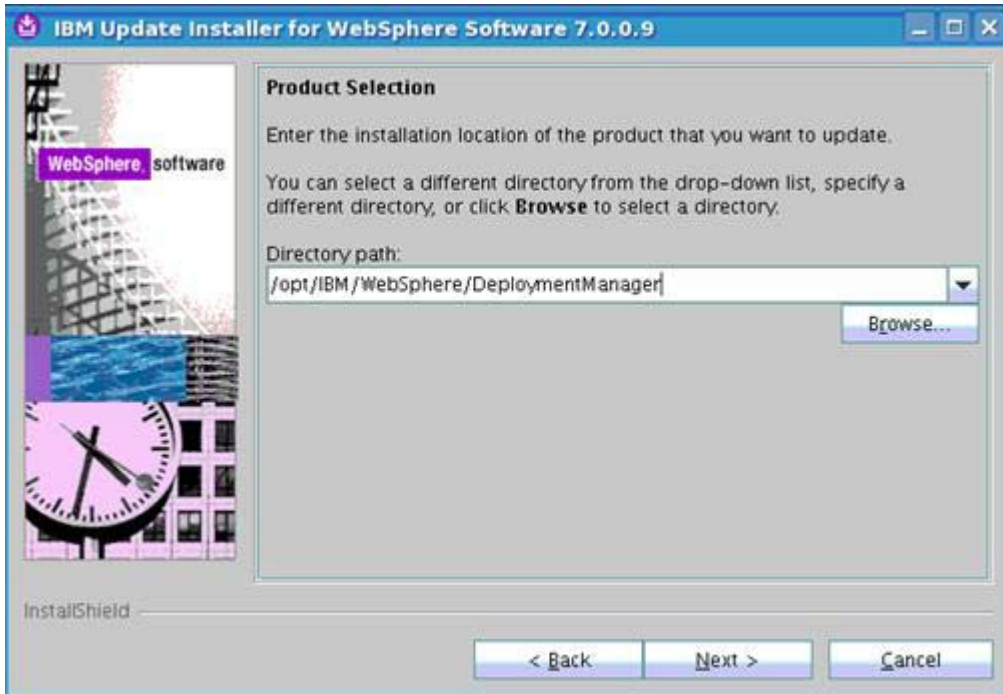


Figure 50. IBM Update Installer for WebSphere Software 7.0.0.9: Product Selection

___ 5. Select Install maintenance package and click **Next** to continue.

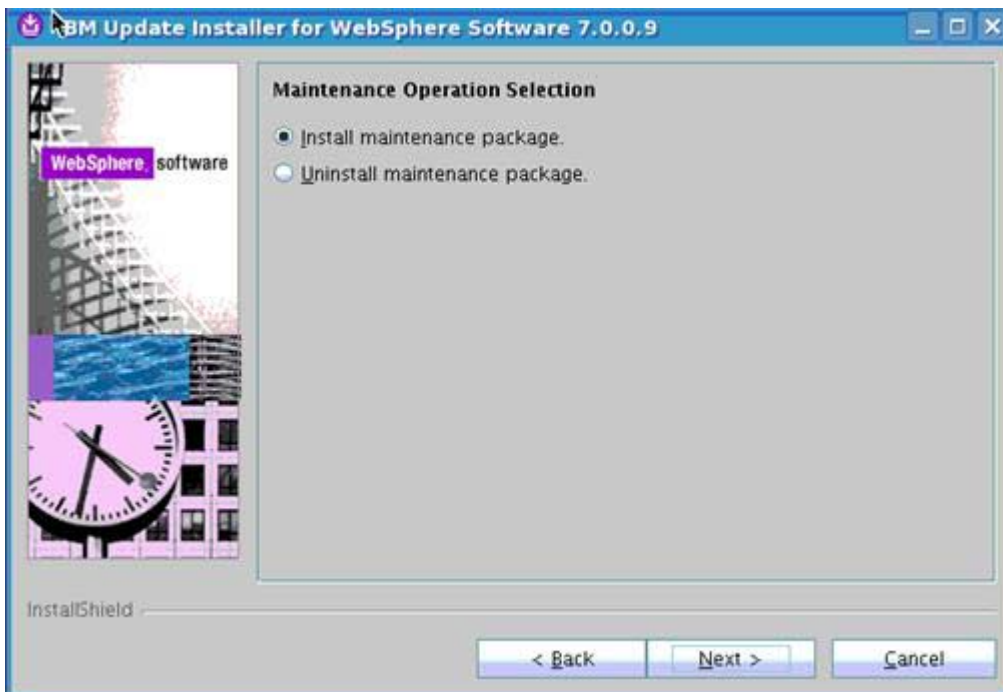


Figure 51. IBM Update Installer for WebSphere Software 7.0.0.9: Maintenance Operation Selection

- ___ 6. Browse to the path of your fix pack 21 files and click **Next** to continue.

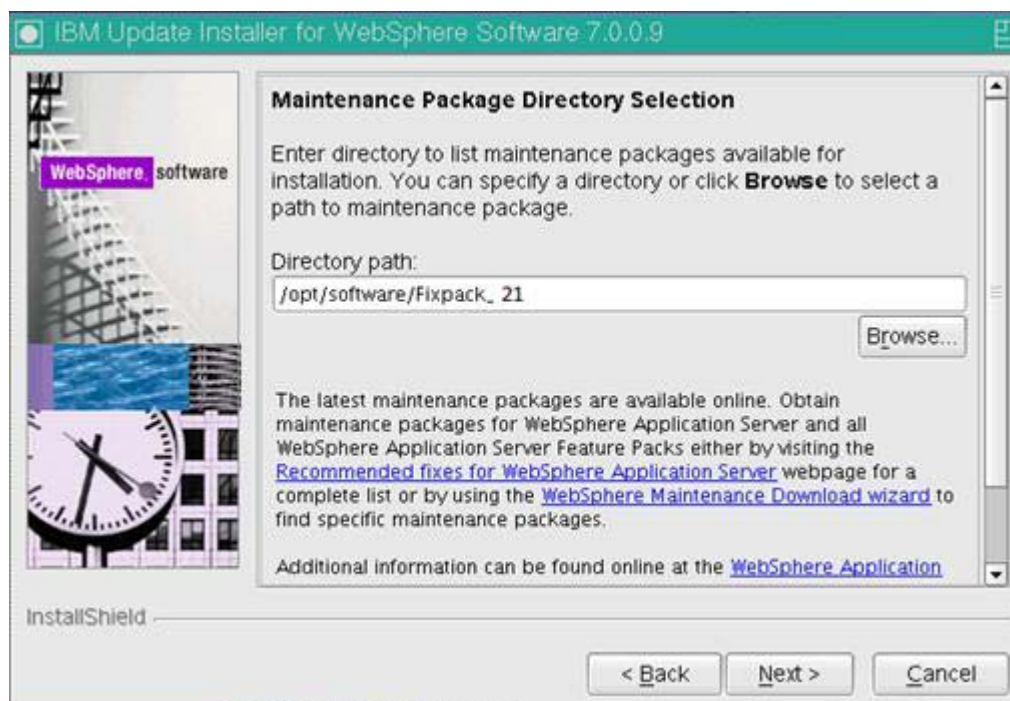


Figure 52. IBM Update Installer for WebSphere Software 7.0.0.9: Maintenance Package Directory Selection

- ___ 7. The installation selects the two packages that need to be installed. Click **Next** to continue.

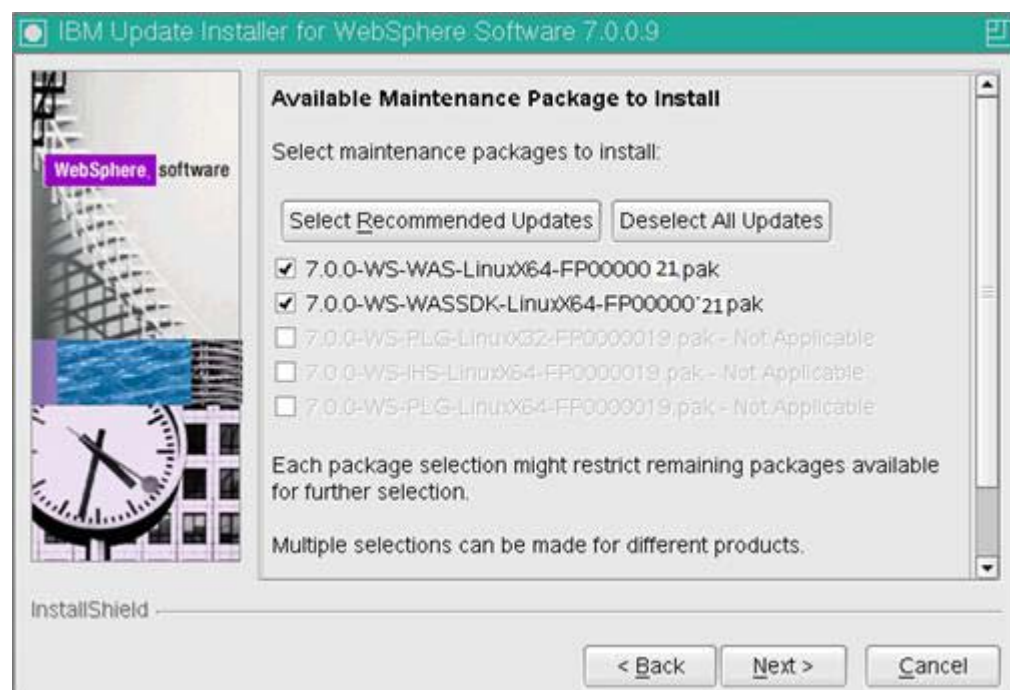


Figure 53. IBM Update Installer for WebSphere Software 7.0.0.9: Available Maintenance Package to install

8. Select Verify my Permissions to perform the installation”and then click **Next** to continue.

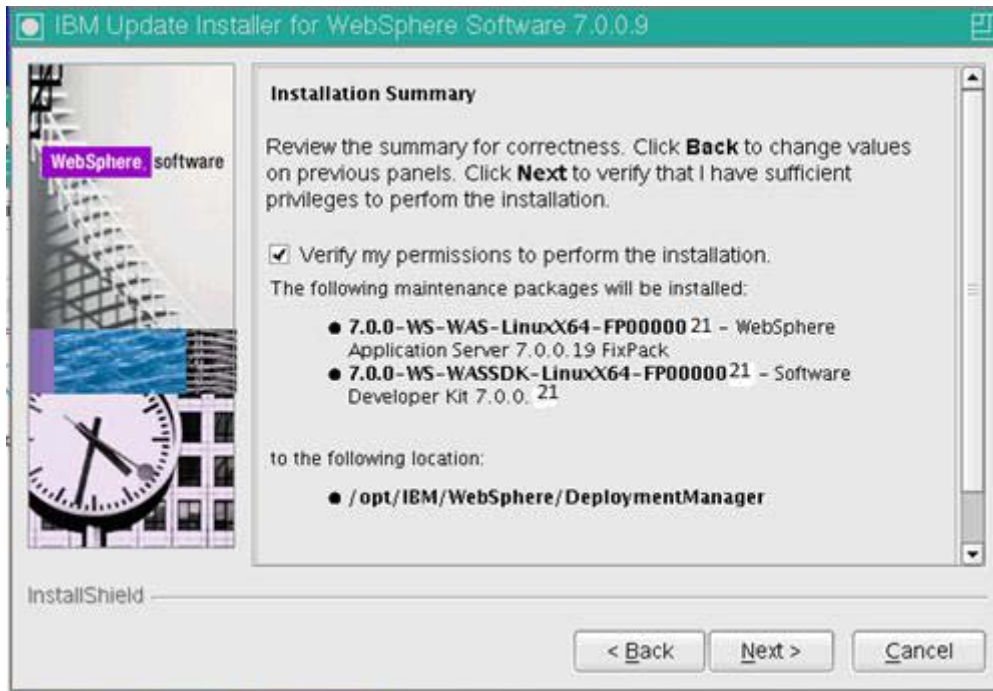


Figure 54. IBM Update Installer for WebSphere Software 7.0.0.9: Installation Summary

9. The verification of permissions starts. Click **Next** when it finishes.

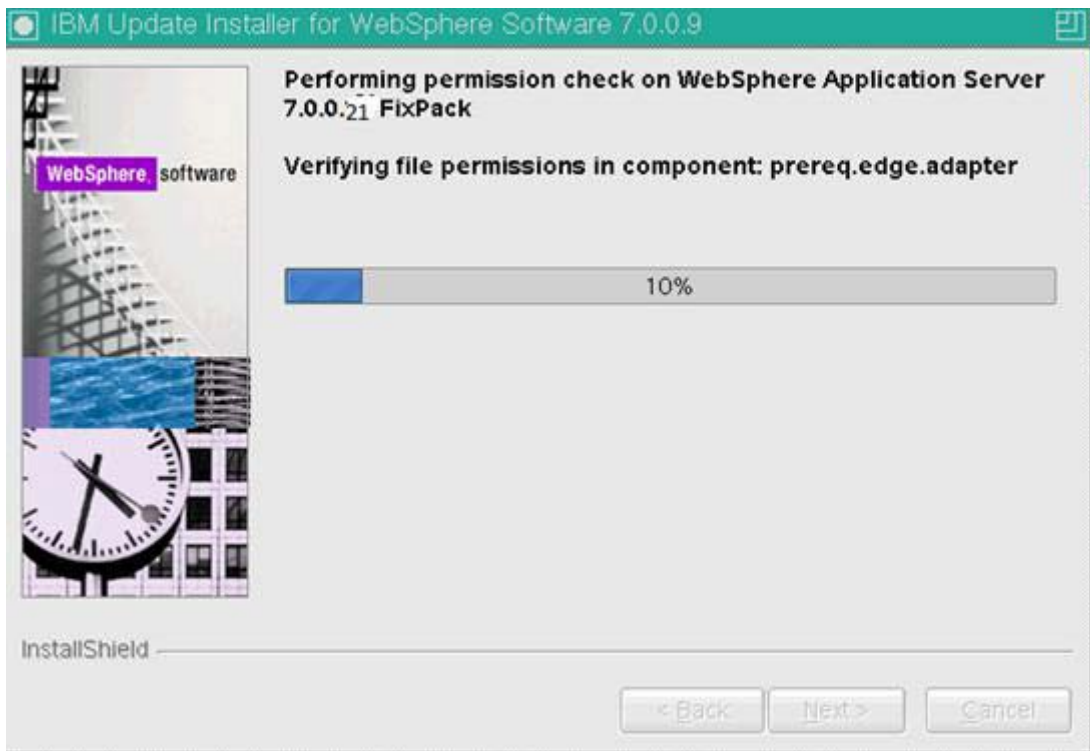


Figure 55. IBM Update Installer for WebSphere Software 7.0.0.9: Verification in progress

10. Review the installation summary and click **Next** to begin the installation.

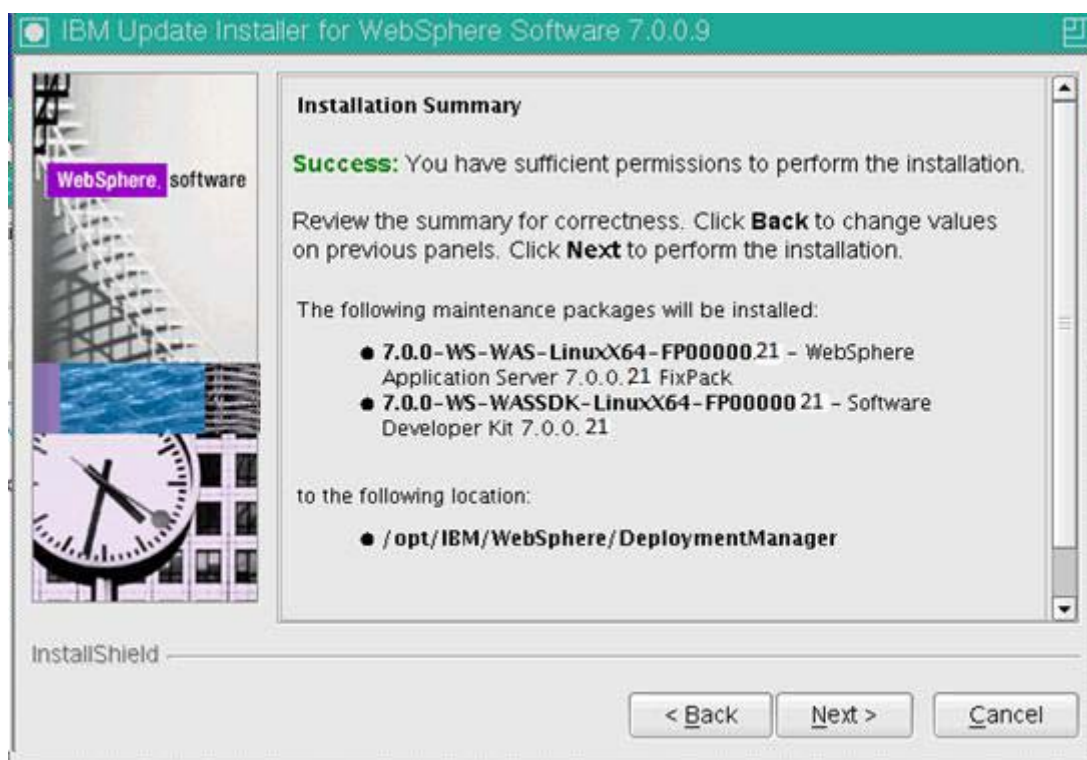


Figure 56. IBM Update Installer for WebSphere Software 7.0.0.9: Installation Summary

The installation begins.

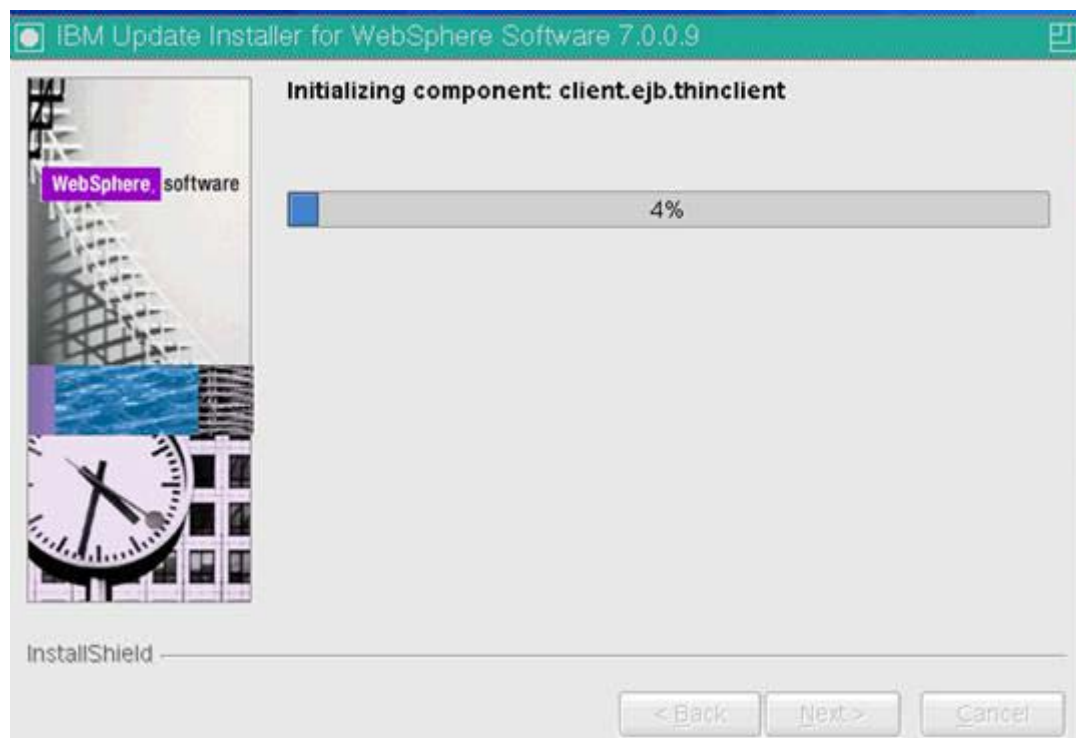


Figure 57. IBM Update Installer for WebSphere Software 7.0.0.9: Installation in progress

11. When the installation completes, click **Finish** to exit the wizard.

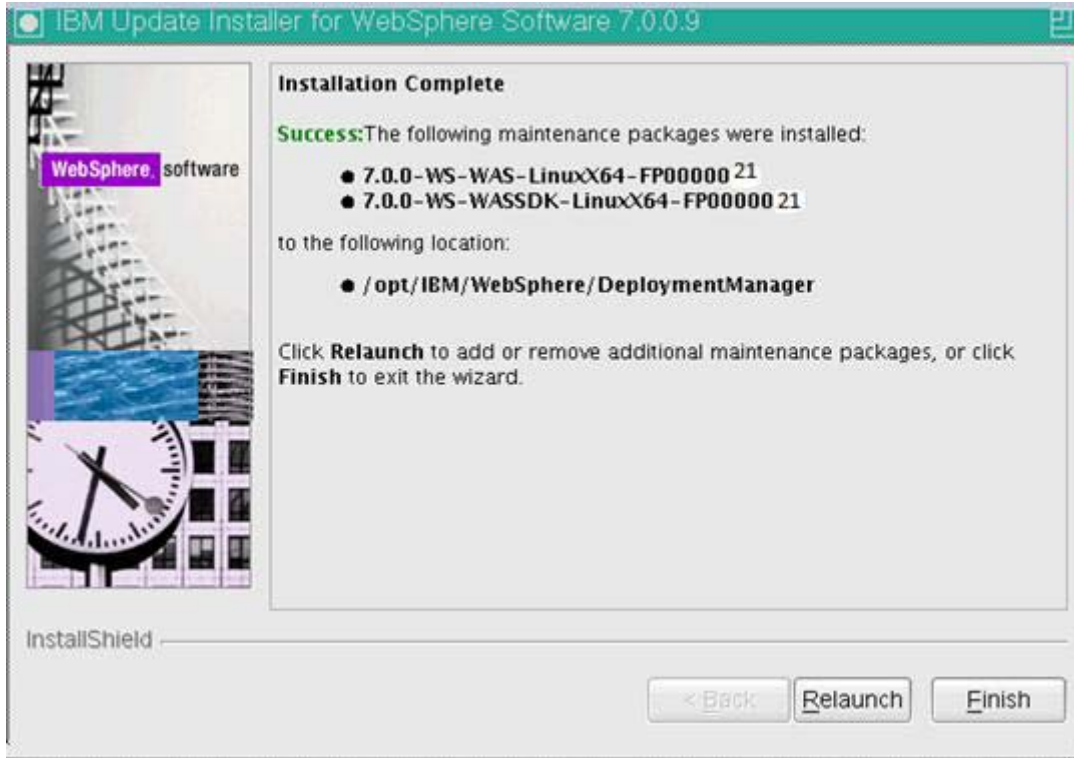


Figure 58. IBM Update Installer for WebSphere Software 7.0.0.9: Installation Complete



Note

The installation is now completed. All you need to do is to follow the same steps, specifying the location of each installed service.

6. Federate Application Server into Deployment Manager

Next, you federate the Application Server into the Deployment Manager. Follow these steps:

- ___ 1. Ensure that the clocks are in synch between your Deployment Manager and Application Server.
- ___ 2. Make sure that the Deployment Manager is started and the Application Server is stopped.
- ___ 3. Then, from both the Nodes within your `/opt/IBM/WebSphere/AppServer/bin`, run the following command:

```
./addNode.sh dm&IBM HTTP Server.machine.com 8879 -user wasadmin -password
example
```

If all goes well, you should see something like the following result:

```

[Root@node1 ~]# /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./addNode.sh dm&IBM HTTP Server.machine.com 8879 -user wasadmin -password
ADMN00116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/addNode.log
ADMN00128I: Starting tool with the AppSrv01 profile
CWFK10309I: All signers from remote keystore already exist in local keystore.
ADMN00001I: Begin federation of node dslvml008Node01 with Deployment Manager at
dslvml008Node01.msi.ie.ibm.com:8879.
ADMN00009I: Successfully connected to Deployment Manager Server:
dslvml008Node01.msi.ie.ibm.com:8879
ADMN00095I: Servers found in configuration:
ADMN00064I: Server name: server1
ADMN00101I: Stopping all server processes for node dslvml008Node01
ADMN00012I: Server server1 cannot be reached. It appears to be stopped.
ADMN00024I: Deleting the old backup directory.
ADMN00015I: Backing up the original cell repository.
ADMN00021I: Creating Node Agent configuration for node: dslvml008Node01
ADMN00014I: Adding node dslvml008Node01 configuration to cell: dslvml008Cell01
ADMN00016I: Synchronizing configuration between node and cell.
ADMN00018I: Launching Node Agent process for node: dslvml008Node01
ADMN00020I: Reading configuration for Node Agent process: nodesagent
ADMN00022I: Node Agent launched. Waiting for initialization status.
ADMN00030I: Node Agent initialization completed successfully. Process id is:
2343

ADMN00001I: The node dslvml008Node01 was successfully added to the
dslvml008Cell01 cell.

ADMN00061I: Note:
ADMN00021I: Any cell-level documents from the standalone dslvml008Cell01
configuration have not been migrated to the new cell.
ADMN00077I: You might want to:
ADMN00030I: Update the configuration on the dslvml008Cell01 Deployment Manager
with values from the old cell-level documents.

ADMN00061I: Note:
ADMN00041I: Because -includesapps was not specified, applications installed on
the standalone node were not installed on the new cell.
ADMN00077I: You might want to:
ADMN00051I: Install applications onto the dslvml008Cell01 cell using wasadmin
&AdminApp or the Administrative Console.

ADMN00031I: Node dslvml008Node01 has been successfully federated.
[Root@node1 ~]# /opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin #

```

Figure 59. Command within `/opt/IBM/WebSphere/AppServer/bin`

4. When completed, if you log in to your Deployment Manager at <http://dm&IBM HTTP Server.machine.com:9060/admin> and go to **Servers > Server Types > WebSphere Application Servers**, you should see something like this:

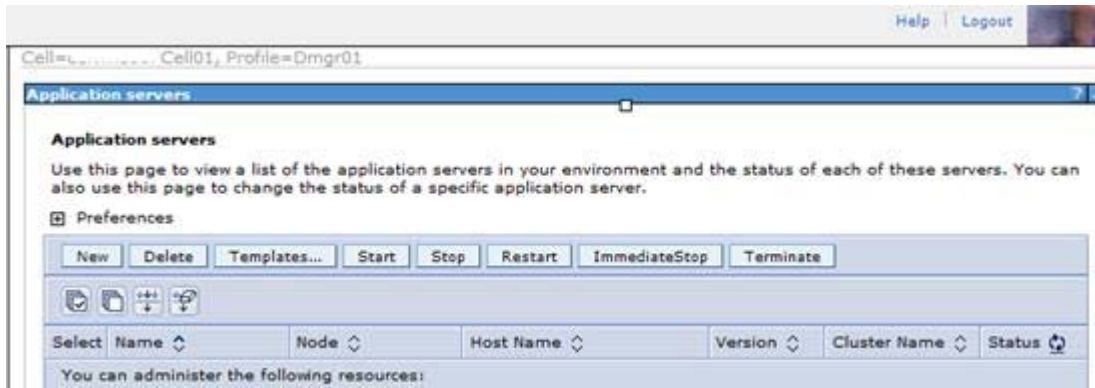


Figure 60. Application servers

<input type="checkbox"/>	server1	Node01	node1.machine.com	ND 7.0.0.21		
<input type="checkbox"/>	server1	Node01	,node2.machine.com	ND 7.0.0.21		
Total 8						

Figure 61. Application servers

7. Enable security on your Deployment Manager

Next, you add the LDAP repository to your configuration.

General settings

- ___ 1. Start WebSphere Application Server and log in to your admin console `http://dm&IBM HTTP Server.machine.com:9060/admin`.
- ___ 2. Select **Security > Global security**. Ensure that **Enable administrative security** and **Enable application security** are selected. Also, ensure that the user account is set to federated repositories.

Global security

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

Security Configuration Wizard Security Configuration Report

Admin **Launches a wizard to configure the basic security settings.**

Enable administrative security

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

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources

Warn if applications are granted custom permissions

Restrict access to resource authentication data

User account repository

Current realm definition
Federated repositories

Available realm definitions
Federated repositories Configure... Set as current

Apply Reset

Authentication

Authentication mechanisms and expiration

LTPA

Kerberos and LTPA

[Kerberos configuration](#)

[Authentication cache settings](#)

Web and SIP security

RMI/IIOP security

Java Authentication and Authorization Service

Use realm-qualified user names

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

Figure 62. Global security

- ___ 3. Select **Apply** and **Save**.

- 4. In **Security > Global security > Web and SIP Security > General Settings**, ensure that Use available authentication data is selected.



Figure 63. Web authentication behavior

- 5. Select **Apply** and **Save**.
- 6. In **Security > Global security > Web and SIP Security > Single sign-on (SSO)**, ensure that the **Interoperability Mode** is selected and enter the domain name.



Figure 64. Global security > Single sign-on (SSO): Interoperability Mode

- 7. Click **Apply** and **Save**.

8. Federate LDAP repositories

- ___ 1. Log in to your admin console `http://dm&IBM HTTP Server.machine.com:9060/admin`.
- ___ 2. Go to **Security > Global security > Configure...** for Federated Repositories.



Figure 65. User account repository

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



Figure 66. Repositories in the realm

- ___ 4. Then, click **Add Repository...**



Figure 67. Adding repository

- ___ 5. Enter the repository identifier, primary host name, bind distinguished name, bind password, login properties, login properties...

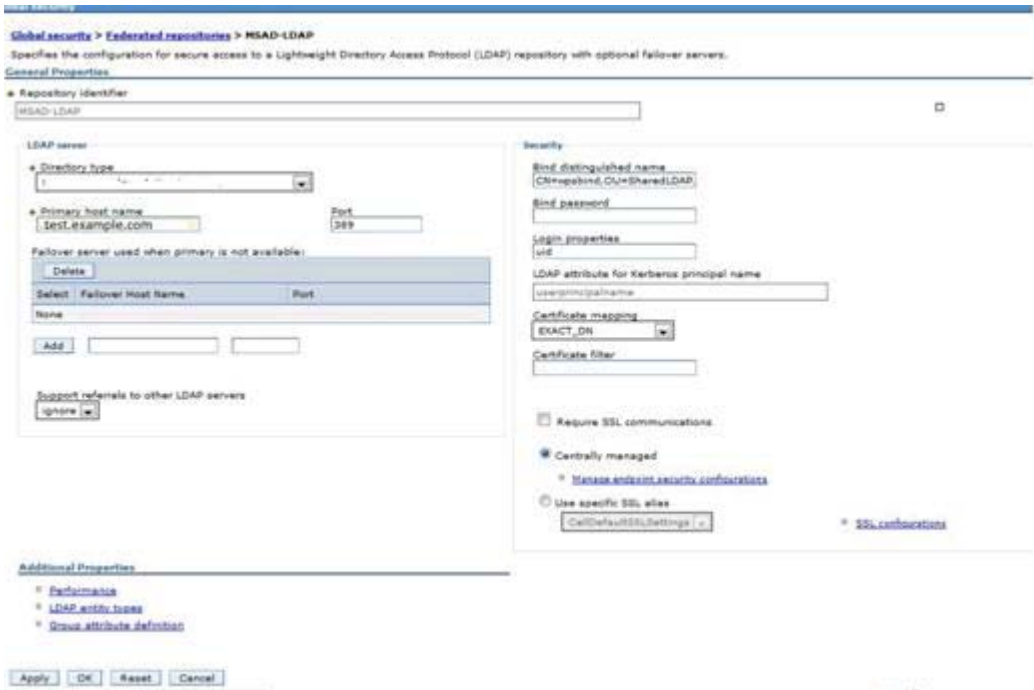


Figure 68. Repository general properties

- ___ 6. Click **OK**. When prompted, enter the base entry.



Figure 69. Entering the base entry

- ___ 7. Click **Apply**, **OK**, and **Save**.
- ___ 8. Restart your Deployment Manager and Node Agents.

**Note**

Log in to the Deployment Manager Console as and make sure that both the Node agents were in sync with each other.

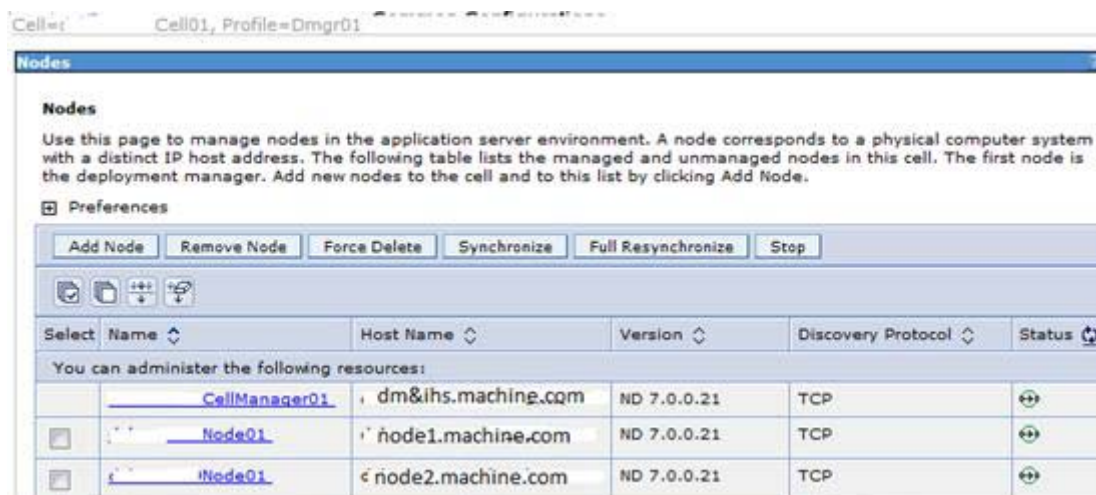


Figure 70. Synchronizing the node agents

If not, then stop the Node agents and run the `./synchNode.sh` as shown in the following figure. Then, restart the Node agents.

```

dellw1008:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./stopNode.sh
ADM00116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent/stopServer.log
ADM00128I: Starting tool with the AppSrv01 profile
ADM01100I: Reading configuration for server: nodeagent
Host/Cell Name: <default>
Username: wasadmin
Password:
ADM01201I: Server stop request issued. Waiting for stop status.
ADM04001I: Server nodeagent stop completed.

dellw1008:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./synchNode.sh ADM00116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/synchNode.log
ADM00128I: Starting tool with the AppSrv01 profile
ADM04001I: Begin synchNode operation for node [redacted] Node01 with Deployment
Manager: [redacted] mail.ie.ibm.com: 8878
ADM00161I: Synchronizing configuration between node and cell.
ADM04001I: The configuration for node [redacted] Node01 has been synchronized
with Deployment Manager [redacted] mail.ie.ibm.com: 8878
dellw1008:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./startNode.sh
ADM00116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent/startServer.log
ADM00128I: Starting tool with the AppSrv01 profile
ADM01100I: Reading configuration for server: nodeagent
ADM01200I: Server launched. Waiting for initialization status.
ADM03001I: Server nodeagent open for e-Business: process id is 11430

```

Figure 71. SynchNode command

9. Installation of DB2 9.7 Server

1. Copy the DB2 installation file, `DB2_ESE_V97_Linux_x86-64.tar` to your computer. Uncompress it and start the installer by running `./db2setup` as the root user. The following setup launchpad opens. Click **Install a Product**.

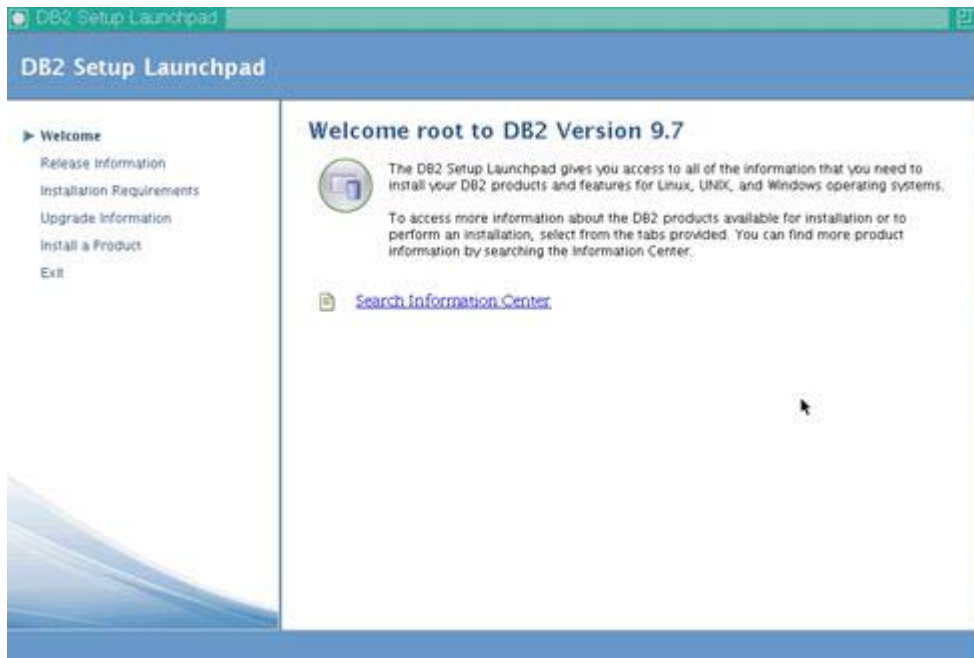


Figure 72. DB2 Setup Launchpad: Welcome

2. Click **Install New**.



Figure 73. DB2 Setup Launchpad: Install a product as root

- ___ 3. The DB2 Setup wizard displays. Click **Next** to continue.



Figure 74. DB2 Setup wizard: Welcome

- ___ 4. Accept the license agreement and click **Next** to continue.

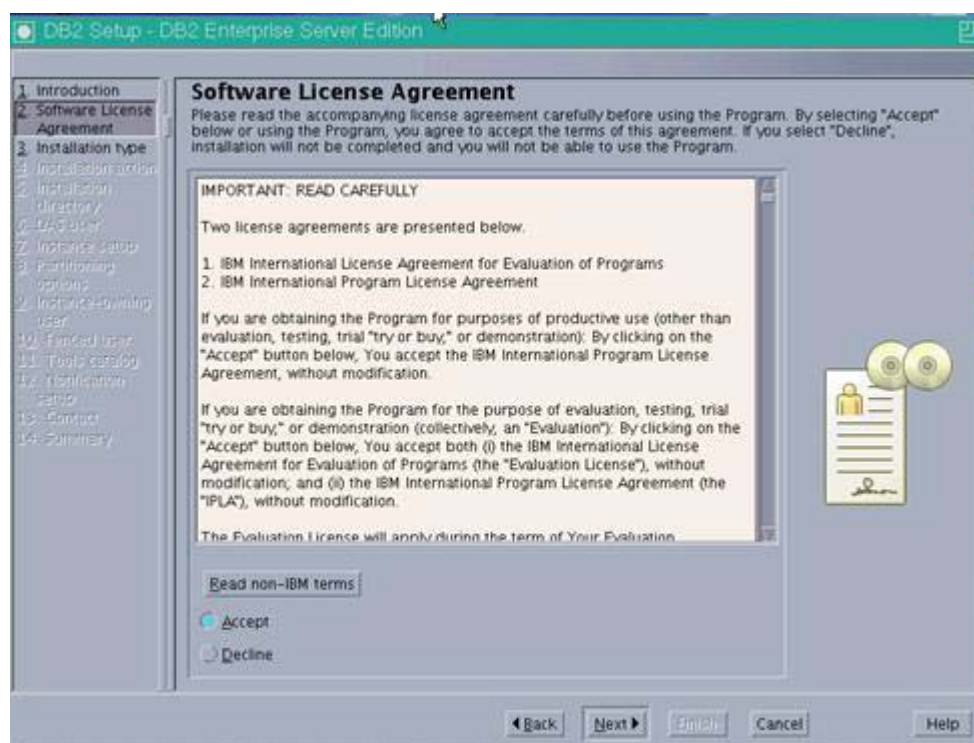


Figure 75. DB2 Setup wizard: Software License Agreement

5. Click **Typical** as the installation type and then **Next** to continue.



Figure 76. DB2 Setup wizard: Select the installation type

- ___ 6. Select the "Install DB2 Enterprise Server Edition on this computer and save my settings in a response file" option and click **Next** to continue.

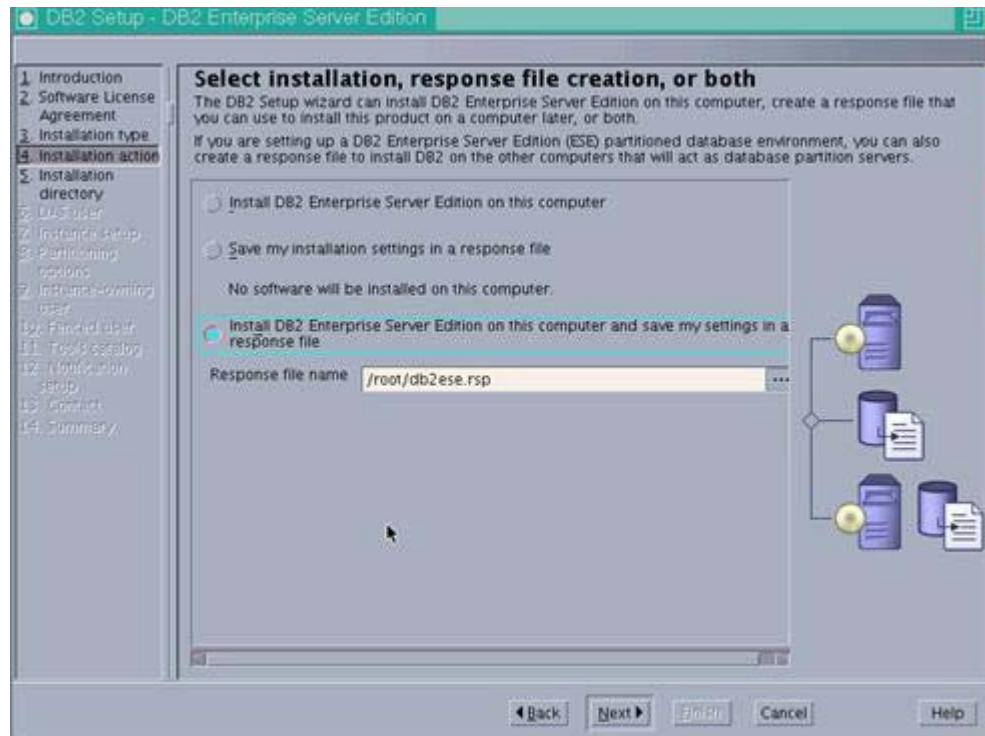


Figure 77. DB2 Setup wizard: Select installation, response file creation, or both

___ 7. Change the default installation path if needed. Then, click **Next** to continue.

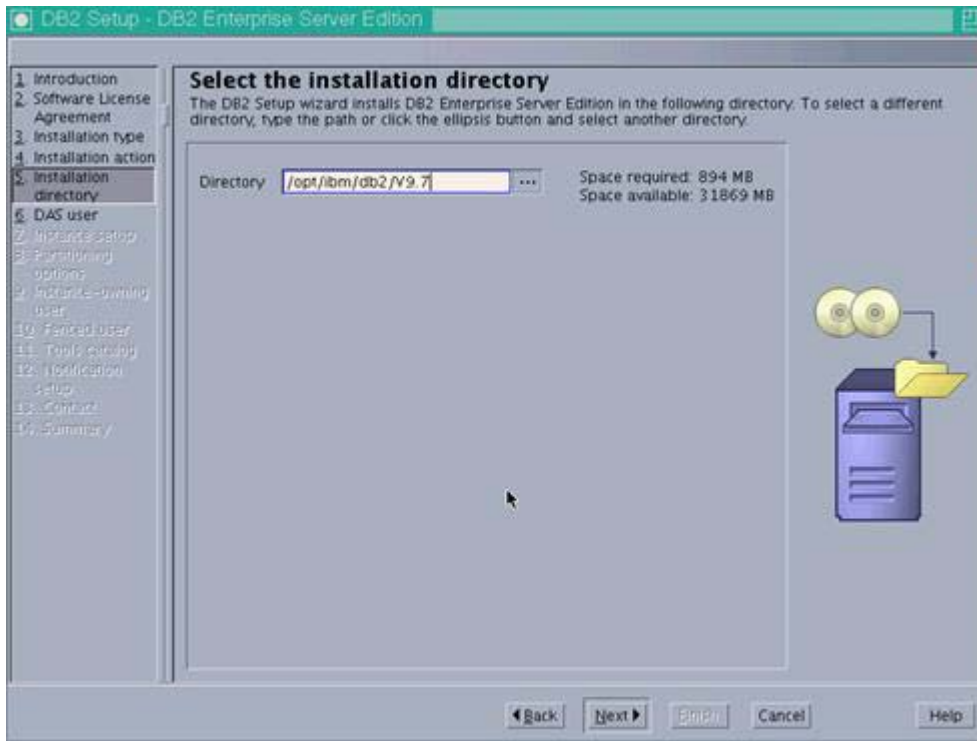


Figure 78. DB2 Setup wizard: Select the installation directory

___ 8. Enter the user name and password for the `dasusr1` user. Click **Next** to continue.

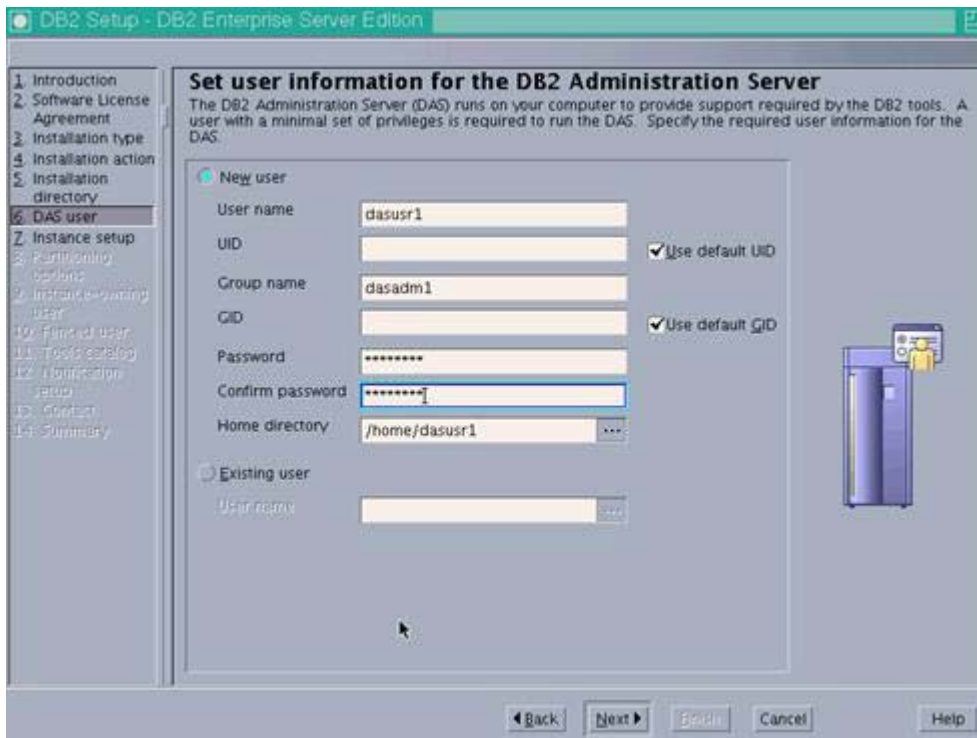


Figure 79. DB2 Setup wizard: Set user information for the DB2 Administration Server

- ___ 9. Select “Create a DB2 Instance” and click **Next** to continue.

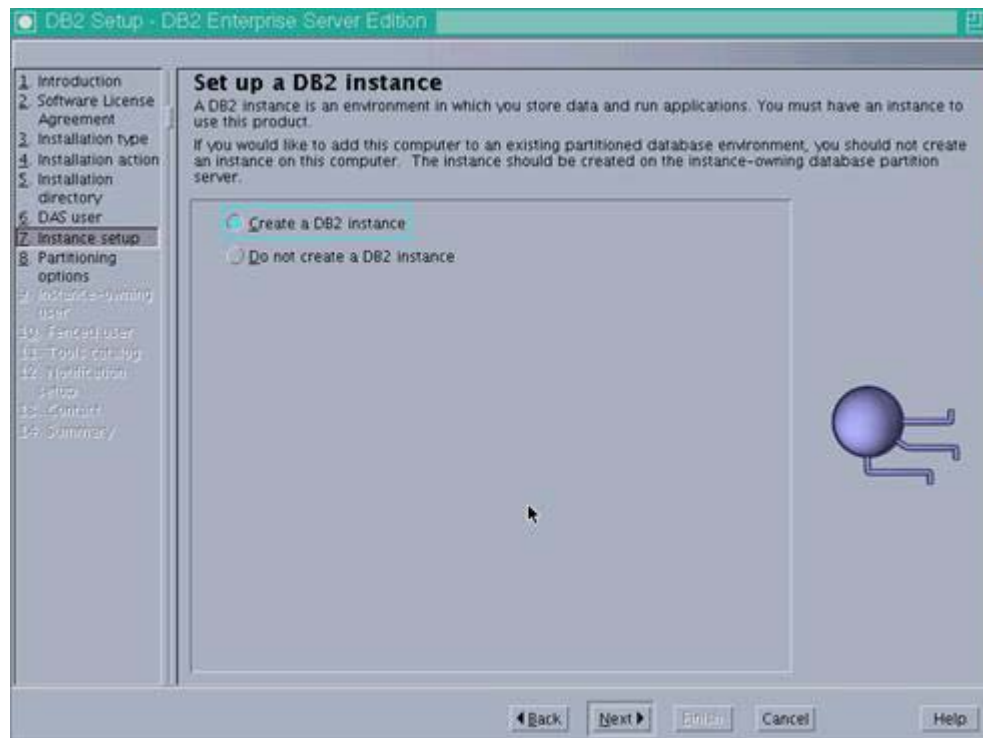


Figure 80. DB2 Setup wizard: Set up a DB2 instance

- ___ 10. Select “Single partition instance” and click **Next** to continue.

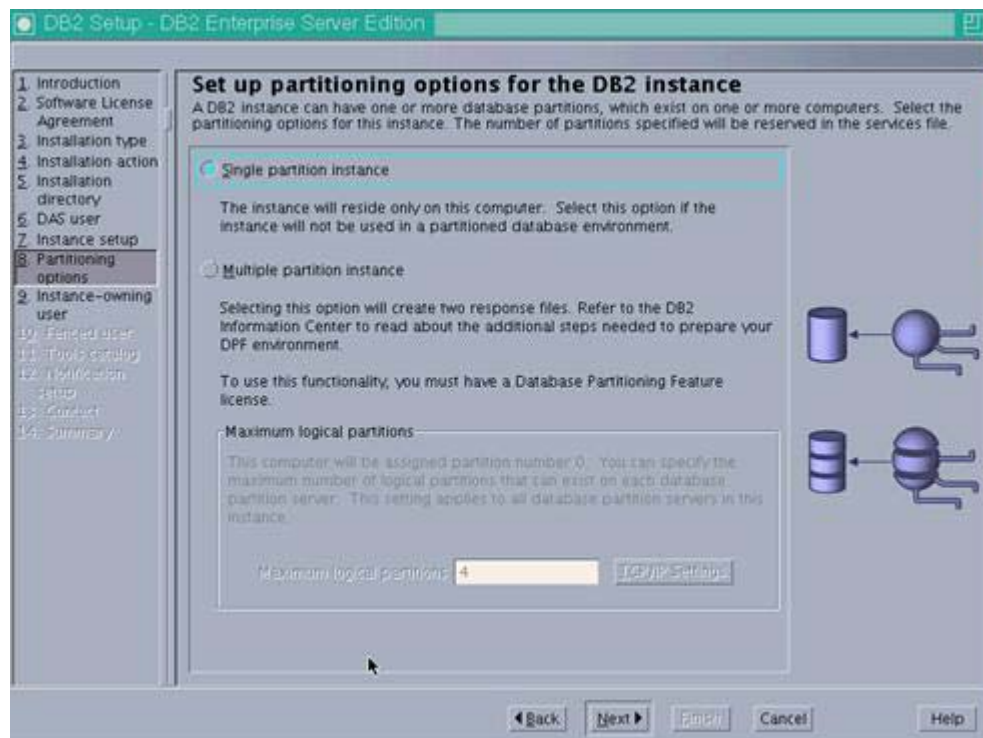
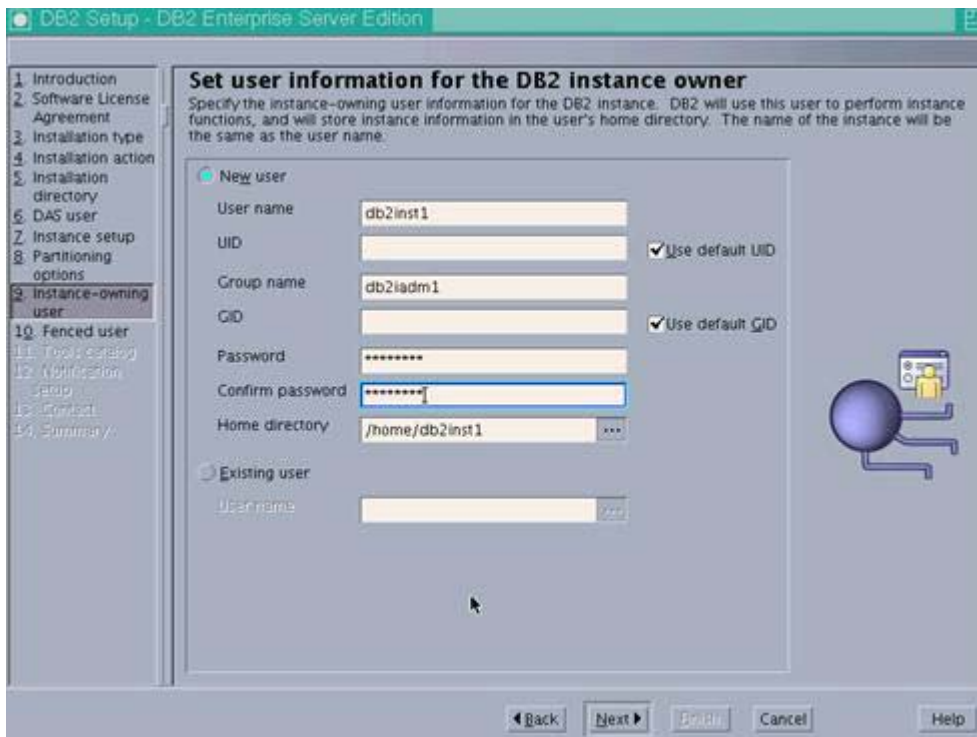


Figure 81. DB2 Setup wizard: Set up partitioning options for the DB2 instance

___ 11. Enter your database administrator user name and password. Then, click **Next** to continue.



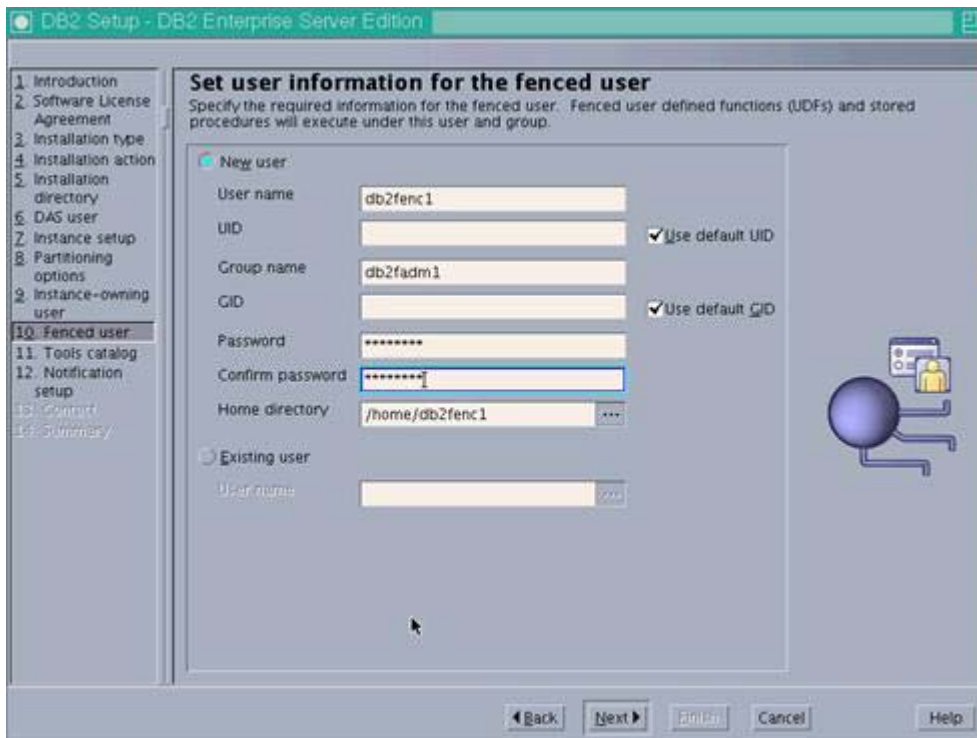
The screenshot shows the 'Set user information for the DB2 instance owner' step of the DB2 Setup wizard. The left sidebar lists steps 1 through 14, with step 9, 'Instance-owning user', highlighted. The main window contains the following fields and options:

- New user** (selected):
 - User name: db2inst1
 - UID: [empty]
 - Group name: db2iadm1
 - GiD: [empty]
 - Password: [masked]
 - Confirm password: [masked]
 - Home directory: /home/db2inst1
- Existing user** (unselected):
 - User name: [empty]

Checkboxes for 'Use default UID' and 'Use default GiD' are checked. Navigation buttons at the bottom include Back, Next, Finish, Cancel, and Help.

Figure 82. DB2 Setup wizard: Set user information for the DB2 instance owner

___ 12. Enter your fenced user name and password. Then, click **Next** to continue.



The screenshot shows the 'Set user information for the fenced user' step of the DB2 Setup wizard. The left sidebar lists steps 1 through 14, with step 10, 'Fenced user', highlighted. The main window contains the following fields and options:

- New user** (selected):
 - User name: db2fenc1
 - UID: [empty]
 - Group name: db2fadm1
 - GiD: [empty]
 - Password: [masked]
 - Confirm password: [masked]
 - Home directory: /home/db2fenc1
- Existing user** (unselected):
 - User name: [empty]

Checkboxes for 'Use default UID' and 'Use default GiD' are checked. Navigation buttons at the bottom include Back, Next, Finish, Cancel, and Help.

Figure 83. DB2 Setup wizard: Set user information for the fenced user

___ 13. Select "Do not prepare the DB2 tools catalog" and click **Next** to continue.

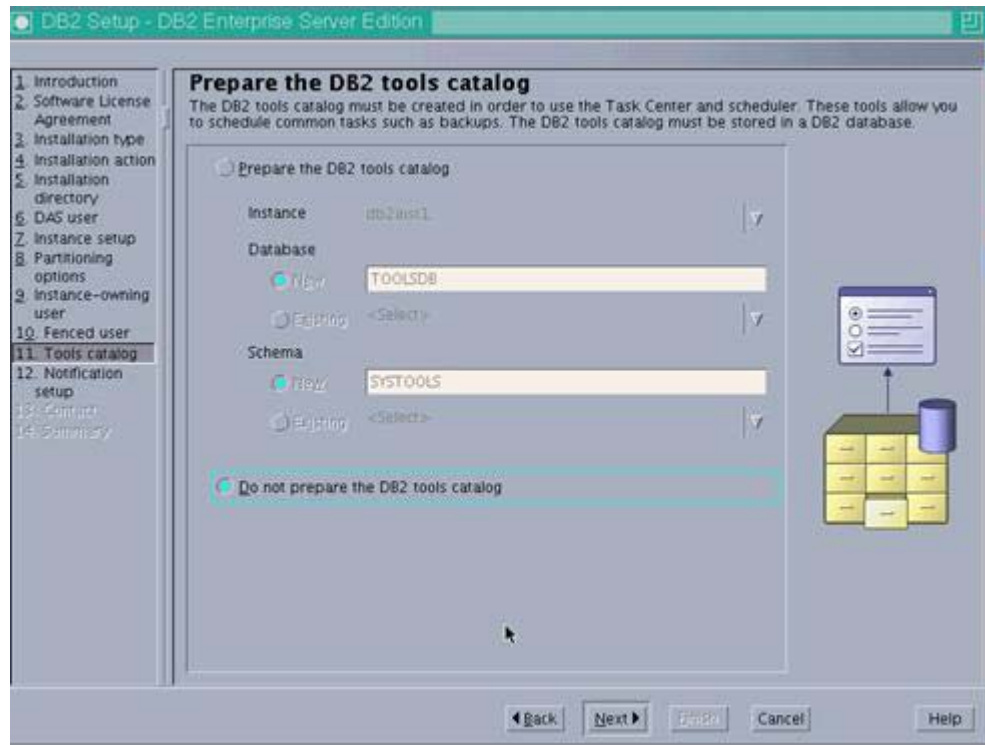


Figure 84. DB2 Setup wizard: Prepare the DB2 tools catalog

- ___ 14. Select "Do not set up your DB2 server to send notifications at this time" and click **Next** to continue.

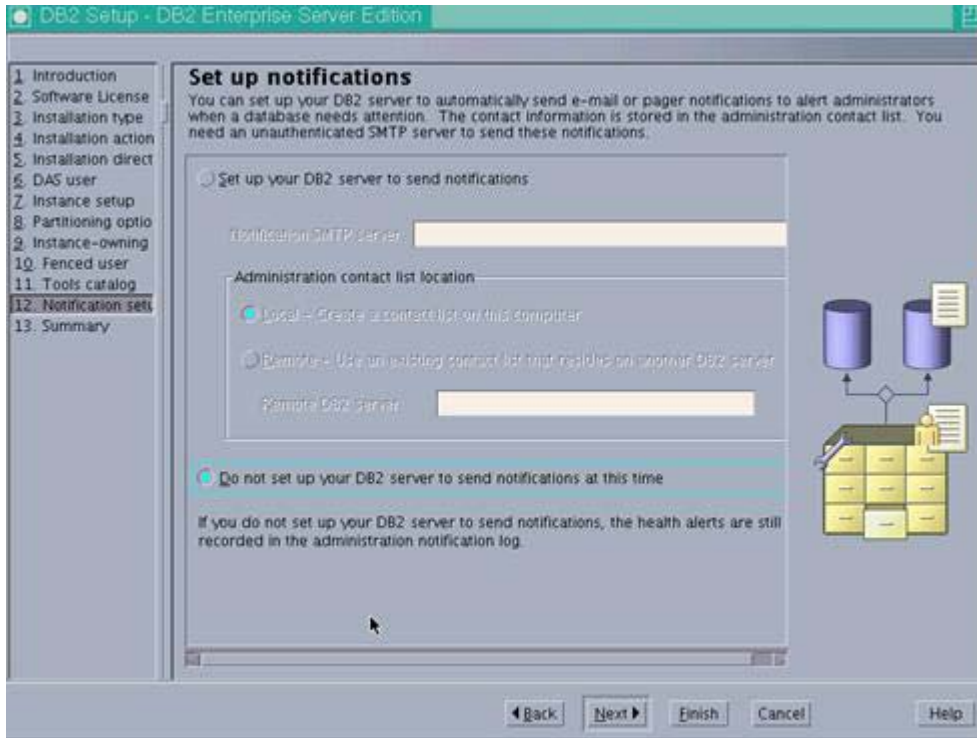


Figure 85. DB2 Setup wizard: Set up notifications

- ___ 15. Click **Finish** from the summary screen to start the installation of the files onto the system.

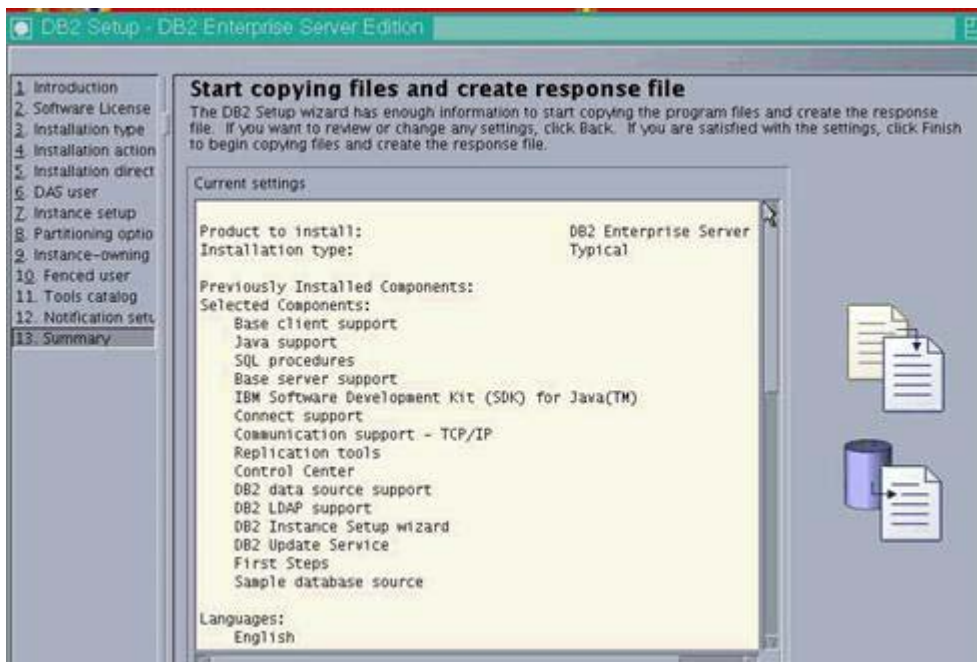


Figure 86. DB2 Setup wizard: Start copying files and create response file

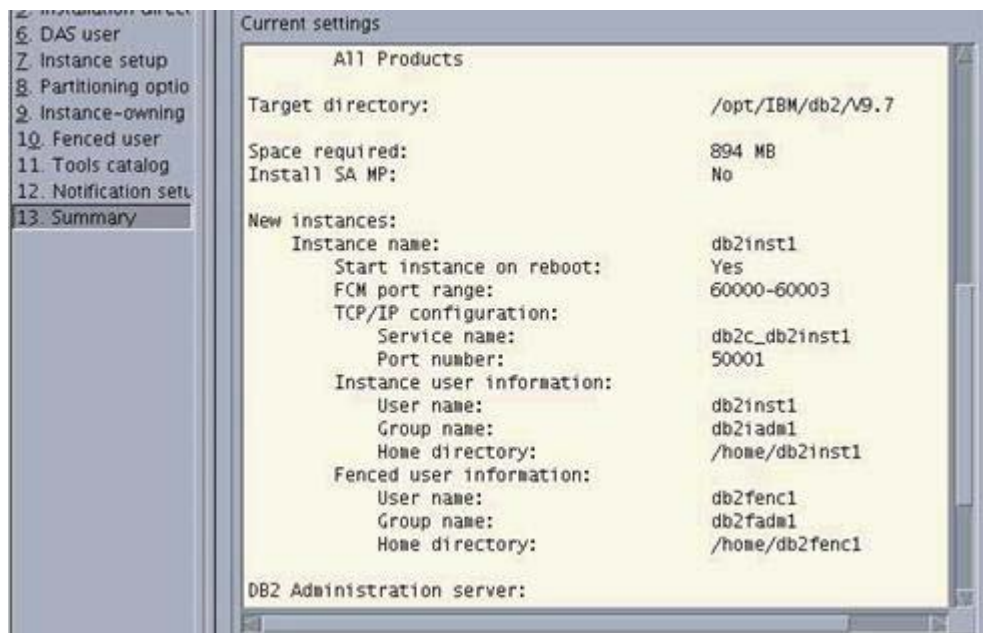


Figure 87. DB2 Setup wizard: Start copying files and create response file

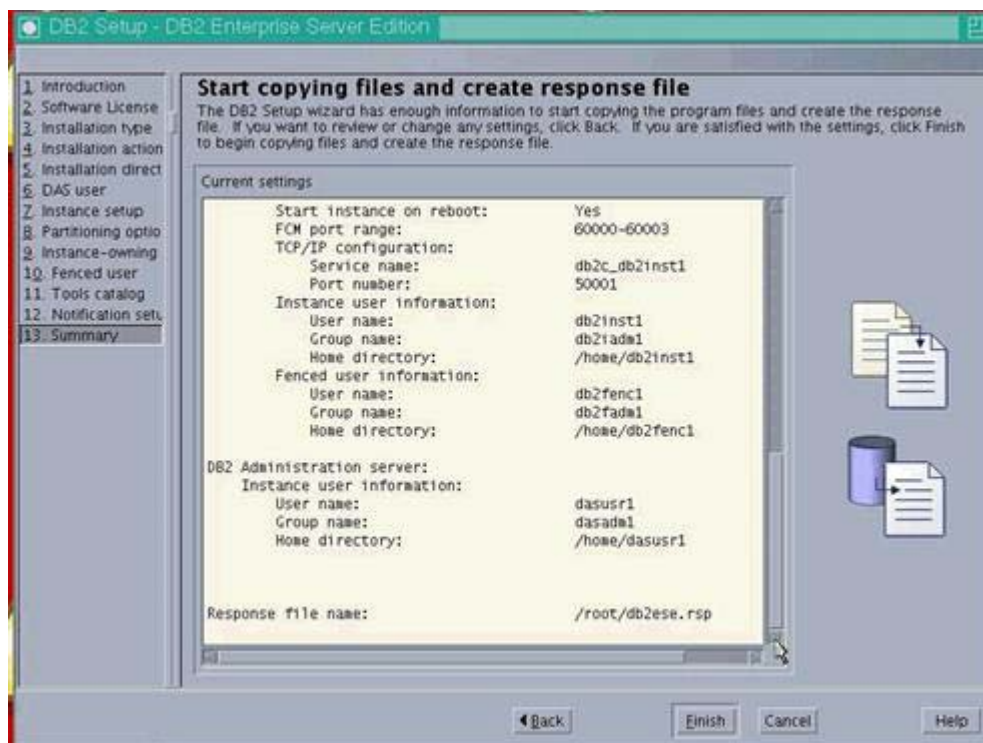


Figure 88. DB2 Setup wizard: Start copying files and create response file

The installation starts.

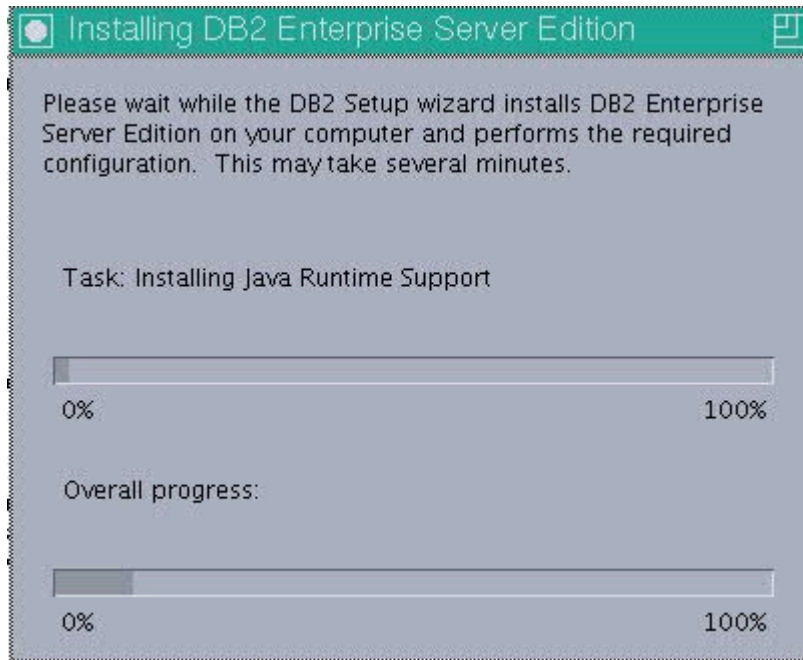


Figure 89. DB2 Enterprise Server Edition: Installation in progress

___ 16. After some time the installation completes. Click **Finish** to close the installer.

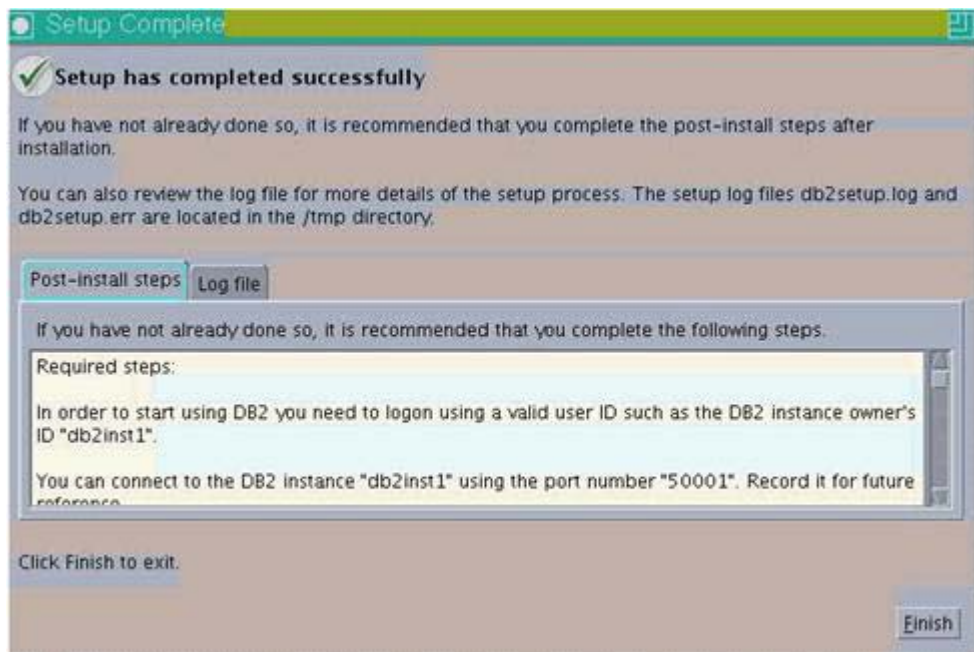


Figure 90. DB2 Setup wizard: Setup complete

- ___ 17. Open a comment terminal prompt and log in as db2admin user. Then, run db2level and you should see:

```
:/ # su - db2inst1
```

Figure 91. Comment terminal prompt

```
db2inst1@: ~$ db2level
DB21085I Instance "db2inst1" uses "64" bits and DB2 code release "SQL09070"
with level identifier "08010107".
Informational tokens are "DB2 v9.7.0.0", "s090521", "LINUXAMD6497", and Fix
Pack "0".
Product is installed at "/opt/IBM/db2/V9.7".

db2inst1@: ~$
```

Figure 92. Comment terminal prompt

10. Installing DB2 9.7 client on your Deployment Manager and Application Server nodes



Hint

The following screen captures in this section are for DB2 9.7 client installation on the Deployment Manager computer. Likewise, you must also do the same steps on both of your Application Server nodes.

1. Copy the DB2 installation file, `DB2_ESE_V97_Linux_x86-64.tar` to your computer. Uncompress it and start the installer by running `./db2setup` as the root user. The DB2 Setup Launchpad opens. Select **Install a Product** and then select **Install New** from the IBM Data Server Runtime Client Version 9.7.



Note

Some users copy the JDBC `.jar` files to their application servers but it is better to install the DB2 client.



Figure 93. DB2 Setup Launchpad: Install a product

- ___ 2. Click **Next** from the introduction panel.



Figure 94. DB2 Setup: Introduction

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



Figure 95. DB2 Setup: Software License Agreement

4. Select **Typical** as the installation type and click **Next** to continue.

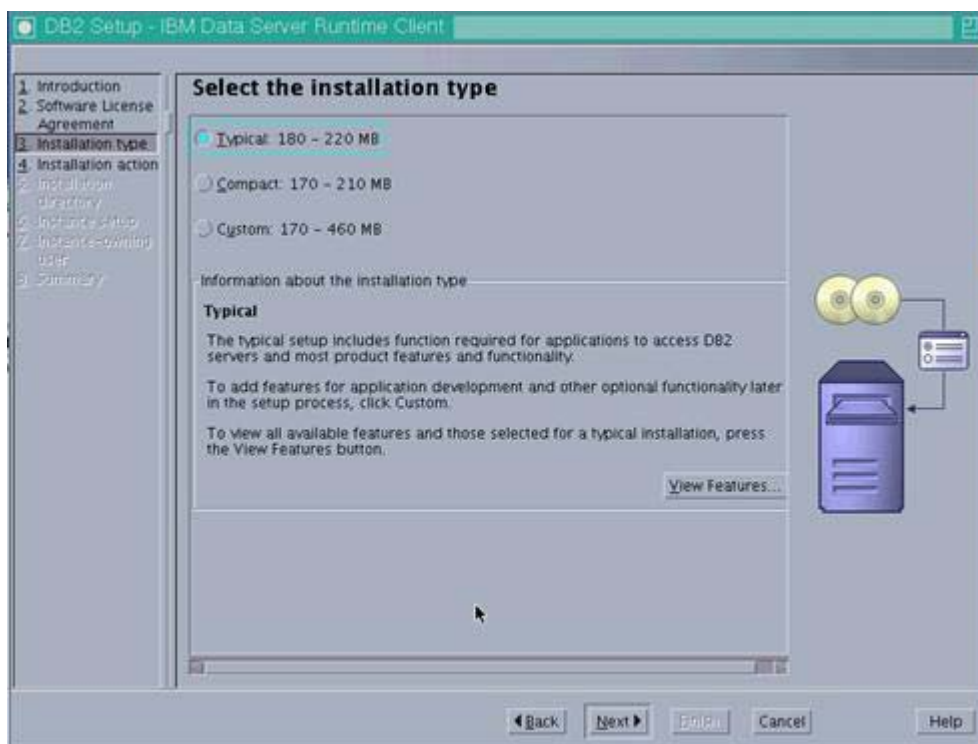


Figure 96. DB2 Setup: Select the installation type

5. Select “Install IBM Data Server Runtime Client on this computer” and then click **Next** to continue.

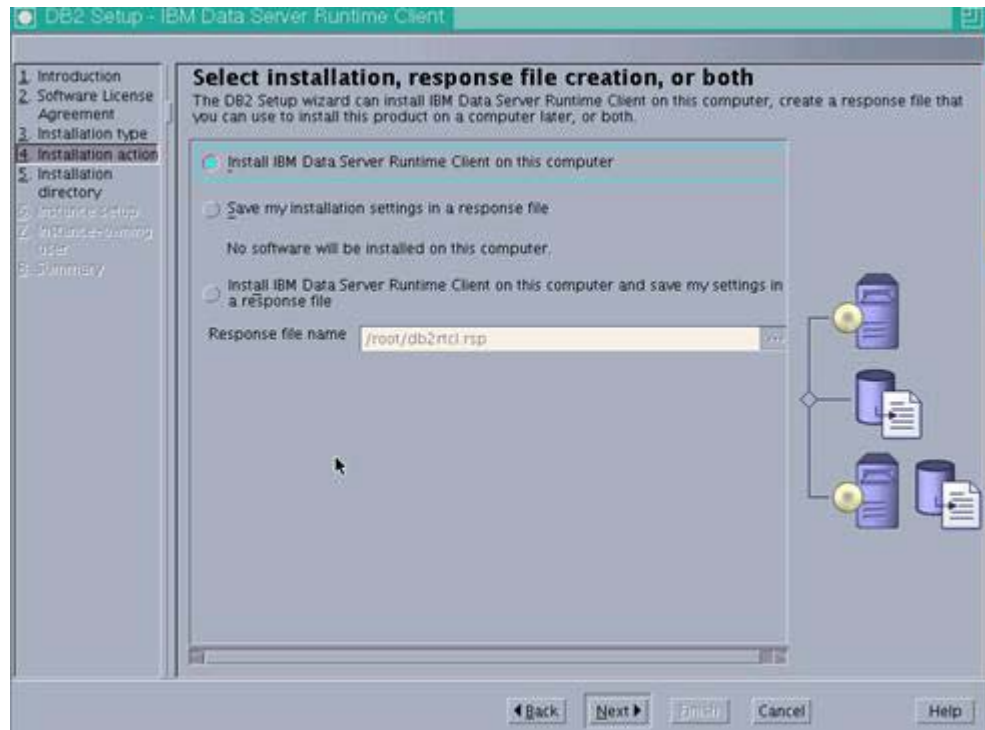


Figure 97. DB2 Setup: Select installation, response file creation, or both

___ 6. Change the installation directory if needed and click **Next** to continue.

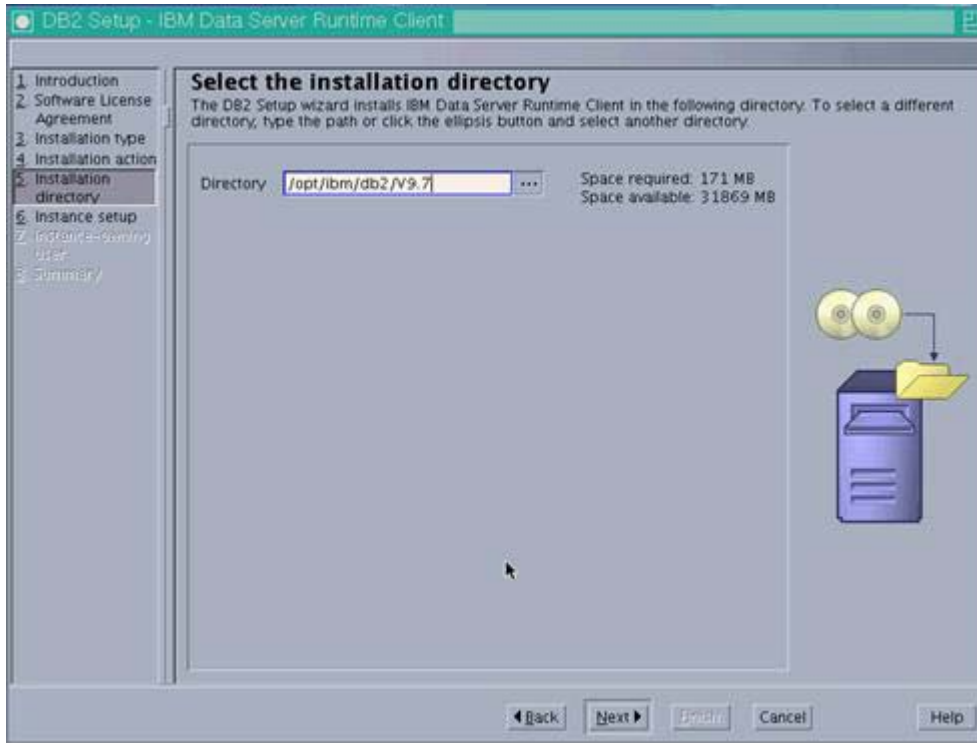


Figure 98. DB2 Setup: Select the installation directory

___ 7. Select "Create a DB2 instance" and click **Next** to continue.

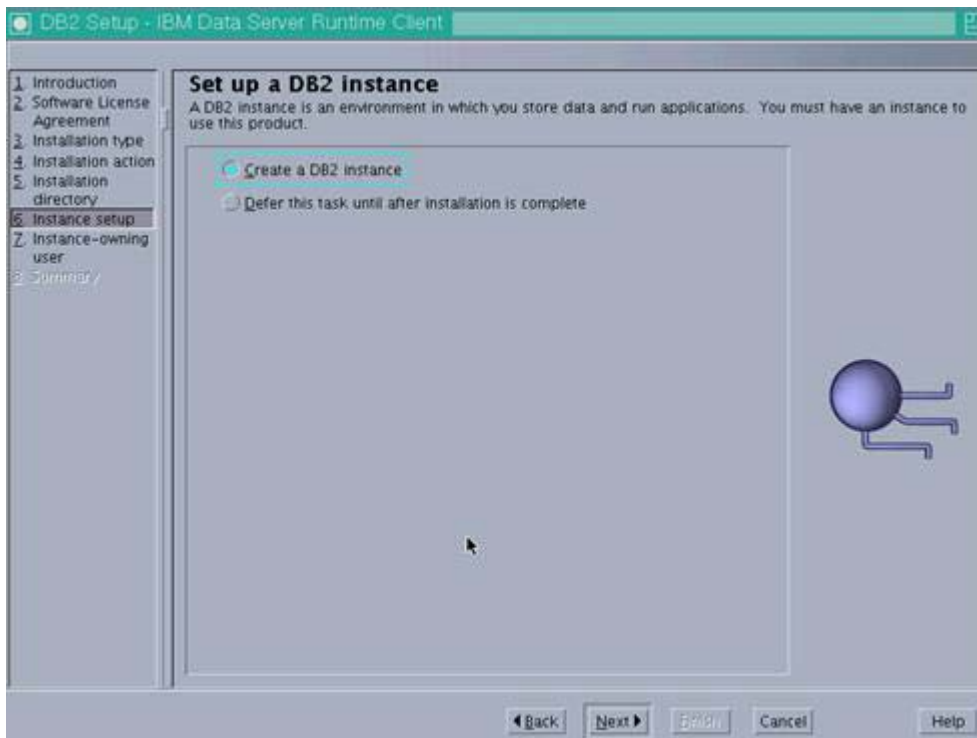


Figure 99. DB2 Setup: Set up a DB2 instance

- ___ 8. Enter your DB2admin user and password and click **Next** to continue.

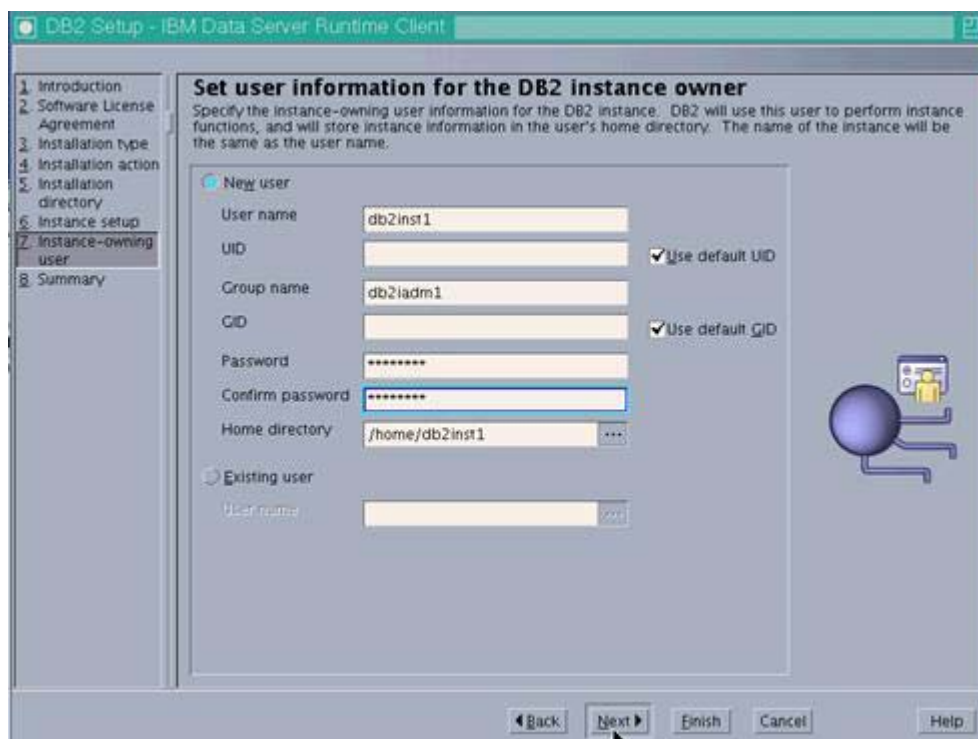


Figure 100. DB2 Setup: Set up user information for the DB2 instance owner

- ___ 9. Click **Finish** from the summary page to start the installation.

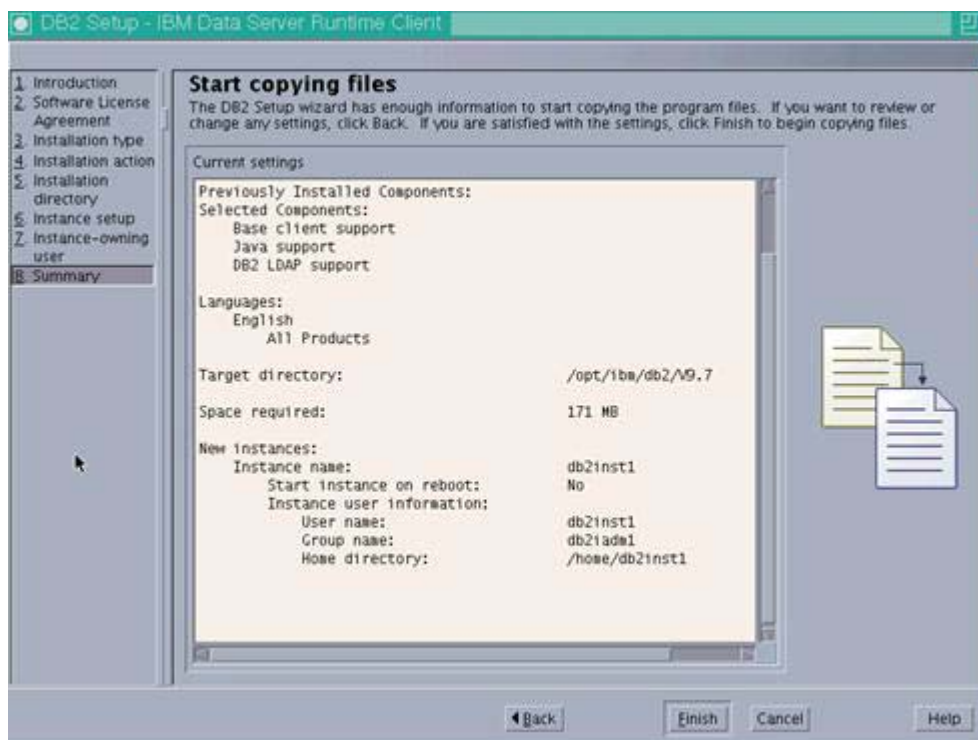


Figure 101. DB2 Setup: Start copying files

The installation starts.

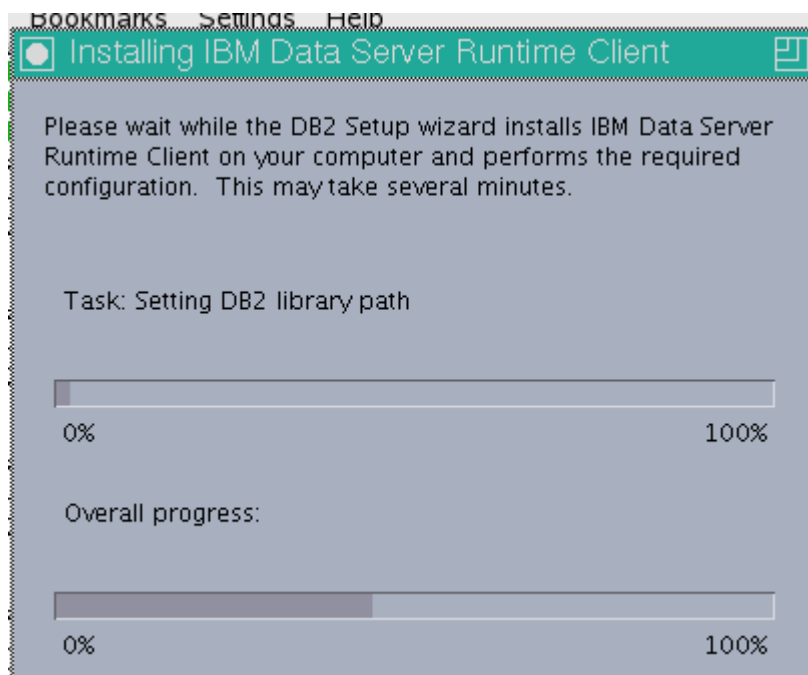


Figure 102. DB2 Setup: Installation in progress

___ 10. After some time the installation completes. Click **Finish** to exit the wizard.

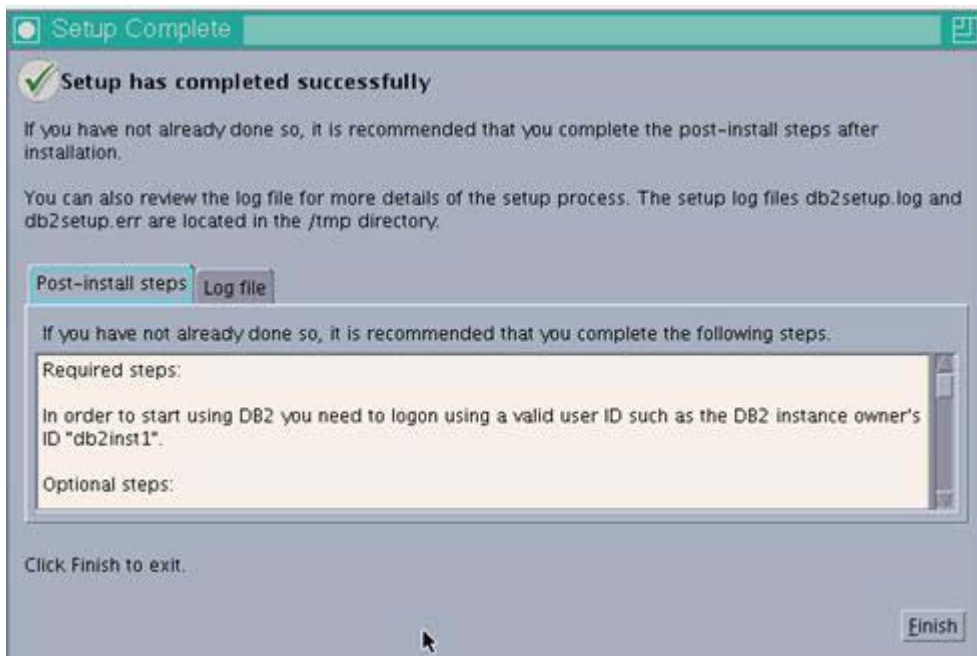


Figure 103. DB2 Setup: Setup Complete

- ___ 11. The installation is now complete. Switch to your DB2 admin user and run `db2level` to check the level.

```
db2inst1@r1:~$ su - db2inst1
db2inst1@r1:~$ db2level
DB21085I Instance "db2inst1" uses "64" bits and DB2 code release "SQL09070"
with level identifier "08010107".
Informational tokens are "DB2 v9.7.0.0", "s090521", "LINUXAMD6497", and Fix
Pack "0".
Product is installed at "/opt/ibm/db2/V9.7".

db2inst1@r1:~$
```

Figure 104. Running `db2level`

11. Installation of DB2 9.7: FixPack 6: Server + Client



Note

This fix pack installation must be on your database server and on each of your DB2 Clients.

1. Copy the DB2 FixPack 6 installation files to your system, `v9.7fp6_linuxx64_server.tar.gz`. Uncompress it and start the installer by running `./installfixpack` as the root user.
2. Enter `/opt/ibm/db2/V9.7` for the full path of the installation directory and press Enter.

```

root@ibm017:/opt/software/DB2/DB2v9.7-64bit/server # ./installFixPack
DBI1073E The -b <baseInstallPathOfDB2> is required for the installer
script installFixPack.

Enter full path name for the install directory -
-----

```

Figure 105. Entering full path name for the installation directory

After some time the FixPack completes its installation.

```

The execution completed successfully.
For more information see the DB2 installation log at
"/tmp/installFixPack.log.384".
root@ibm017:/opt/software/DB2/DB2v9.7-64bit/server # █

```

Figure 106. FixPack installation completed

3. Now, you update the instances. Go to `/opt/ibm/db2/V9.7/instance` and run `./db2iupdt db2inst1`. It is run as the root user.

```

root@ibm017:/opt/ibm/db2/V9.7/instance # ./db2iupdt db2inst1
DBI1070I Program db2iupdt completed successfully.
█
root@ibm017:/opt/ibm/db2/V9.7/instance # █
-----

```

Figure 107. Updating the instances



Note

Do the following steps on the DB2 database server but not on the DB2 client.

4. Then, update the `dasusr1` instance from the root user.

```
[root@db2inst1 ~]# ./dasupdt dasusr1
SQL4407W The DB2 Administration Server was stopped successfully.
SQL4406W The DB2 Administration Server was started successfully.
DBI1070I Program dasupdt completed successfully.
```

Figure 108. Updating the `dasusr1` instance from the root user

5. Start DB2 and run `db2level`. You see that FP4 is now installed.

```
db2inst1@db2inst1:~$ db2start
06/21/2012 15:00:34 0 0 SQL1026N The database manager is already active
```

Figure 109. Running `db2level`

```
db2inst1@db2inst1:~$ db2level
DB21085I Instance "db2inst1" uses "64" bits and DB2 code release "SQL09074"
with level identifier "08050107".
Informational tokens are "DB2 v9.7.0.6", "s110330", "IP23243", and Fix Pack
"6".
Product is installed at "/opt/IBM/db2/V9.7".
```

Figure 110. FP4 successfully installed

12. Apply the DB2 license to your server

1. The factory-shipped database product comes without a license installed. To check, you can run `db2licm -l`.

```
db2inst1@...:~> db2start
06/21/2012 15:00:34      0  0  SQL1026N The database manager is already active
.
SQL1026N The database manager is already active.
db2inst1@...:~> db2licm -l
Product name:          "DB2 Enterprise Server Edition"
License type:          "License not registered"
Expiry date:           "License not registered"
Product identifier:    "db2ese"
Version information:   "9.7"
```

Figure 111. DB license

2. You can see that this copy is reported as unregistered. Copy your license to the computer and run `db2licm -a <database license file>`.

```
db2inst1@...:~> db2licm -a /opt/software/DB2v9.7-64bit/db2ese_u.lic
LIC1402I License added successfully.

LIC1426I This product is now licensed for use as outlined in your License Agree-
ment. USE OF THE PRODUCT CONSTITUTES ACCEPTANCE OF THE TERMS OF THE IBM LICENSE
AGREEMENT, LOCATED IN THE FOLLOWING DIRECTORY: "/opt/IBM/db2/V9.7/license/en_US
.iso88591"
db2inst1@...:~> whoami
db2inst1
db2inst1@...:~> db2level
DB21085I Instance "db2inst1" uses "64" bits and DB2 code release "SQL09074"
with level identifier "08050107".
Informational tokens are "DB2 v9.7.0.6", "s110330", "IP23243", and Fix Pack
"6".
Product is installed at "/opt/IBM/db2/V9.7".

db2inst1@...:~> db2licm -l
Product name:          "DB2 Enterprise Server Edition"
License type:          "Authorized User Option"
Expiry date:           "Permanent"
Product identifier:    "db2ese"
Version information:   "9.7"
Enforcement policy:   "Soft Stop"
Number of licensed authorized users: "25"
Features:
DB2 Performance Optimization ESE: "Not licensed"
DB2 Storage Optimization: "Not licensed"
DB2 Advanced Access Control: "Not licensed"
DB2 Geodetic Data Management: "Not licensed"
IBM Homogeneous Replication ESE: "Not licensed"

db2inst1@...:~>
```

Figure 112. License added successfully

3. When the license is run, you can then check the license again and its reported as permanent.

13. Create Connections databases on DB2 server



Note

You can create Connections databases in two different ways: one way through Database wizard and other way by using SQL scripts.

Before you can use the wizard to create databases for your IBM Connections deployment, prepare the database server. Follow these steps:

- ___ 1. Log in to your database server as the root user or system administrator.
- ___ 2. Grant display authority to all users by running the following commands under the root user or system administrator: `xhost + // Grant display authority to other users.`

```

Terminal
File Edit View Terminal Tabs Help
:~ # xhost +
access control disabled, clients can connect from any host
:~ # echo $DISPLAY
:1.0
:~ # █
  
```

Figure 113. Granting display authority to other users

- ___ 3. `echo $DISPLAY`: Echo the value of DISPLAY under the root user. Ensure that the current user is qualified or else switch to a qualified user by running the following commands.

```

Terminal
File Edit View Terminal Tabs Help
:~ # xhost +
access control disabled, clients can connect from any host
:~ # echo $DISPLAY
:1.0
:~ # █
  
```

Figure 114. `echo $DISPLAY`

- ___ 4. Log in as db2 admin.
- ___ 5. Export `DISPLAY=<hostname:displaynumber.screennumber>`, where `<hostname:displaynumber.screennumber>` represents the client system, monitor number, and window number.

- ___ 6. xclock: Display the clock, confirming that the current user has display authority and can run the wizard.



Figure 115. Displaying the clock

- ___ 7. Start the database instance.

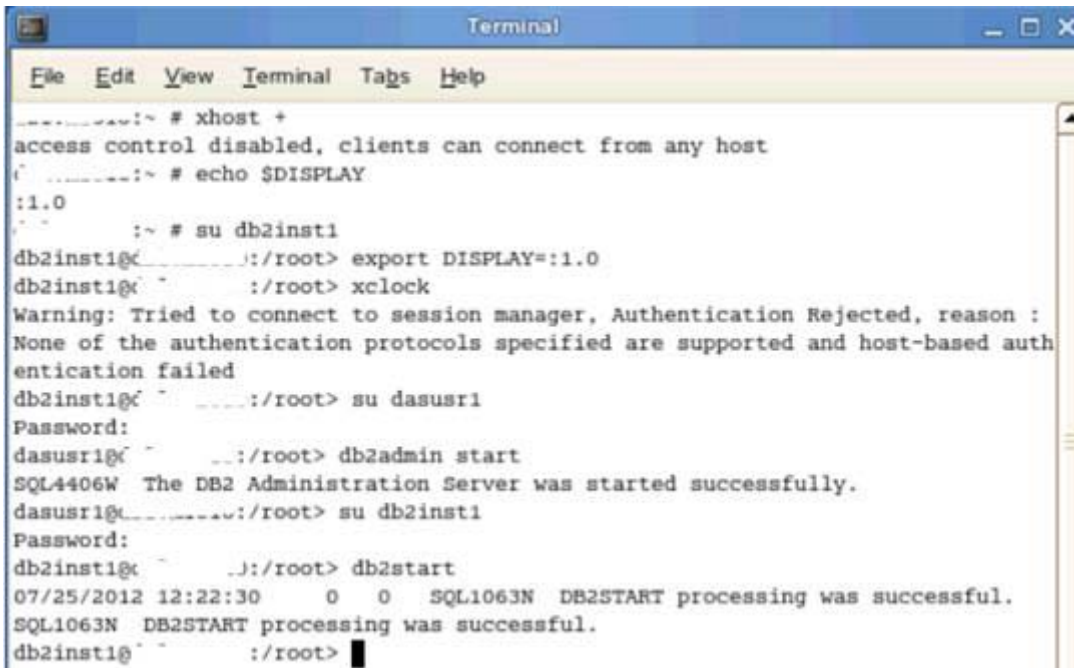


Figure 116. Starting the database instance

8. The creation of the Connections databases is now done with a wizard. Copy the Lotus_Connections_4.0_wizards_lin_aix.tar to your computer and extract it. Do it as the db2admin user on the operating system and **not** root. Then, go into the wizard folder and run ./dbWizard.sh. You see the following result:



```
Terminal
File Edit View Terminal Tabs Help
dslvm1010:~ # xhost +
access control disabled, clients can connect from any host
dslvm1010:~ # echo $DISPLAY
:1.0
dslvm1010:~ # su db2inst1
db2inst1@~:~:~:/root> export DISPLAY=:1.0
db2inst1@~:~:~:/root> xclock
Warning: Tried to connect to session manager, Authentication Rejected, reason :
None of the authentication protocols specified are supported and host-based authentication failed
db2inst1@~:~:~:/root> su dasusr1
Password:
dasusr1@~:~:~:/root> db2admin start
SQL4406W The DB2 Administration Server was started successfully.
dasusr1@~:~:~:/root> su db2inst1
Password:
db2inst1@~:~:~:/root> db2start
07/25/2012 12:22:30 0 0 SQL1063N DB2START processing was successful.
SQL1063N DB2START processing was successful.
db2inst1@~:~:~:/root> cd /wiz/Wizards/
db2inst1@~:~:~:/wiz/Wizards> ./dbwizard.sh
```

Figure 117. Running the database wizard for IBM Connections 4.0

___ 9. In the database wizard for IBM Connections 4.0, click **Next** to continue.

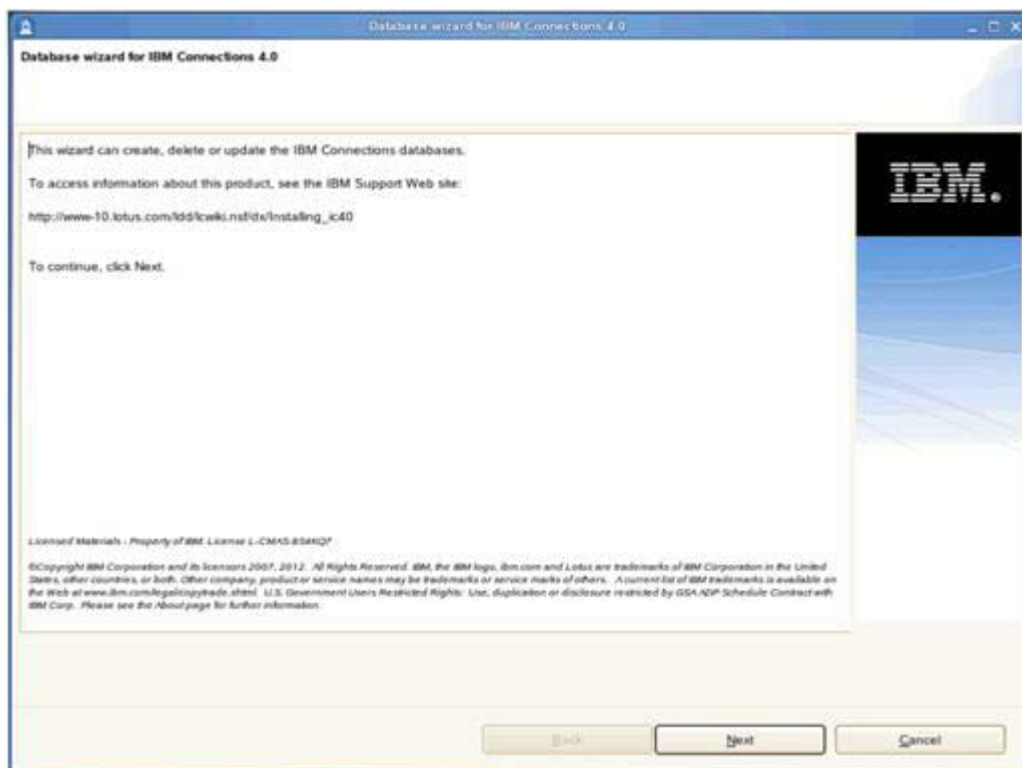


Figure 118. Database wizard for IBM Connections 4.0: Welcome

- ___ 10. Choose what you want to do: Create, delete, or upgrade. Click **Create** and then **Next** to continue.

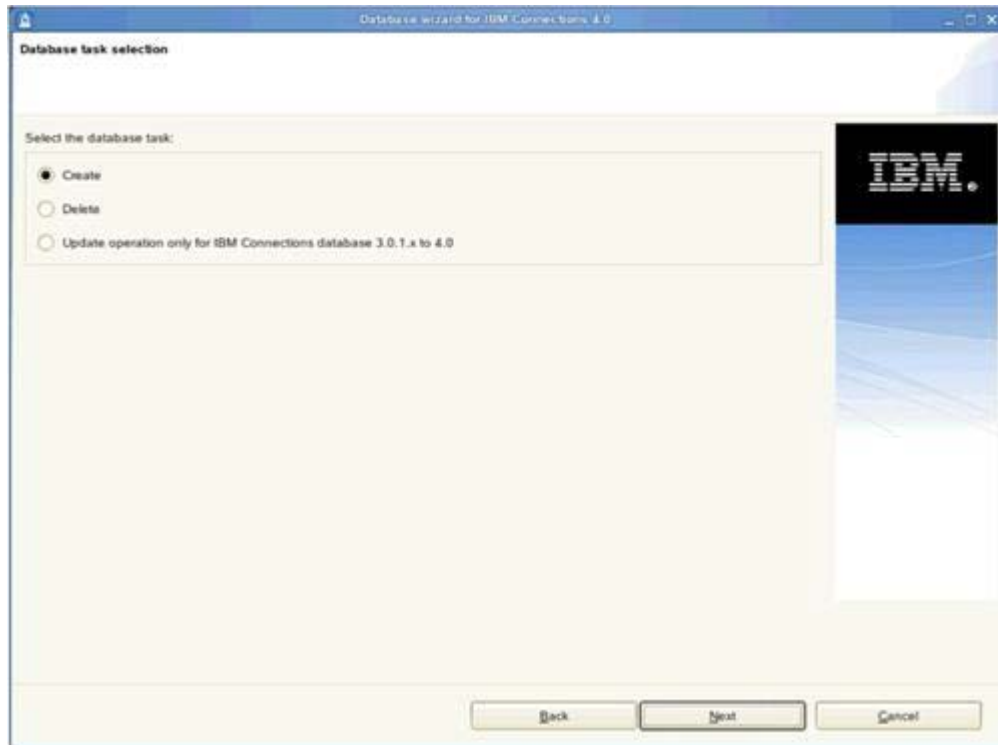


Figure 119. Database wizard for IBM Connections 4.0: Database task selection

- ___ 11. Select the path for your database installation location and the database instance name. Click **Next** to continue.

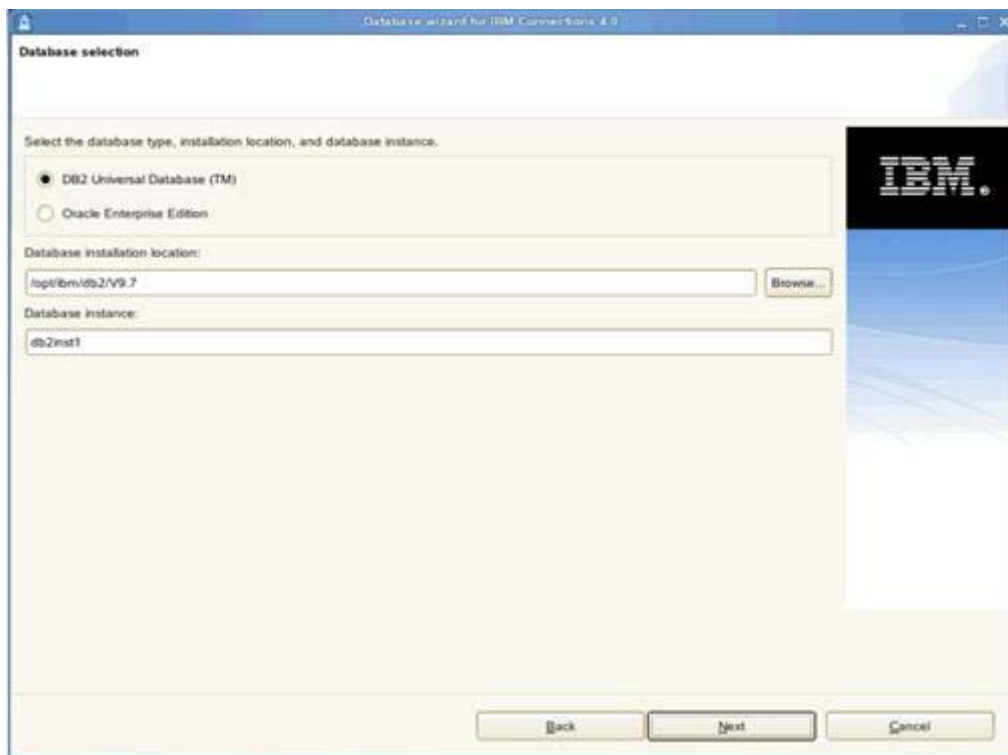


Figure 120. Database wizard for IBM Connections 4.0: Database selection

___ 12. Ensure that databases are selected and then click **Next** to continue.

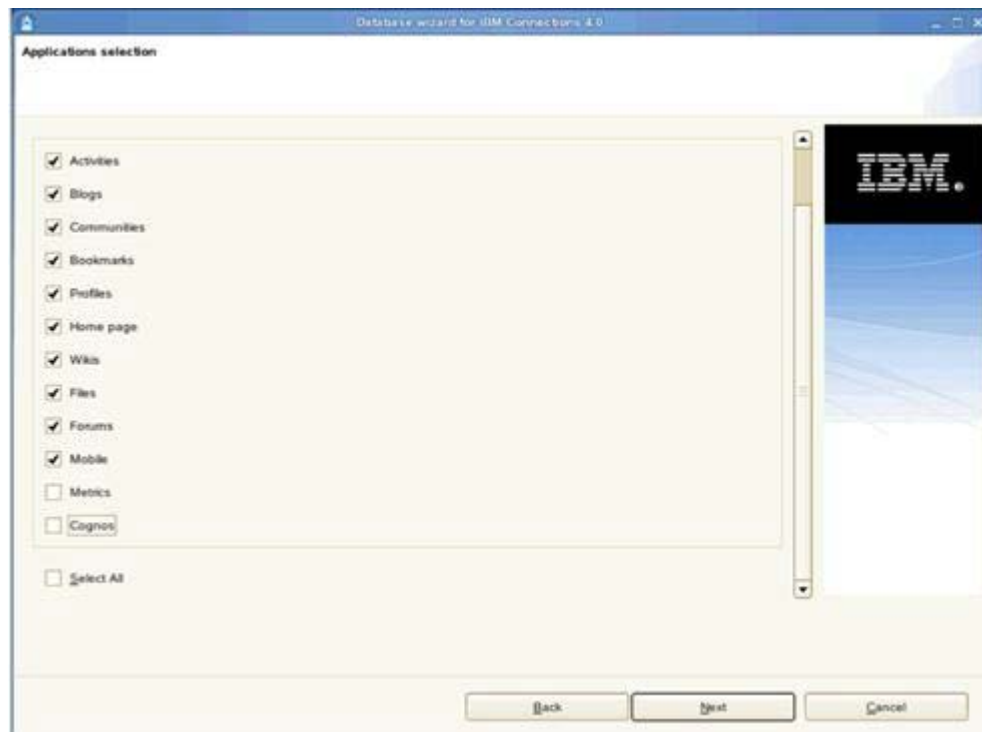


Figure 121. Database wizard for IBM Connections 4.0: Applications selection

___ 13. Click **Create** in the summary screen.

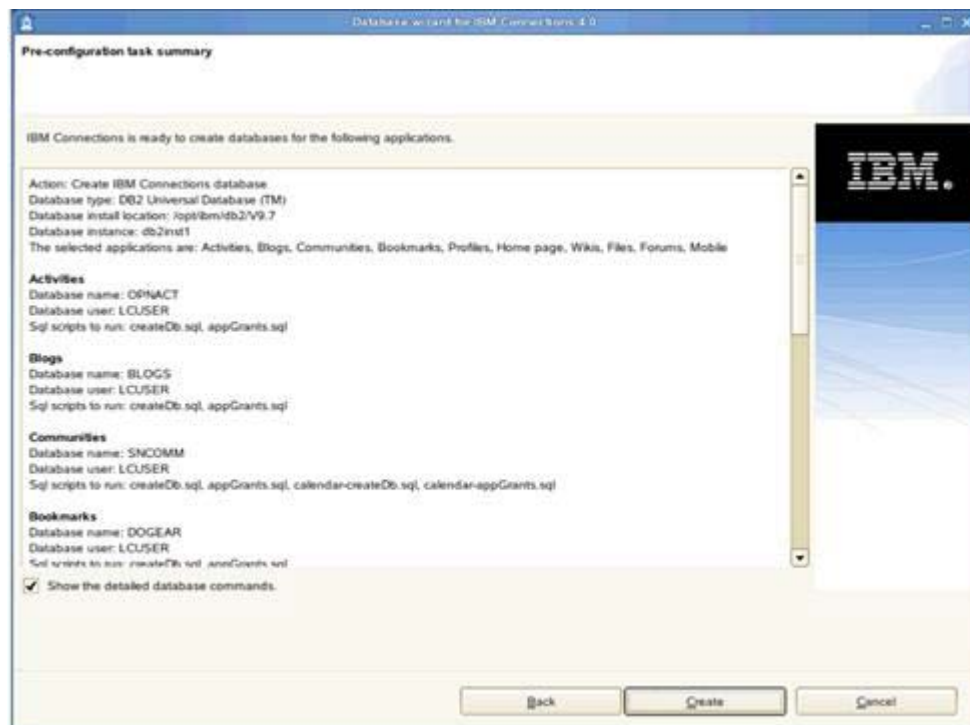


Figure 122. Database wizard for IBM Connections 4.0: Pre-configuration task summary

___ 14. Finally, click **Execute** to create the databases.

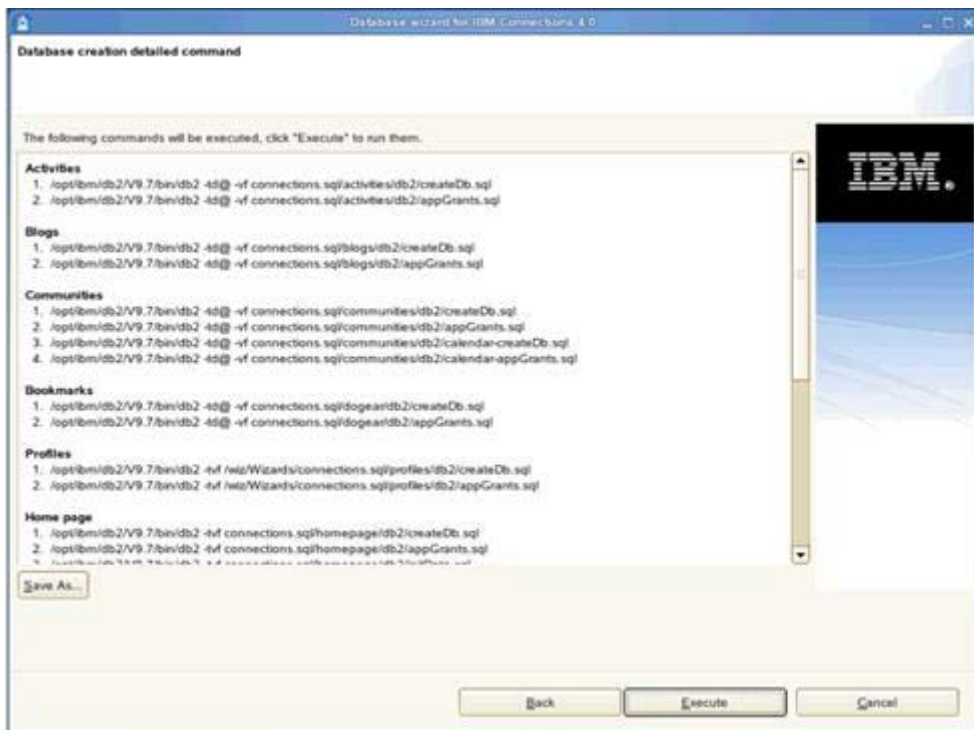


Figure 123. Database wizard for IBM Connections 4.0: Database creation detailed command

The database creation starts:

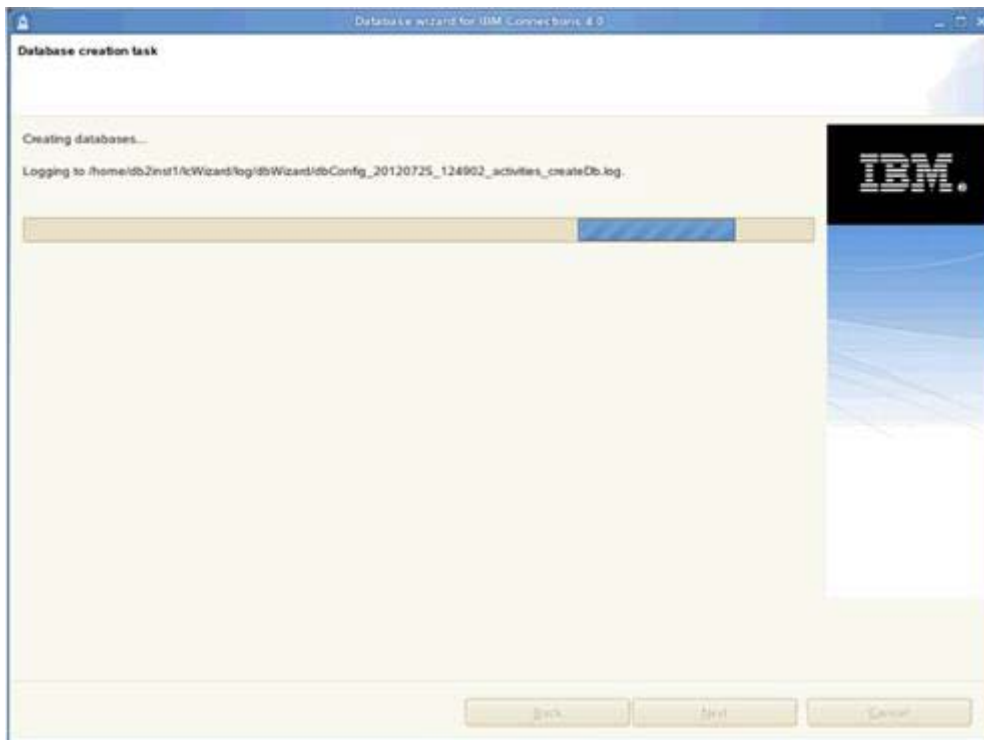


Figure 124. Database wizard for IBM Connections 4.0: Databases creation in progress

After some time the databases are successfully created.

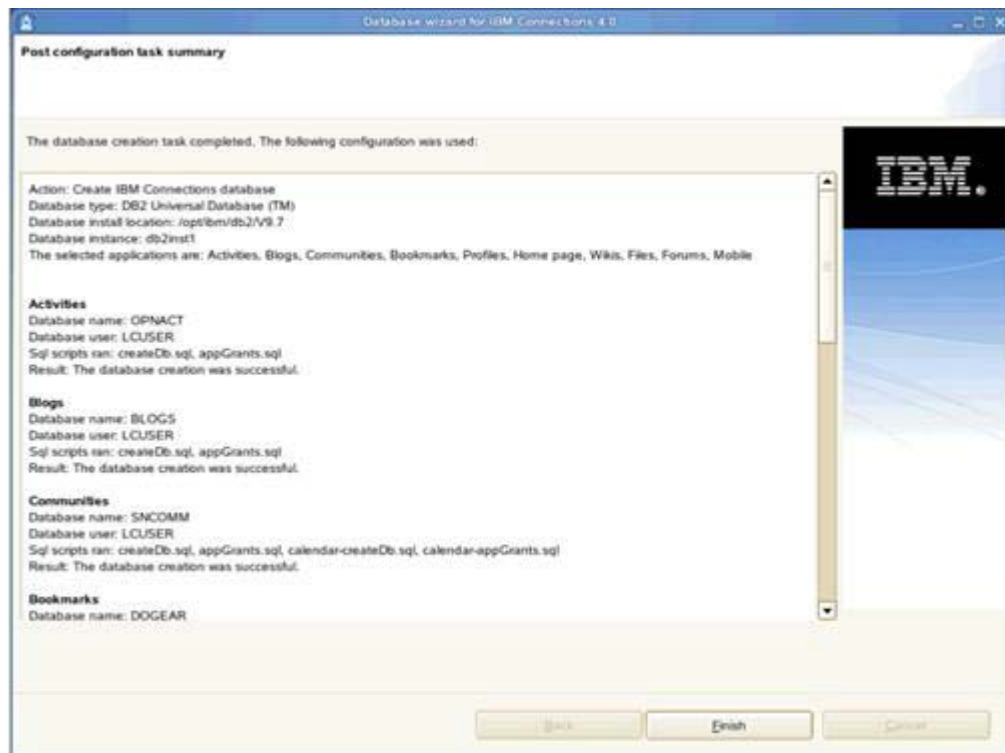


Figure 125. Database wizard for IBM Connections 4.0: Post configuration task summary

The databases are now created. If you run `db2 list database directory`, you should see that each database is created.

14. Configuring Tivoli Directory Integrator

IBM Tivoli Directory Integrator 7.1 installation

The installation of Tivoli Directory Integrator is needed so the profiles DB can be populated with LDAP information.

1. Copy the Tivoli Directory Integrator 7.1 installer to your computer, `CZ9MNML.tar`, and extract it. Start the launchpad by running `./launchpad.sh`. You see the welcome screen as in the following figure.



Figure 126. IBM Tivoli Directory Integrator 7.1 Launchpad: Welcome

- ___ 2. Click **Install IBM Tivoli Directory Integrator** from the launchpad and then **Tivoli Directory Integrator 7.1 Installer**.



Figure 127. IBM Tivoli Directory Integrator 7.1 Launchpad: Tivoli Directory Integrator 7.1 installer

___ 3. Select **English** as your language and click **OK**.

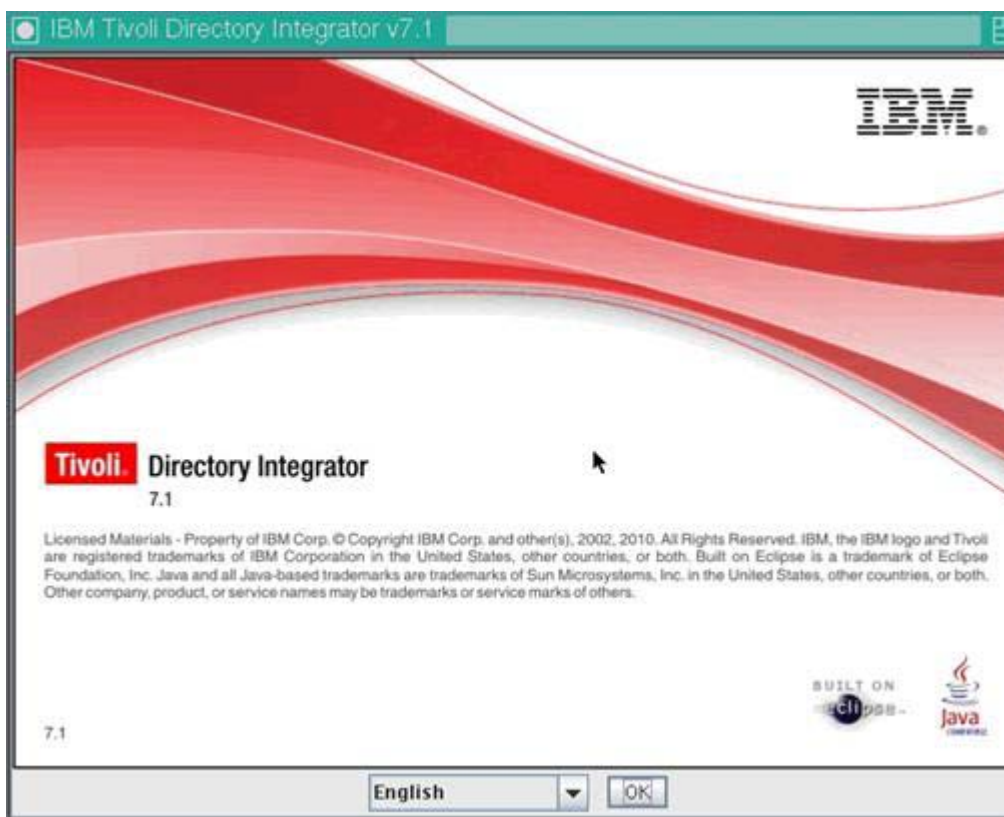


Figure 128. Selecting installation language

- ___ 4. In the introduction panel, click **Next**.

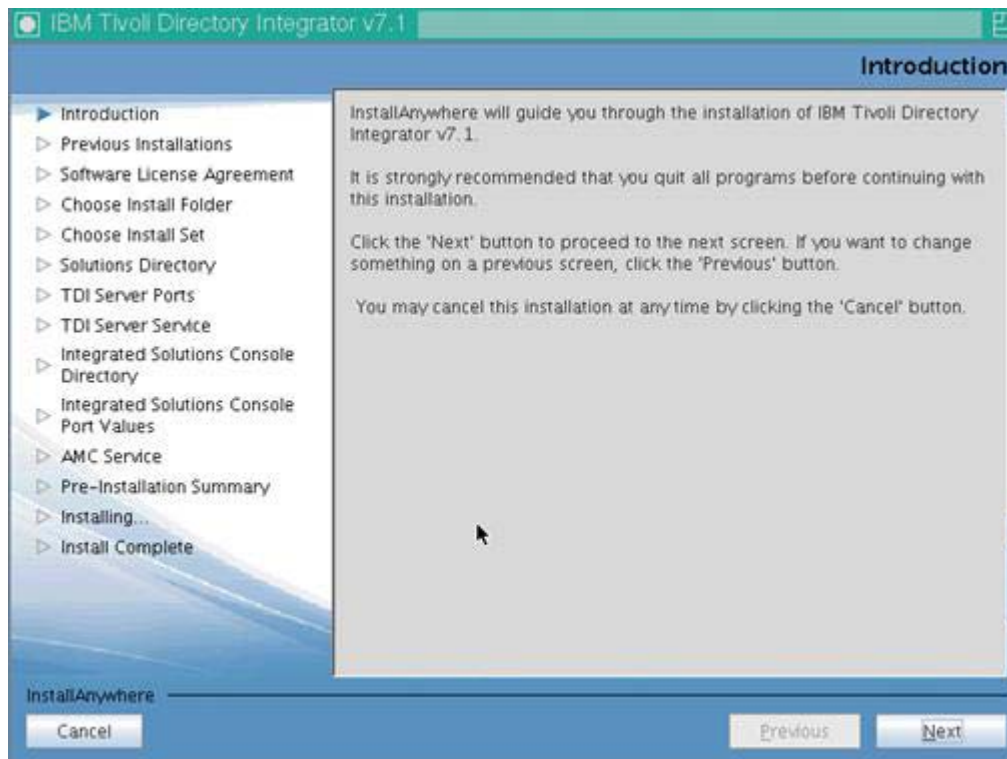


Figure 129. IBM Tivoli Directory Integrator v7.1: Introduction

5. You then see the following panel where the installation searches to see whether Tivoli Directory Integrator is already installed. Click **Next**.

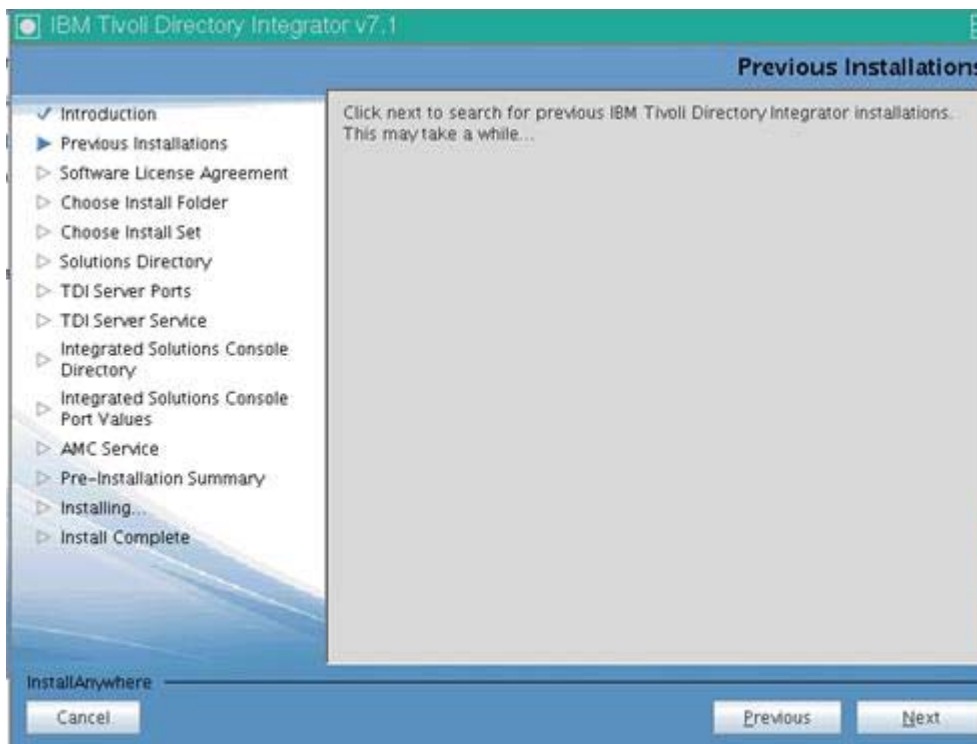


Figure 130. IBM Tivoli Directory Integrator v7.1: Previous installations

- ___ 6. After some time it finishes. Accept the license agreement and click **Next**.



Figure 131. IBM Tivoli Directory Integrator v7.1: Software License Agreement

- ___ 7. Change the path where Tivoli Directory Integrator is installed. Click **Next** to continue.

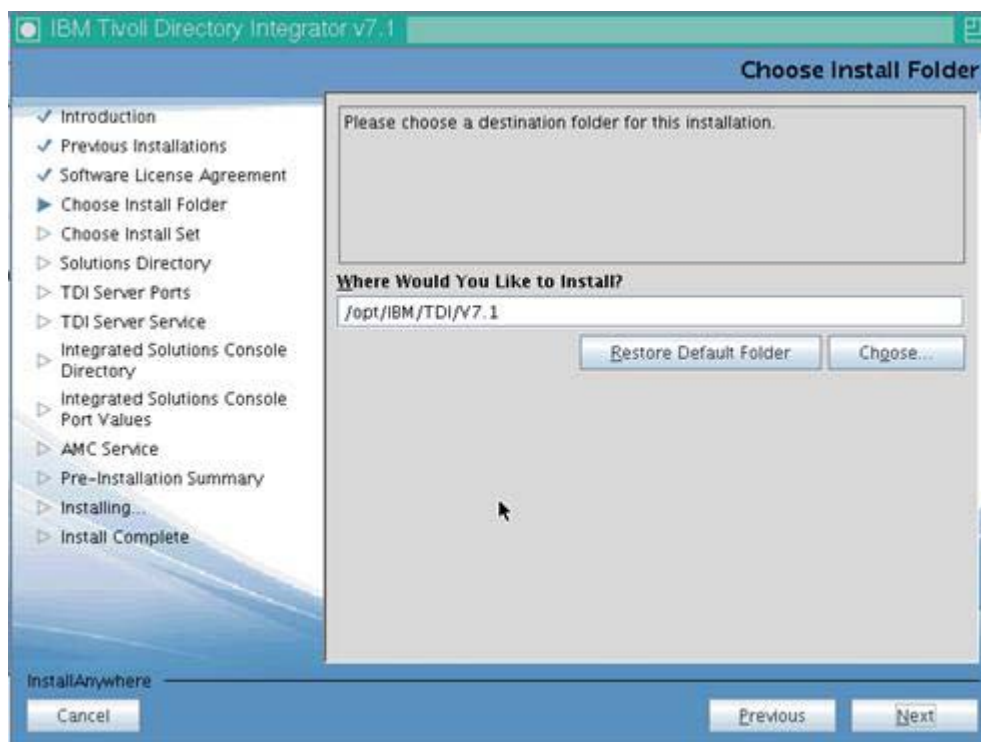


Figure 132. IBM Tivoli Directory Integrator v7.1: Choose Install Folder

___ 8. Choose the **Typical** installation type and **Next** to continue.



Figure 133. IBM Tivoli Directory Integrator v7.1: Choose Install Set

- ___ 9. Select “Do not specify: use current working directory at startup time” and click **Next** to continue.

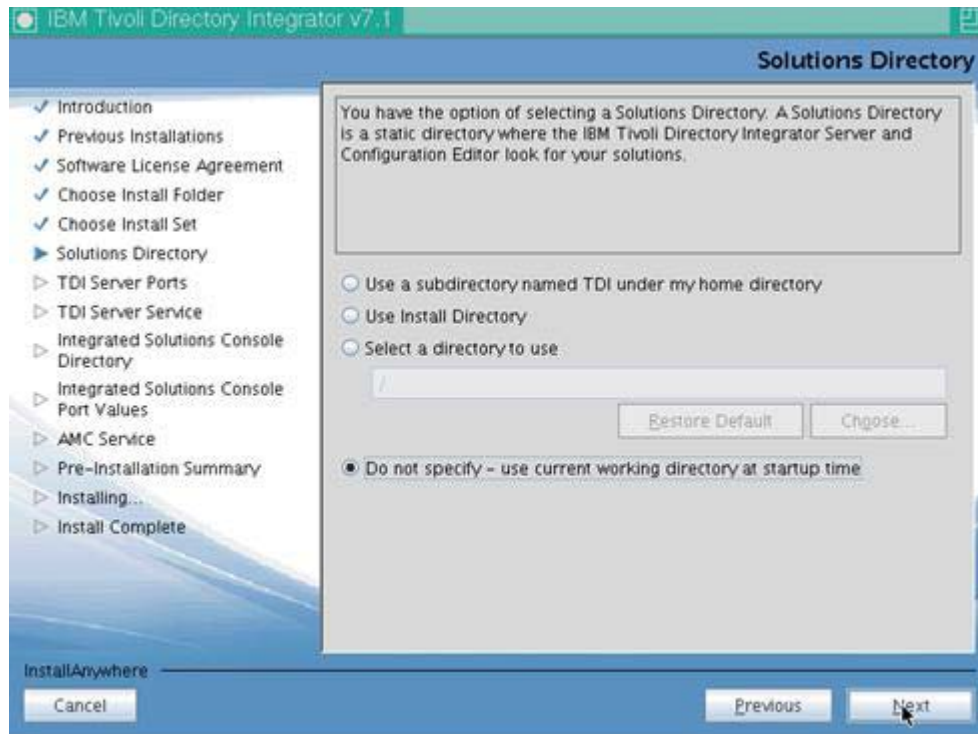


Figure 134. IBM Tivoli Directory Integrator v7.1: Solutions Directory

___ 10. Use the default ports and click **Next** to continue.

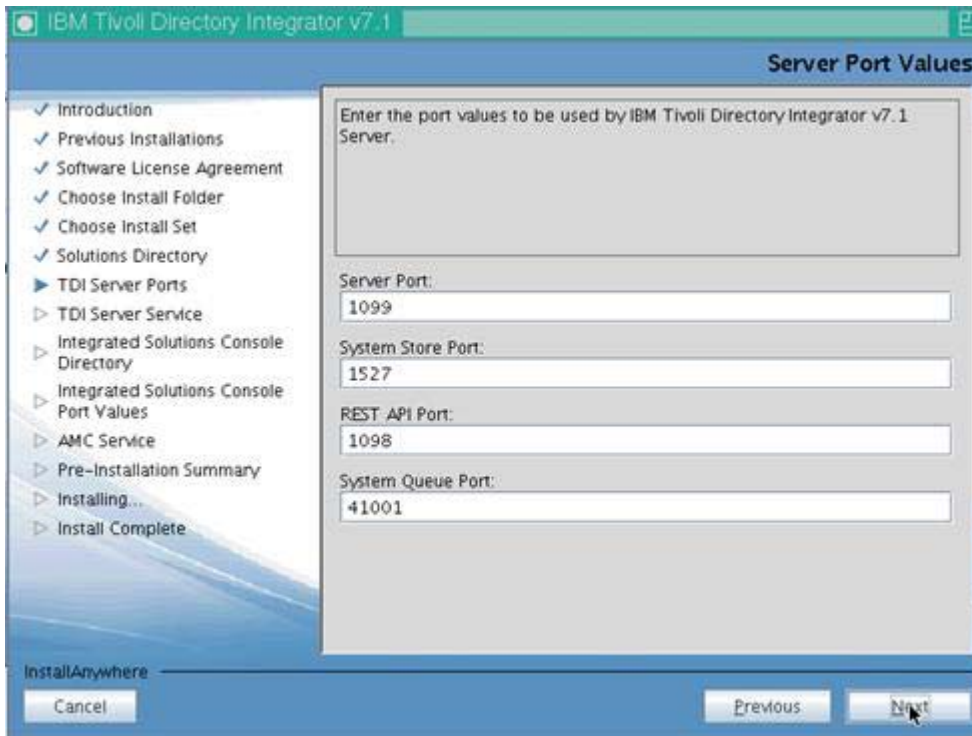


Figure 135. IBM Tivoli Directory Integrator v7.1: Server Port Values

___ 11. Do not select “Register as a system service. Click Next to continue.

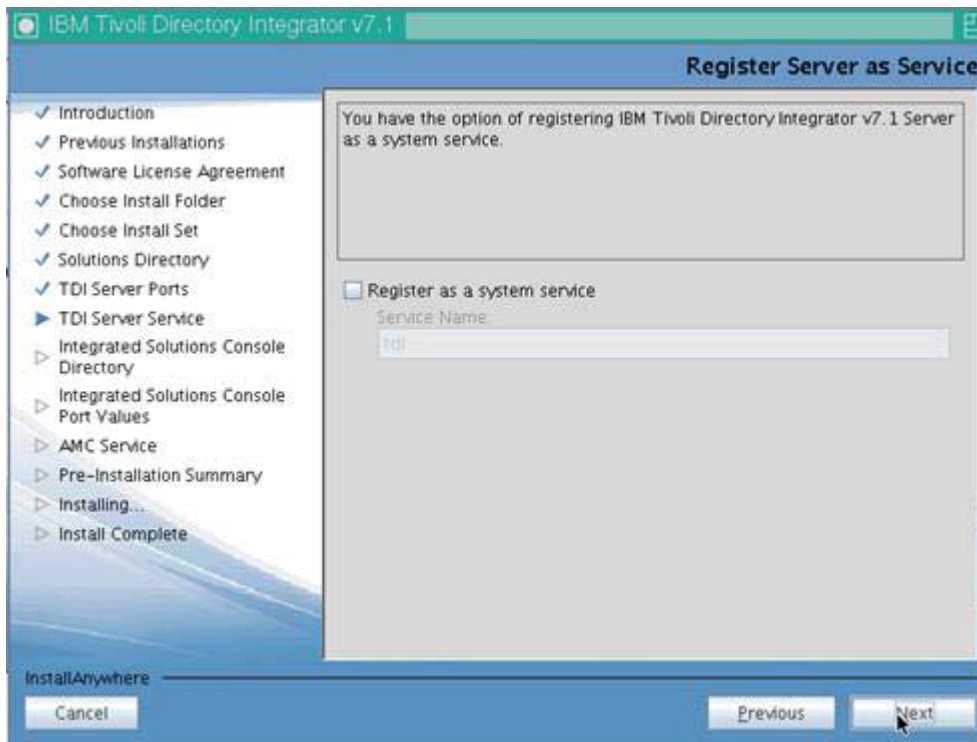


Figure 136. IBM Tivoli Directory Integrator v7.1: Register Server as Service

___ 12. Use the default ports and click **Next** to continue.

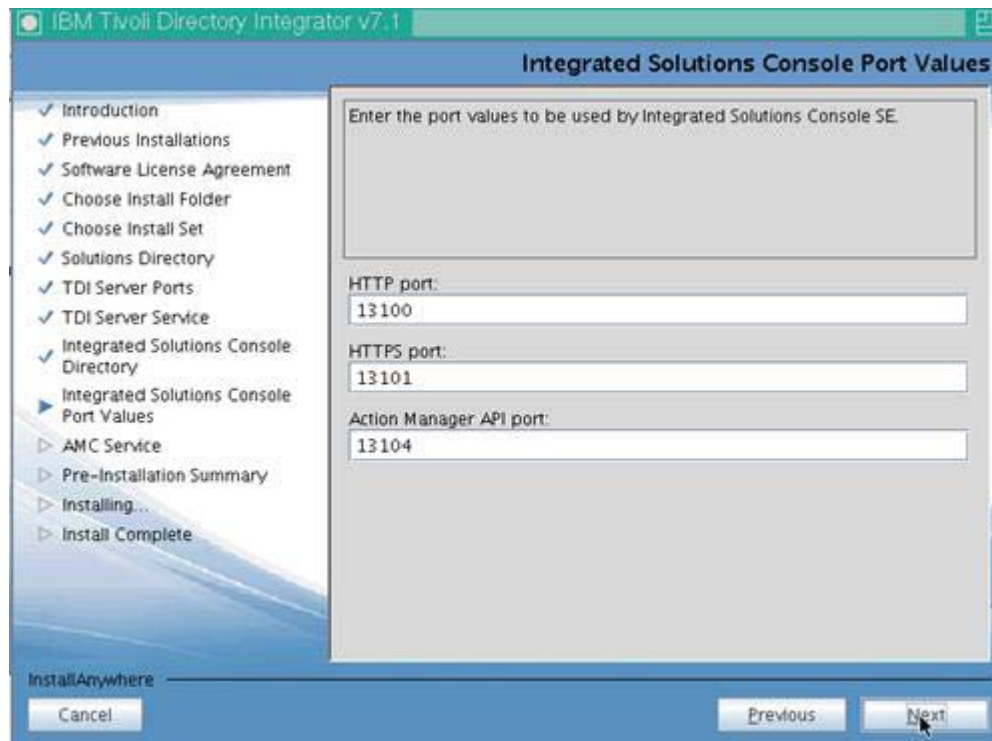


Figure 137. IBM Tivoli Directory Integrator v7.1: Integrated Solutions Console Port Values

___ 13. Do not select “Register as a system service”. Click **Next** to continue.

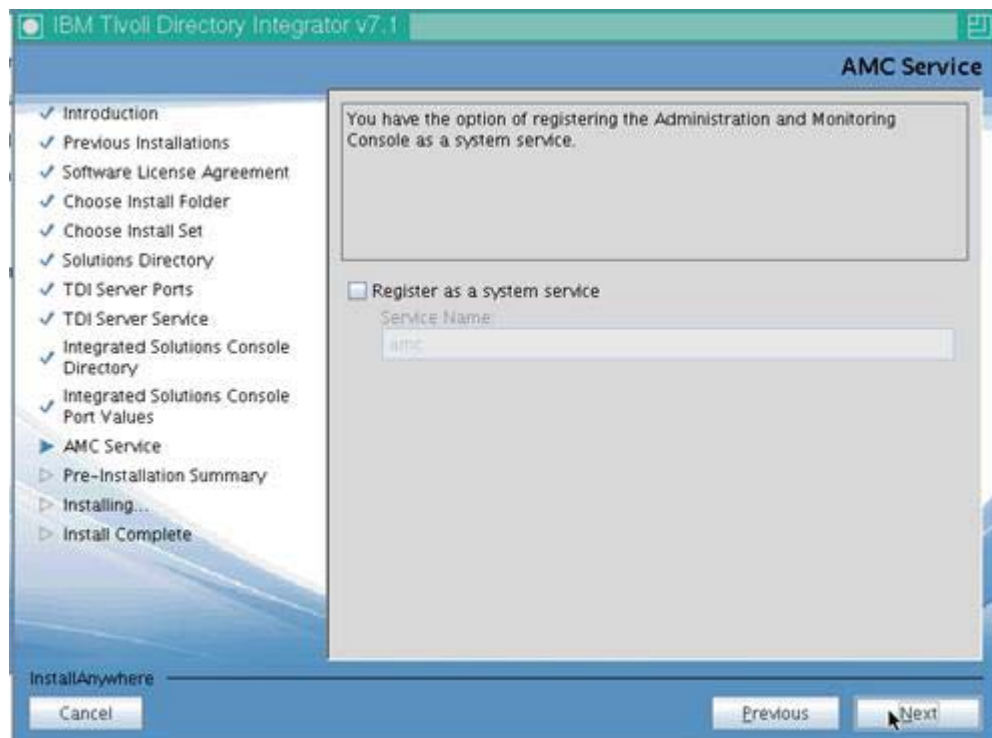


Figure 138. IBM Tivoli Directory Integrator v7.1: AMC Service

___ 14. A summary screen displays. Click **Next** to start the installation.

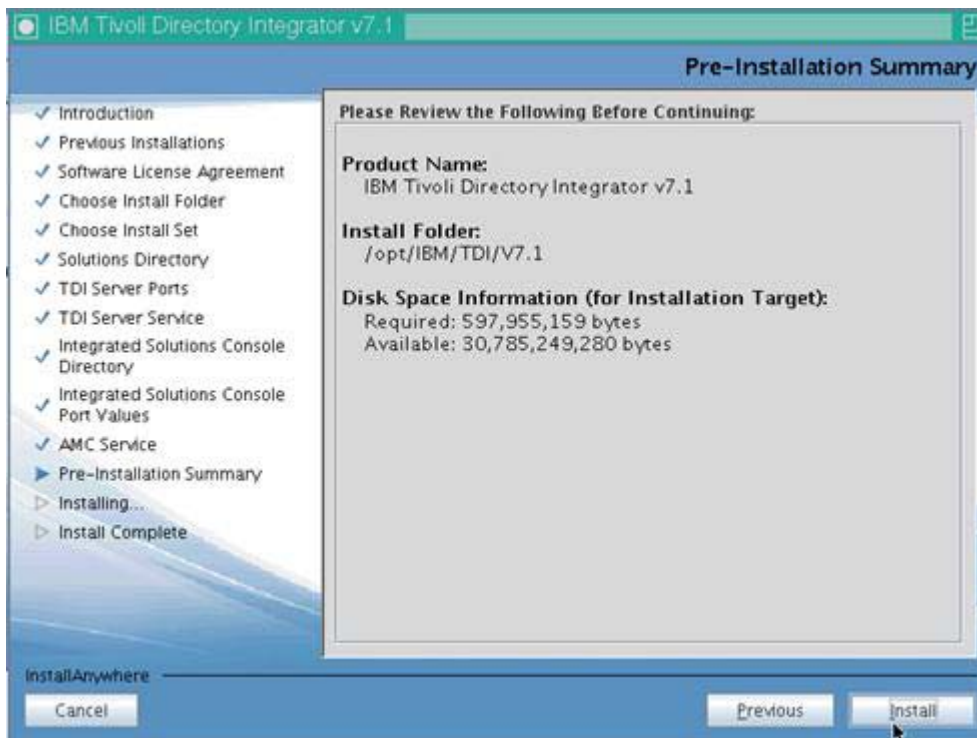


Figure 139. IBM Tivoli Directory Integrator v7.1: Pre-Installation Summary

The files are installed.

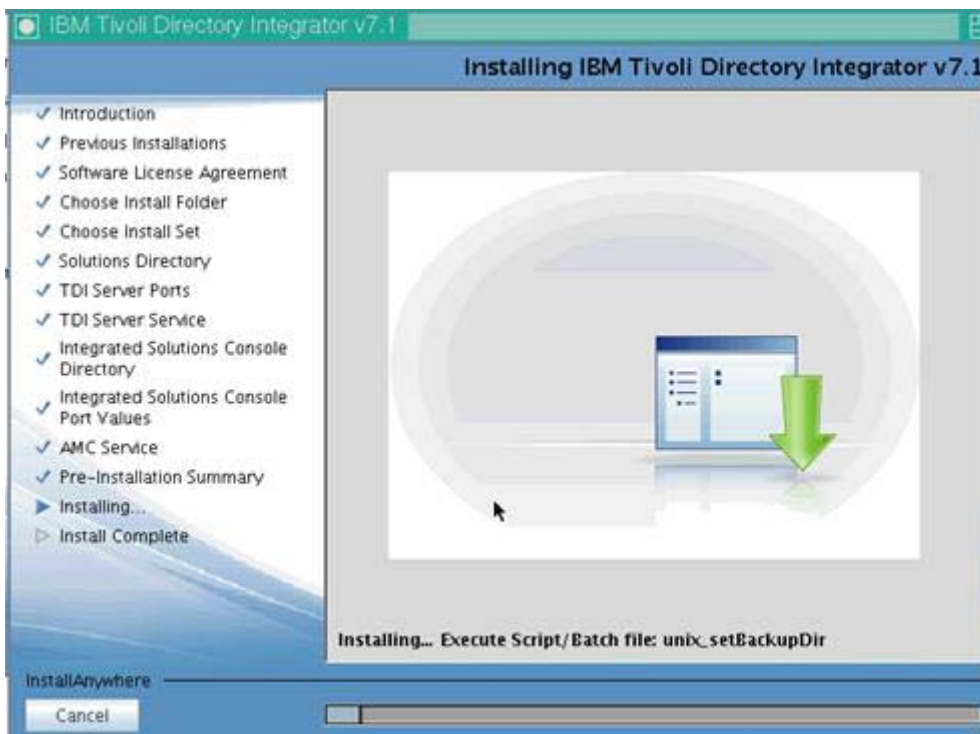


Figure 140. IBM Tivoli Directory Integrator v7.1: Installation in progress

- ___ 15. After some time the installation finishes. Clear the “Start Configuration Editor” check box and click **Finish** to close the installer.

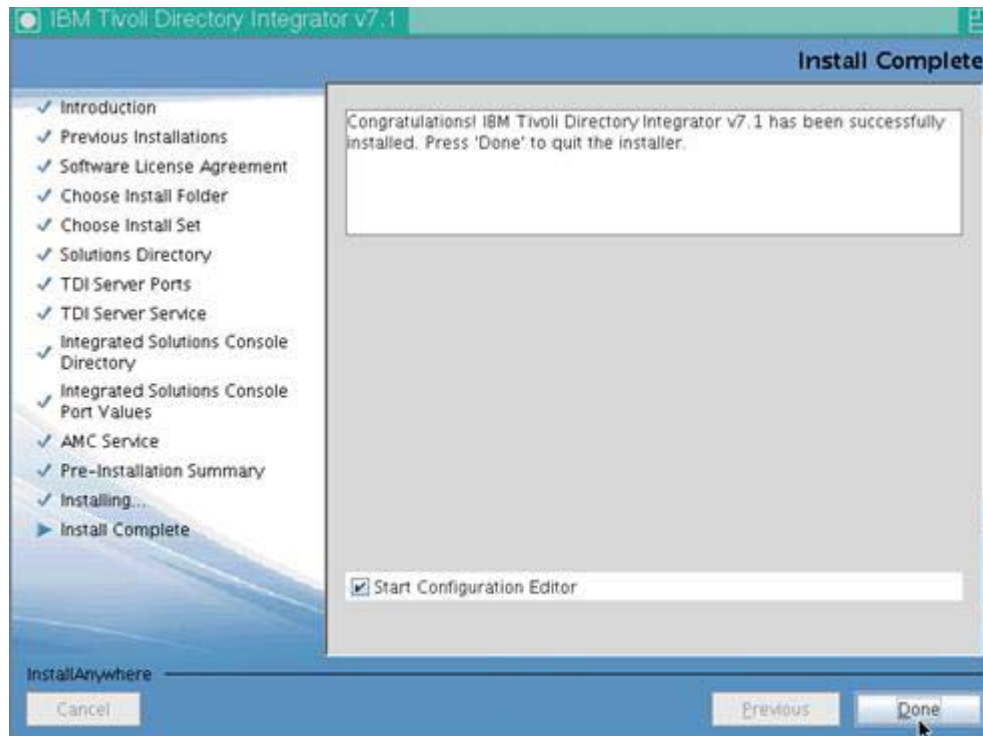


Figure 141. IBM Tivoli Directory Integrator v7.1: Installation complete

Tivoli Directory Integrator 7.1 is now installed. Now you need to install fix pack 5 on top of it.


IBM Tivoli Directory Integrator 7.1 FixPack 5 Installation

- ___ 1. Copy the fix pack to a location on your system. Extract the 7.1.0-TIV-TDI-FP0005.zip.
- ___ 2. Make sure Tivoli Directory Integrator is not running before applying the fix pack.
- ___ 3. The go to /opt/IBM/TDI/V7.1/bin and run the following command:

```
Export DISPLAY=db2server.machine.mul.ie.ibm.com:1.0.
```

```
./applyUpdates.sh -update /software/TDI
7.1/7.1.0-TIV-TDI-FP0005/TDI-7.1-FP0005.ZIP/
```

The FixPack is then installed.



```
[... bin]# ./applyUpdates.sh -update /software/TDI7.1/7.1.0-TIV-TDI-FP0
005/TDI-7.1-FP0005.zip
./applyUpdates.sh: line 57: -Dlog4j.configuration=file:/opt/IBM/TDI/V7.1/etc/upd
ateinstaller-log4j.properties: No such file or directory
log4j:WARN No appenders could be found for logger (UpdateInstaller.UpdateInstall
erMsgs).
log4j:WARN Please initialize the log4j system properly.
CTGDKO023I Applying fix 'TDI-7.1-FP0005' using backup directory '/opt/IBM/TDI/V7
se Agree
LICENSE
se/en_US
.1/maintenance/BACKUP/TDI-7.1-FP0005'.
CTGDKO027I Updating SERVER.
CTGDKO027I Updating CE.
CTGDKO027I Updating EXAMPLES.
074"
```

Figure 142. Running commands in /opt/IBM/TDI/V7.1/bin

- ___ 4. Check that the installation was OK. Run ./applyUpdates.sh -queryreg. It does report that FP3 is installed.



```
[... bin]# ./applyUpdates.sh -queryreg
./applyUpdates.sh: line 57: -Dlog4j.configuration=file:/opt/IBM/TDI/V7.1/etc/updateinstaller-log4j.properties: No such file
r directory
log4j:WARN No appenders could be found for logger (UpdateInstaller.UpdateInstallerMsgs).
log4j:WARN Please initialize the log4j system properly.
Information from .registry file in: /opt/IBM/TDI/V7.1
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
```

Figure 143. FP3 is installed

5. Make the database libraries available to Tivoli Directory Integrator by copying the `db2jcc.jar` and `db2jcc_license_cu.jar` files from the `java` subdirectory of the directory where you installed DB2 (`/opt/ibm/db2/V9.7/java`). Paste the files into the `jvm/jre/lib/ext` subdirectory of Tivoli Directory Integrator. If you installed Tivoli Directory Integrator in `/opt/IBM/TDI/V7.1`, the path would be `/opt/IBM/TDI/V7.1/jvm/jre/lib/ext`.

```

/opt/IBM/TDI/V7.1/jvm/jre/lib/ext # ls
CapCred.jar          db2jcc.jar          dtfj-interface.jar  gskitn.jar          libjccfipe.jar      libjccimpl.jar      jaccess.jar         salenrw.jar
IBMManagementServer.jar  db2jcc_license_cu.jar  dtfj.jar            healthcenter.jar    libjccprovider.jar  libmailprovider.jar  ldapview.jar
JavaDiagnosticCollector.jar  db2jcc.jar          dtfjview.jar        libcomprovider.jar  libjccvost.jar      libmailprovider.jar  localedata.jar
/opt/IBM/TDI/V7.1/jvm/jre/lib/ext #

```

Figure 144. Copying the `db2jcc.jar` and `db2jcc_license_cu.jar` files

Populate the Profiles database with LDAP user information



Note

Do it on the computer where you installed Tivoli Directory Integrator. In this example, it is on the db2 computer.

The population of the profiles DB with LDAP user can now be done with a wizard.

- ___ 1. Copy the `Lotus_Connections_4.0_wizards_lin_aix.tar` to your computer and extract it. Then, go into the wizard folder and run `./populationWizard.sh` to open the wizard. Click **Next** to continue.
- ___ 2. On the Welcome page of the wizard, click **Launch Information Center** to open the IBM Connections Information Center in a browser window. Click **Next** to continue.

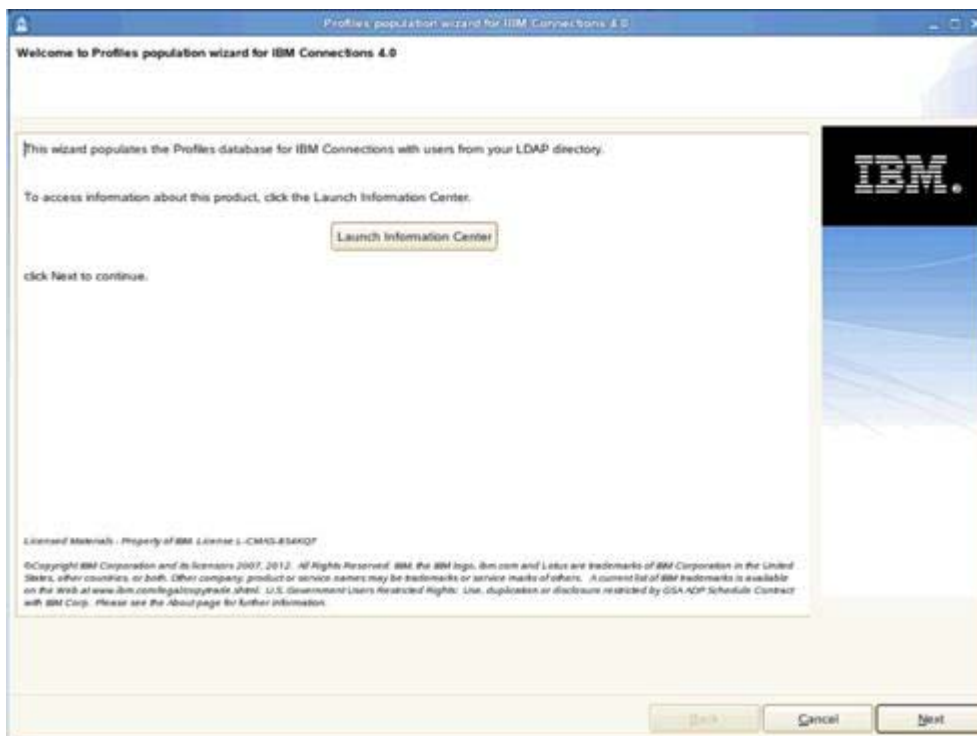


Figure 145. Profiles population wizard for IBM Connections 4.0: Welcome

- ___ 3. Select **Default settings** or, if you are resuming an earlier session, click **Last successful default settings** and click **Next**.



Note

This page is shown only if you already used the wizard to populate the Profiles database.

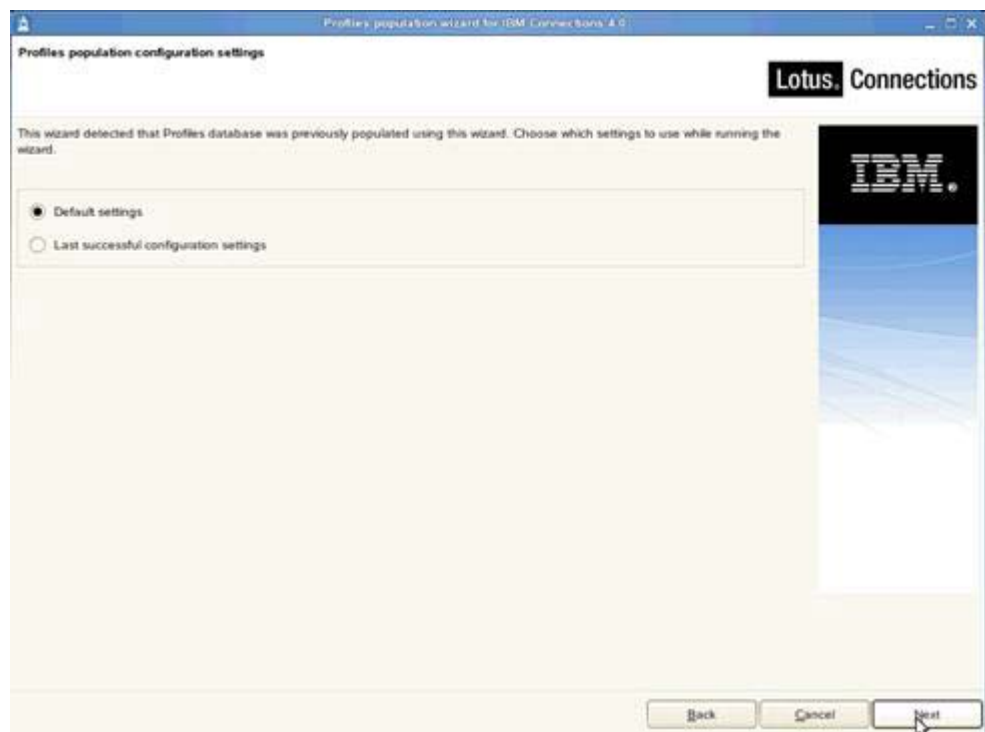


Figure 146. Profiles population wizard for IBM Connections 4.0: Profile population configuration settings

___ 4. Enter the location of Tivoli Directory Integrator and then click **Next**.



Note

This page is shown only if the wizard cannot automatically detect your Tivoli Directory Integrator directory.

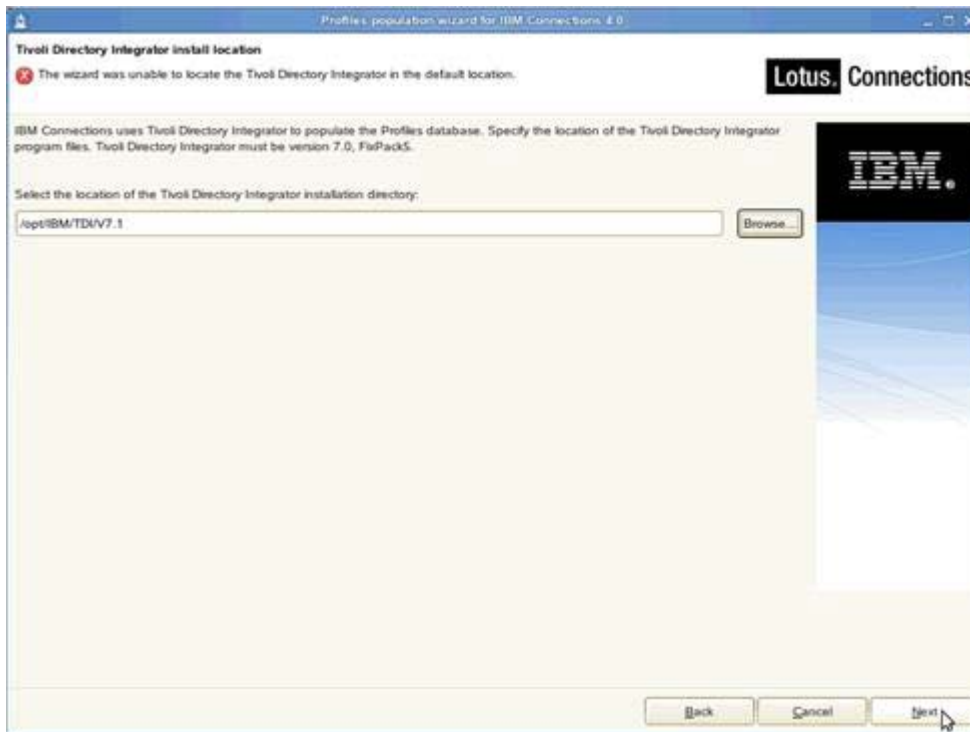


Figure 147. Profiles population wizard for IBM Connections 4.0: Tivoli Directory Integrator installation location

___ 5. Choose a database type and click **Next**.

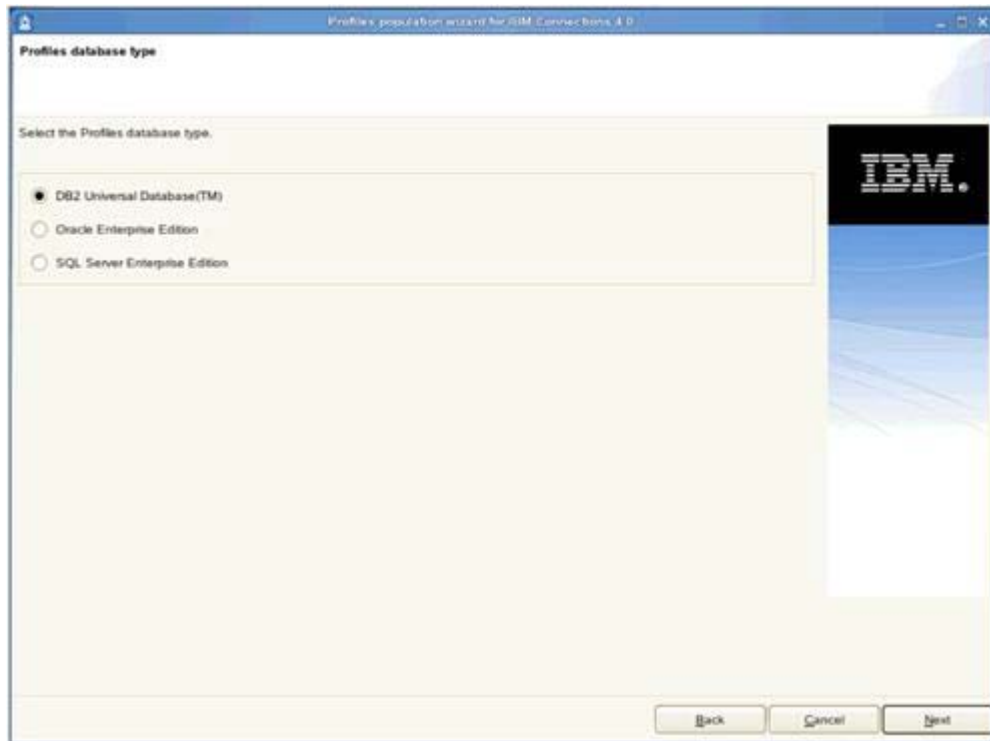


Figure 148. Profiles population wizard for IBM Connections 4.0: Profile database type

- ___ 6. Next, enter the database information for where your PEOPLEDB database is located and click **Next** to continue.

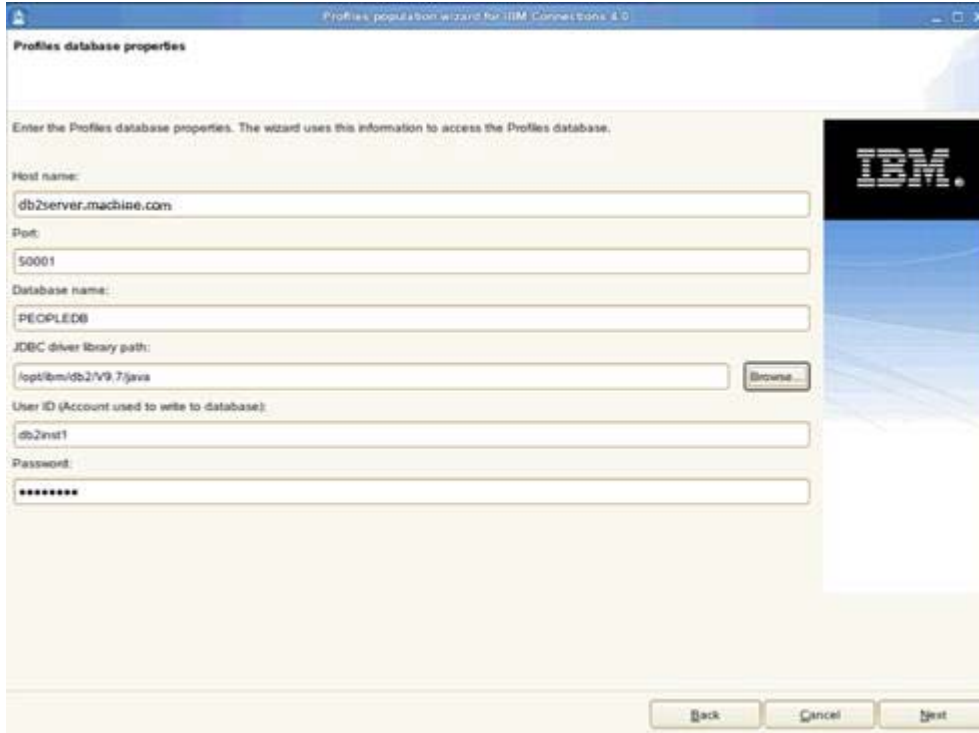


Figure 149. Profiles population wizard for IBM Connections 4.0: Profile database properties

- ___ 7. Enter your LDAP server and port and then click **Next** to continue.

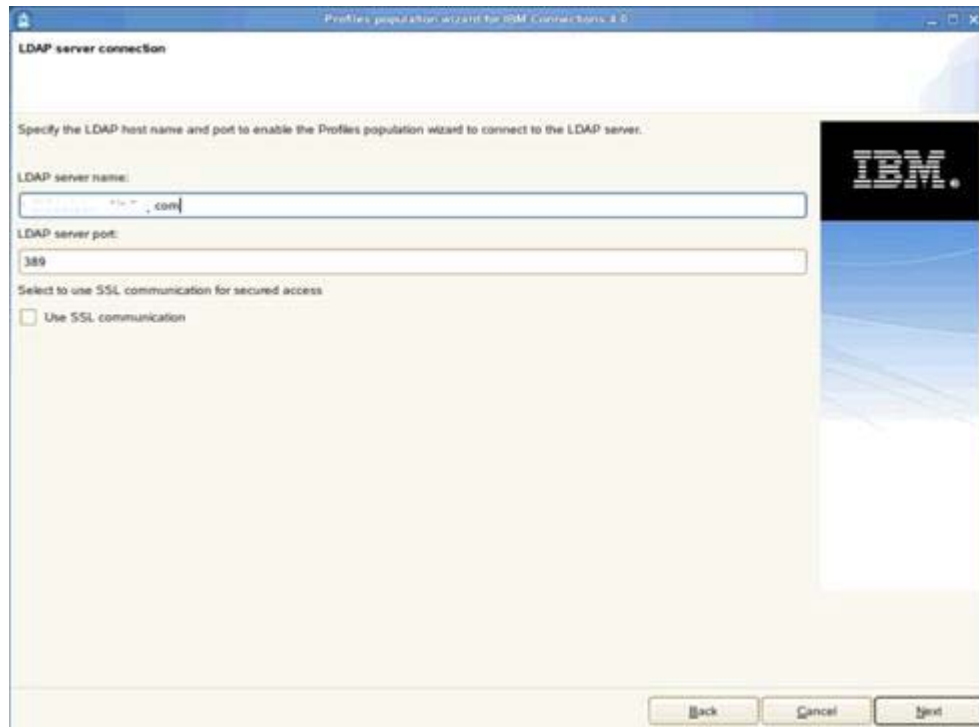


Figure 150. Profiles population wizard for IBM Connections 4.0: LDAP server connection

- ___ 8. You are then asked about your bind user. Enter a bind distinguished name and password and click **Next** to continue.

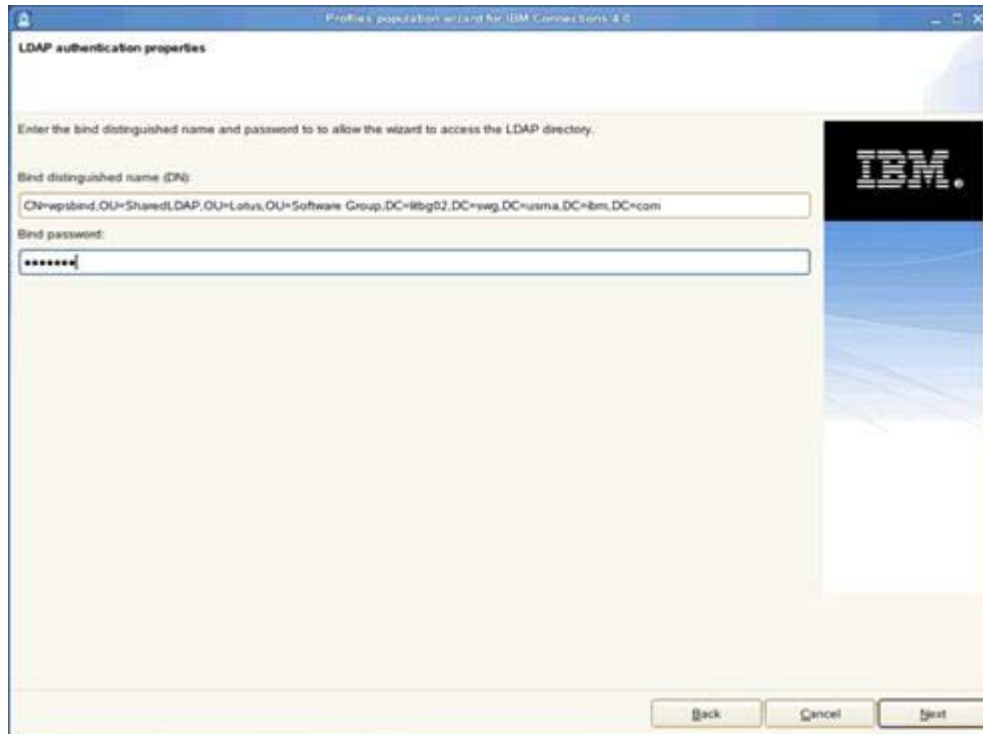


Figure 151. Profiles population wizard for IBM Connections 4.0: LDAP authentication properties

___ 9. Enter the search base and search filter. Click **Next** to continue.

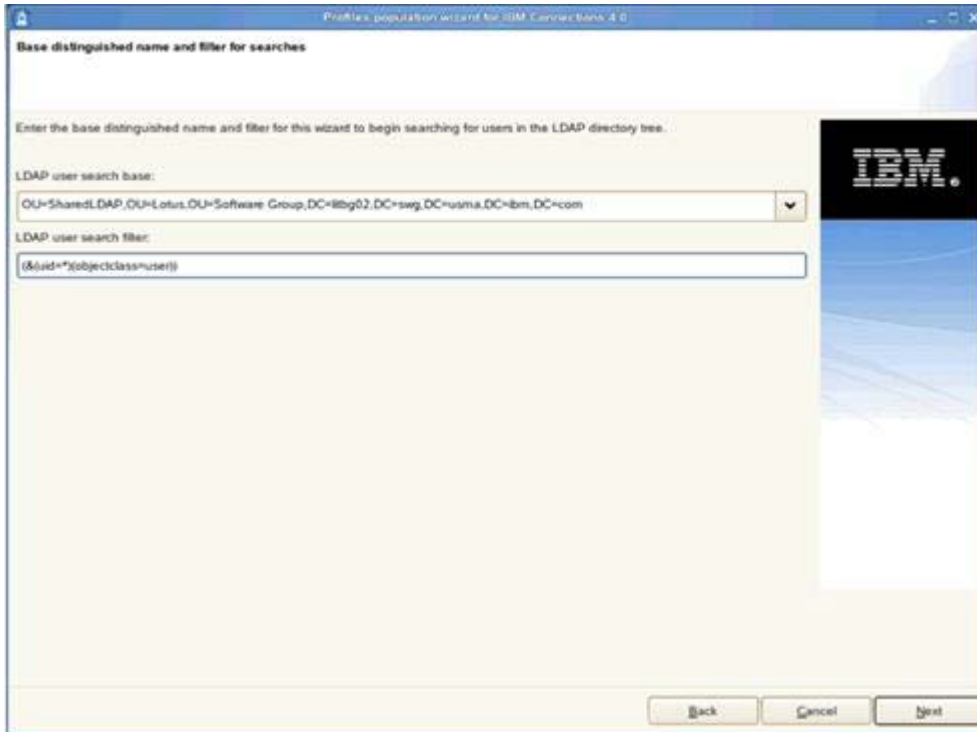


Figure 152. Profiles population wizard for IBM Connections 4.0: Base distinguished name and filter for searches

___ 10. Select the default database mappings for this example. Click **Next** to continue.

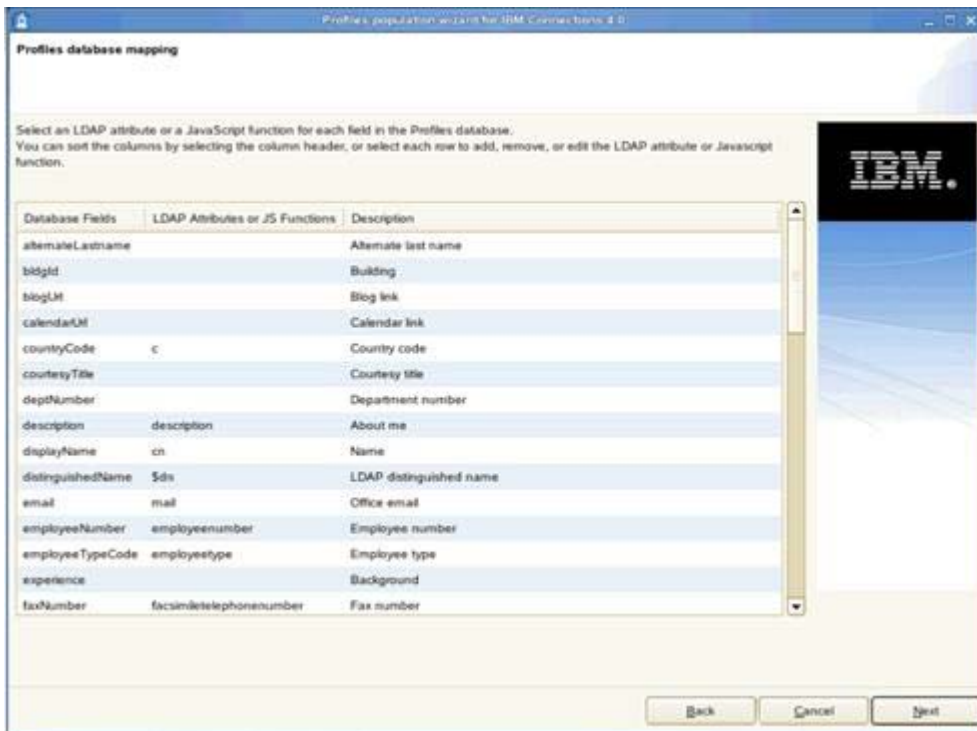


Figure 153. Profiles population wizard for IBM Connections 4.0: Profiles database mapping

___ 11. Do not select any of the optional database tasks. Then, click **Next** to continue.

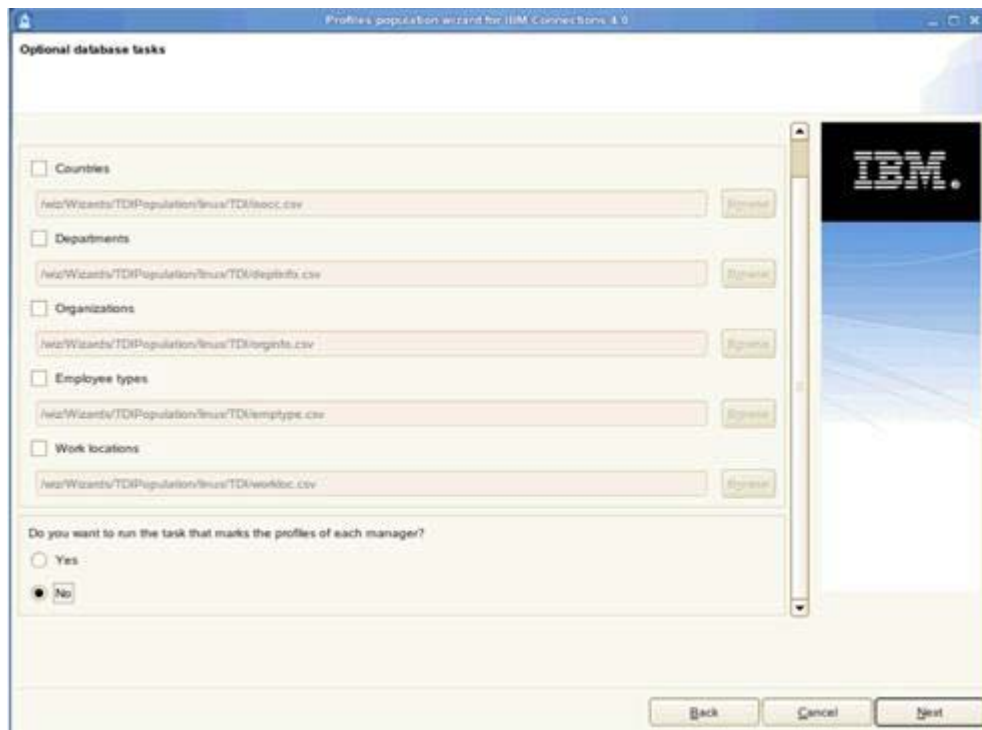


Figure 154. Profiles population wizard for IBM Connections 4.0: Optional database task

12. Review the summary panel to ensure that the information that you entered in the previous panels is correct. To make changes, click **Back** to return to the relevant page and edit the information. Otherwise, click **Configure** to begin populating the database.

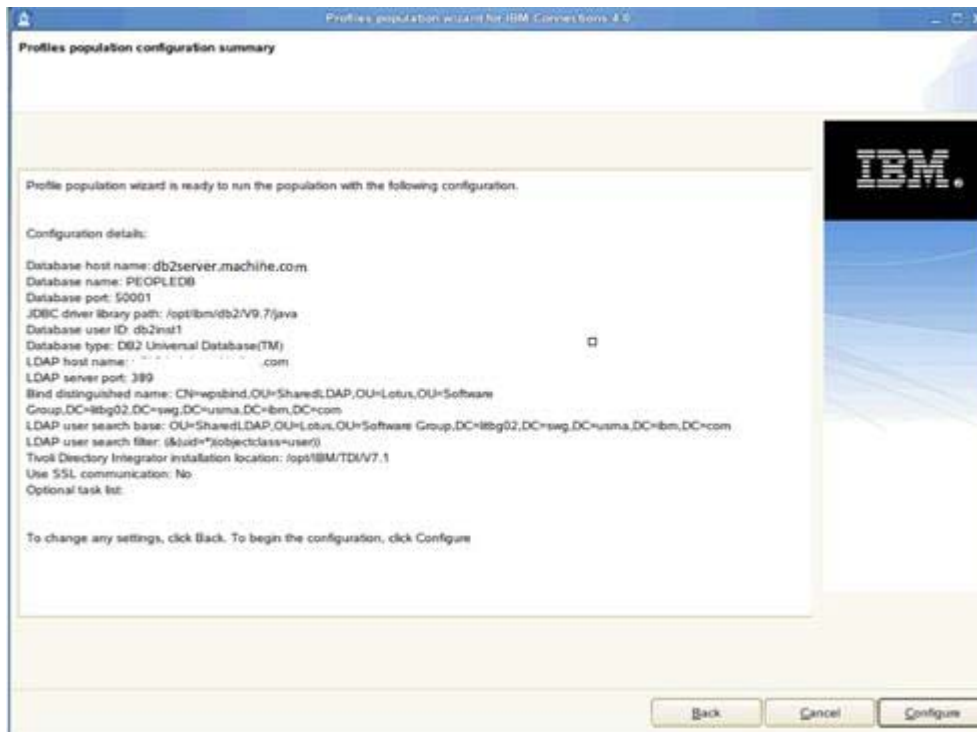


Figure 155. Profiles population wizard for IBM Connections 4.0: Profiles population configuration summary

The population task starts to run.

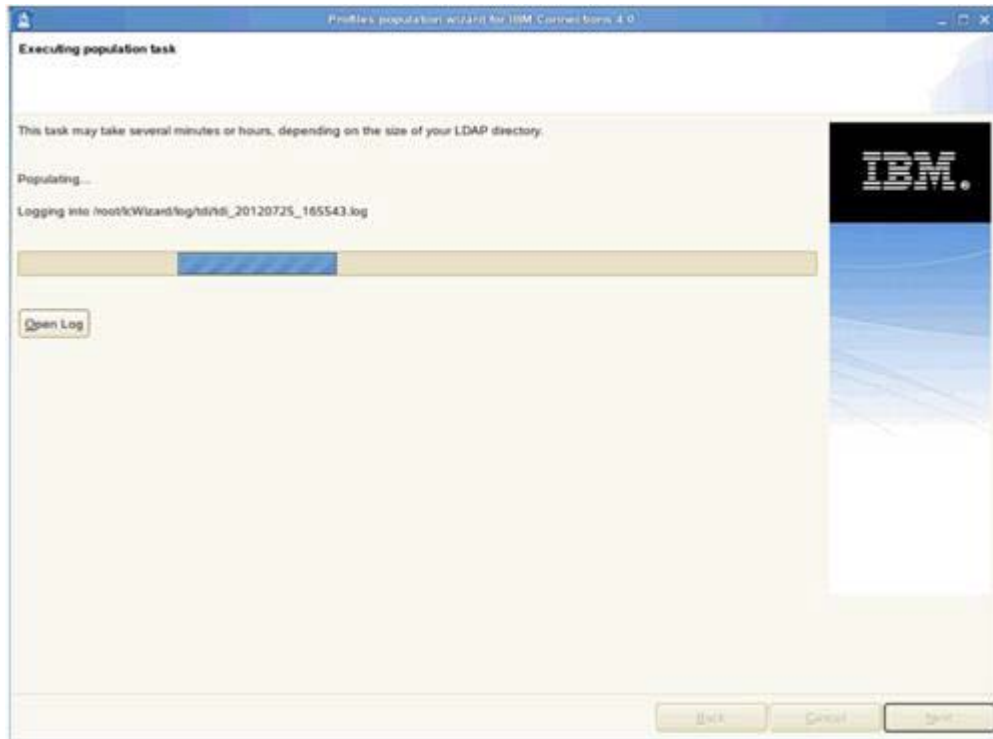


Figure 156. Profiles population wizard for IBM Connections 4.0: Running population task

13. When it completes, you see a completion summary. This task can take a long time (3 - 4 hours), so tail the previous log which is being referenced. Click **Finish** to exit the wizard.



Figure 157. Profiles population wizard for IBM Connections 4.0: Population completion summary

Setup of an NFS server on SUSE: Shared area needed

In a multi-node cluster, you must configure network share directories for content stores. When using NFS, use NFS v4 because NFS v3 lacks advanced locking capability.



Linux

On Linux, the easiest way to do it is to set up an NFS share on a computer (such as your Deployment Manager) and then map that on each node.

Here is how to do it.

- __ 1. Share out a folder on an NFS v4 Server:
 - __ a. Create a folder on the system where you want to share the folder. For example, create a share that is called `LC_Share` within the `/opt/IBM/LC_Share` directory on `dm&IBM HTTP Server.machine.com`.
 - __ b. Give full read/write access to this folder, `chmod -R 777 /opt/IBM/LC_Share`.

With NFS v4 you can export just one file system, so all the folders you need to mount on the clients should be under this one.

Server config: (Deployment Manager)

- __ 1. Edit the Export file:
 - __ a. `#vi /etc/exports.`
 - __ b. Add the following line:


```
/<folder_to_export>
*(fsid=0,rw,insecure,no_subtree_check,no_wdelay,sync,no_root_squash).
```
 - __ c. Save and Close.

```

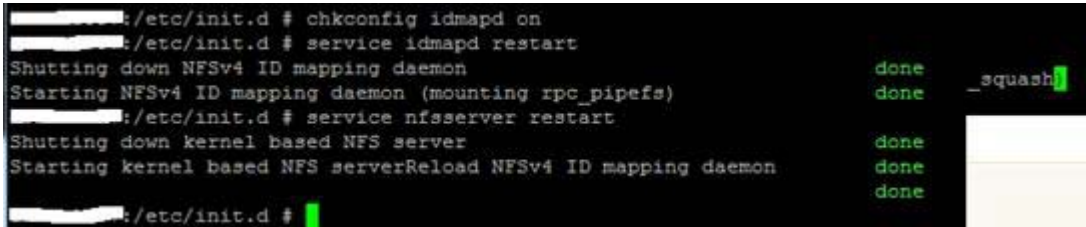
root@dm:~ # vi /etc/exports
/opt/IBM/LC_Share *(fsid=0,rw,insecure,no_subtree_check,no_wdelay,sync,no_root_squash)

```

Figure 158. Editing the export file

- __ 2. Activate `idmapd/nfs`:
 - __ a. `#chkconfig idmapd on.`

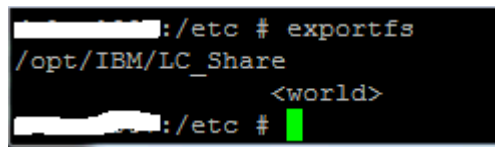
- ___ 3. Restart the services:
 - ___ a. # service idmapd restart.
 - ___ b. # service nfsserver restart.



```
_____: /etc/init.d # chkconfig idmapd on
_____: /etc/init.d # service idmapd restart
Shutting down NFSv4 ID mapping daemon           done
Starting NFSv4 ID mapping daemon (mounting rpc_pipefs) done  _squash
_____: /etc/init.d # service nfsserver restart
Shutting down kernel based NFS server           done
Starting kernel based NFS serverReload NFSv4 ID mapping daemon done
_____: /etc/init.d #
```

Figure 159. Restarting the services

- ___ 4. Check the exports:
 - ___ a. # exportfs.
 - ___ b. If everything goes well, you should see this message: /<folder_to_export> <world>.



```
_____: /etc # exportfs
/opt/IBM/LC_Share
                <world>
_____: /etc #
```

Figure 160. Checking the exports

Client configuration (Node 1)

- ___ 1. Make sure that idmapd service is enabled and started
 - ___ a. #chkconfig idmapd on.
 - ___ b. #service idmapd restart.
- ___ 2. Test manual mount by using nfs version 4:
 - ___ a. #mount -t nfs4 <nfs_server>:/ /<mount_point_on_client>.
- ___ 3. Update the /etc/fstab as follows:
 - ___ a. #vi /etc/fstab.
 - ___ b. Add the following line:

```
<nfs_server>:/ /<mount_point_on_client> nfs4
rszise=32768,wszise=32768,intr,noatime 0 1
```
- ___ 4. Mount the remote file system.

___ 5. #mount <nfs_server>:/

```
_____: /etc/init.d # chkconfig idmapd on
_____: /etc/init.d # service idmapd restart
Shutting down NFSv4 ID mapping daemon
Starting NFSv4 ID mapping daemon (mounting rpc_pipefs)
_____: /etc/init.d #
_____: /etc/init.d # cd /
_____: / # mount -t nfs4 _____: /opt/IBM/LC_Share
_____: / # vi /etc/fstab
_____: / # mount _____:/
mount: _____:/ already mounted or /opt/IBM/LC_Share busy
mount: according to mtab, _____:/ is already mounted on /opt/IBM/LC_Share
_____: / #
```

Figure 161. #mount <nfs_server>

___ 6. Repeat the same previous client configuration steps on Node 2.

15. Installation of Connections 4.0

The installation of Lotus Connections 4.0 is done on the Deployment Manager computer and then synched with the nodes.

Make sure that your Deployment Manager is started and On each node, stop all running instances of WebSphere Application Server and WebSphere node agents.

If you are installing the Metrics application, ensure that you installed and configured Cognos.

Ensure that the directory paths that you enter contain no spaces.

Ensure that the Open File Descriptor limit is 8192.

Follow these steps for how to set the limit:

- ___ 1. Open a command line and enter the following command to find the current open file limit:
ulimit -n.
- ___ 2. Add the following line to the user's profile file: ulimit -n 8192.

```

[redacted]:~ # cat .profile
export LD_LIBRARY_PATH=/usr/local/staf/lib
export LD_LIBRARY_PATH=/usr/local/staf/lib      :e

ulimit -n 8192                                busy
                                              i on /opt/IBM/LC_Share

```

Figure 162. User's profile file

```

[redacted]:~ # ulimit -a
core file size          (blocks, -c) 0
data seg size           (kbytes, -d) unlimited
file size               (blocks, -f) unlimited
pending signals         (-i) 31582
max locked memory       (kbytes, -l) 32
max memory size         (kbytes, -m) unlimited
open files              (-n) 8192
pipe size               (512 bytes, -p) 8
POSIX message queues    (bytes, -q) 819200
stack size              (kbytes, -s) 8192
cpu time                (seconds, -t) unlimited
max user processes      (-u) 31582
virtual memory          (kbytes, -v) unlimited
file locks              (-x) unlimited
[redacted]:~ #

```

Figure 163. User's profile file: ulimit -n 8192



Reminder

Check that the previous steps on Node1 and Node 2 as well.

- ___ 3. Ensure that the GTK library is available on your system. If you are installing on a 64-bit system, you also need the 32-bit version of the GTK library.



Reminder

Check on Deployment Manager, Node 1, and Node 2 as well.

```
ds1vm1007:/ # rpm -ra | grep -i gtk
rpm: arguments to --root (-r) must begin with a /
ds1vm1007:/ # rpm -qa | grep -i gtk
gtk-engines-0.12-982.4.1
gtk2-engines-32bit-2.6.7-17.2
gtk-sharp2-2.8.3-43.10
gtk-32bit-1.2.10-907.11
gtk-sharp2-32bit-2.8.3-43.10
python-gtk-2.8.2-21.2
firefox3-gtk2-2.10.6-0.8.27
gtk-1.2.10-907.11
gtksourceview-1.5.6-18.2
gtkspell-2.0.11-20.11
gtk2-2.8.11-0.27.11
firefox3-gtk2-32bit-2.10.6-0.8.27
gtk-engines-32bit-0.12-982.4.1
gtk2-engines-2.6.7-17.2
gtk2-32bit-2.8.11-0.27.11
gtk2-themes-0.1-653.2
gtkhtml2-3.10.0-15.23
```

Figure 164. GTK library

- ___ 4. Copy the installation files to your computer and extract the Lotus_Connections_4.0_lin_aix.tar file. Start the installation by running the ./launchpad.sh under Lotus_Connections_Install. The following panel is displayed.

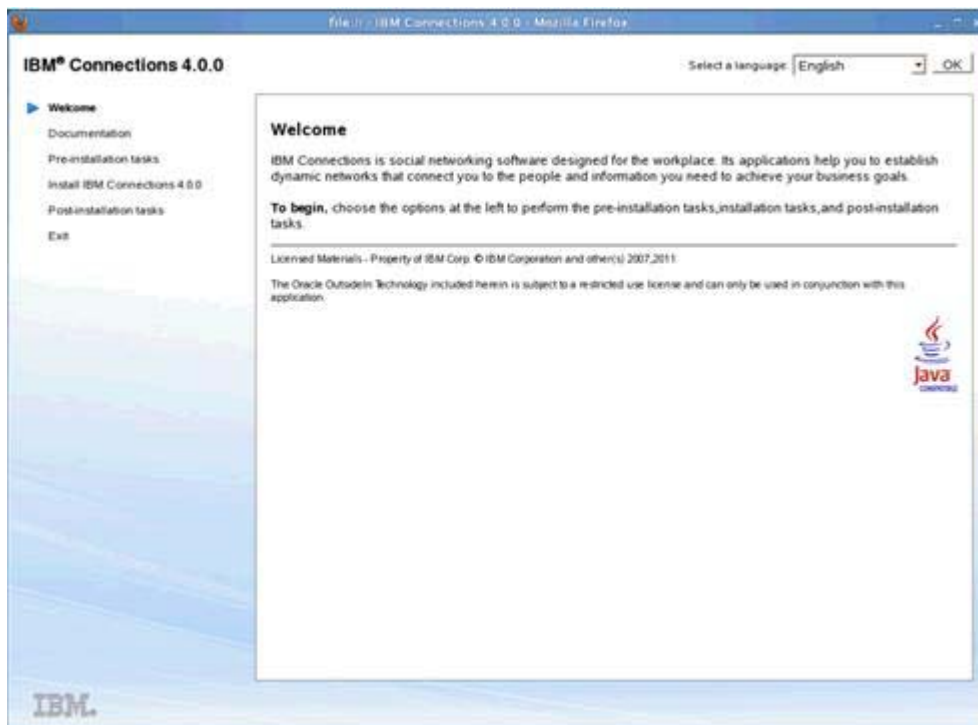


Figure 165. IBM Connections 4.0.0: Welcome

5. In the left pane of the launchpad, click **Install IBM Connections 4.0.0** and then click **Launch the IBM Connections 4.0** installation wizard in the right pane.



Figure 166. IBM Connections 4.0.0: Install IBM Connections 4.0.0

6. In the Select packages to install window, select the packages that you want to install and click **Next** to continue.

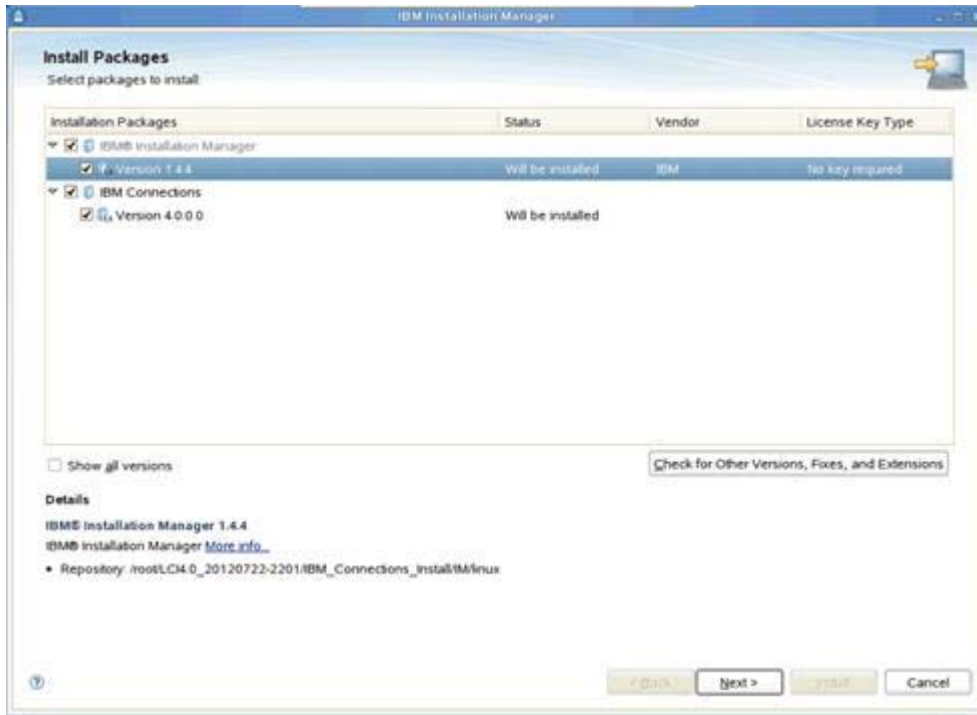


Figure 167. IBM Connections 4.0.0: Install Packages

7. Review and accept the license agreement by clicking “I accept the terms in the license agreements”. Click **Next**.

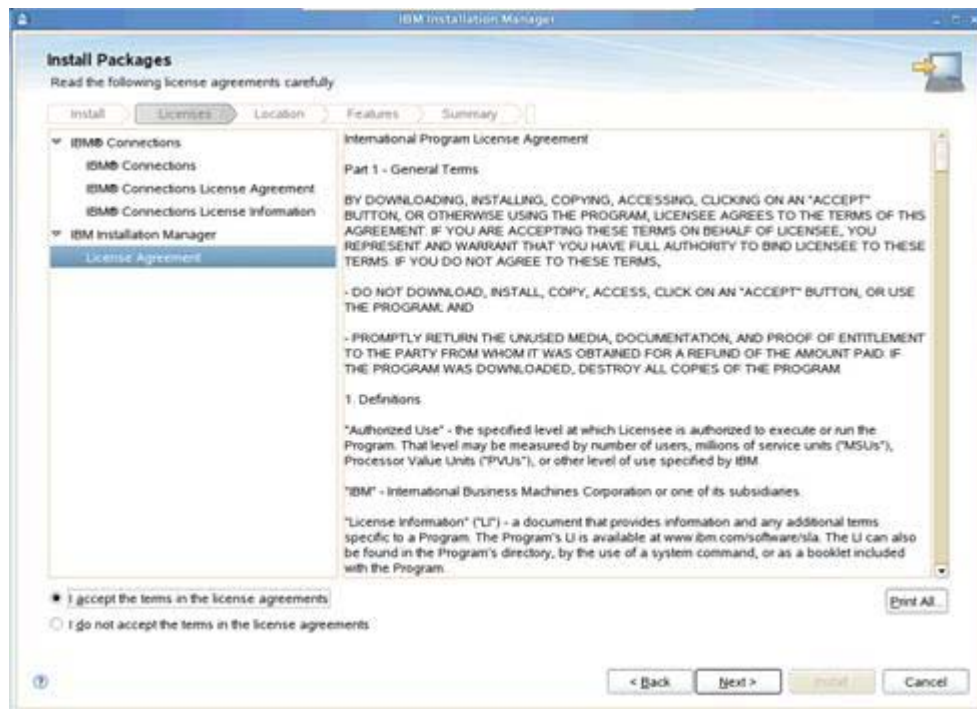


Figure 168. IBM Connections 4.0.0: License agreement

- ___ 8. Specify the location of shared directories for IBM Installation Manager. Click **Next** to continue.

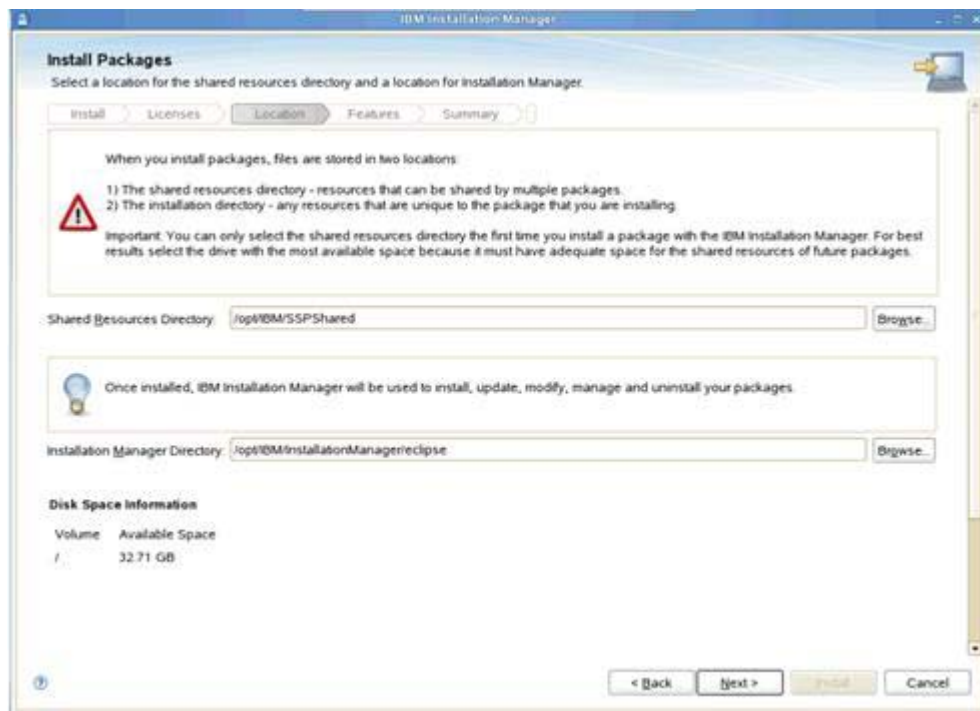


Figure 169. IBM Connections 4.0.0: Shared directories for IBM Installation Manager

- ___ 9. Choose **Use the existing package group** or **Create a new package group**. Select **Next** to continue.



Note

If you are using the wizard for the first time, the “Use the existing package group” option is not available.

- 10. Specify the location of the installation directory for IBM Connections. You can accept the default directory location, or enter a new directory name, or click **Browse** to select an existing directory. Click **Next**.

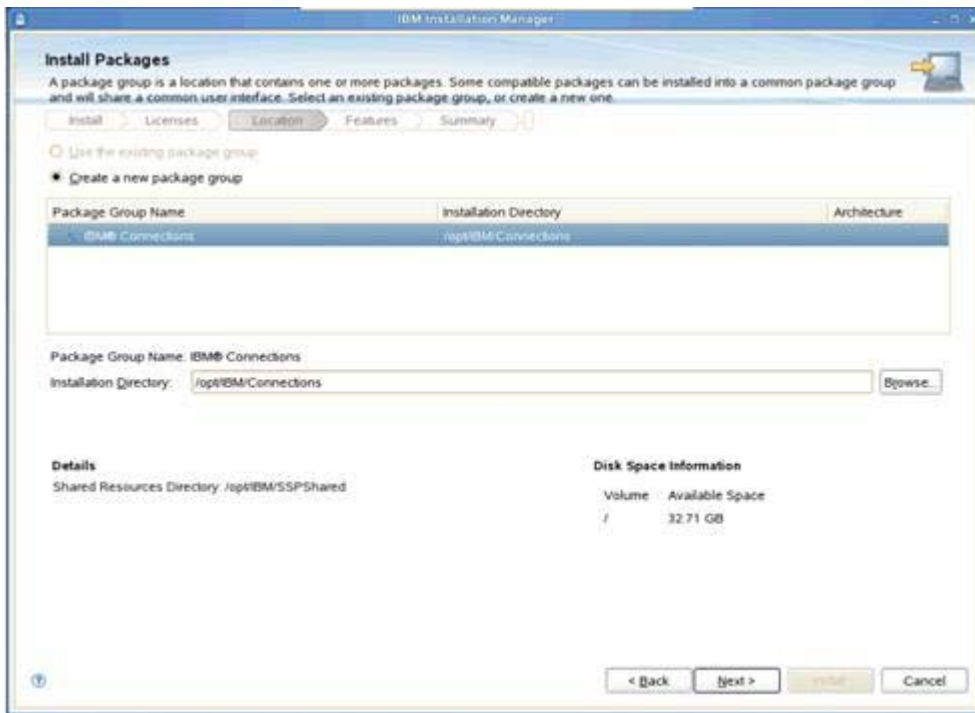


Figure 170. IBM Connections 4.0.0: Installation directory

- 11. Confirm the applications that you want to install and click **Next** to continue.

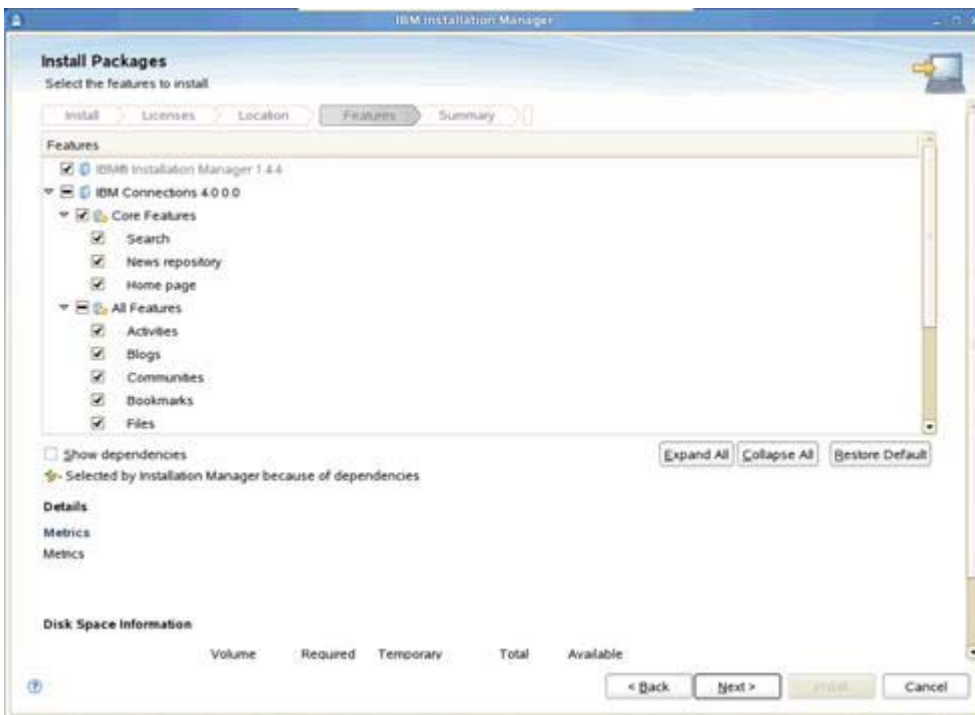


Figure 171. IBM Connections 4.0.0: Applications to install

- ___ 12. Select the path to the WebSphere Application Server instance that runs on your deployment manager. In this example, it was under `/opt/IBM/WebSphere/DeploymentManager`. Enter the host name, wasadmin user, and password and then click **Validate** at the bottom.

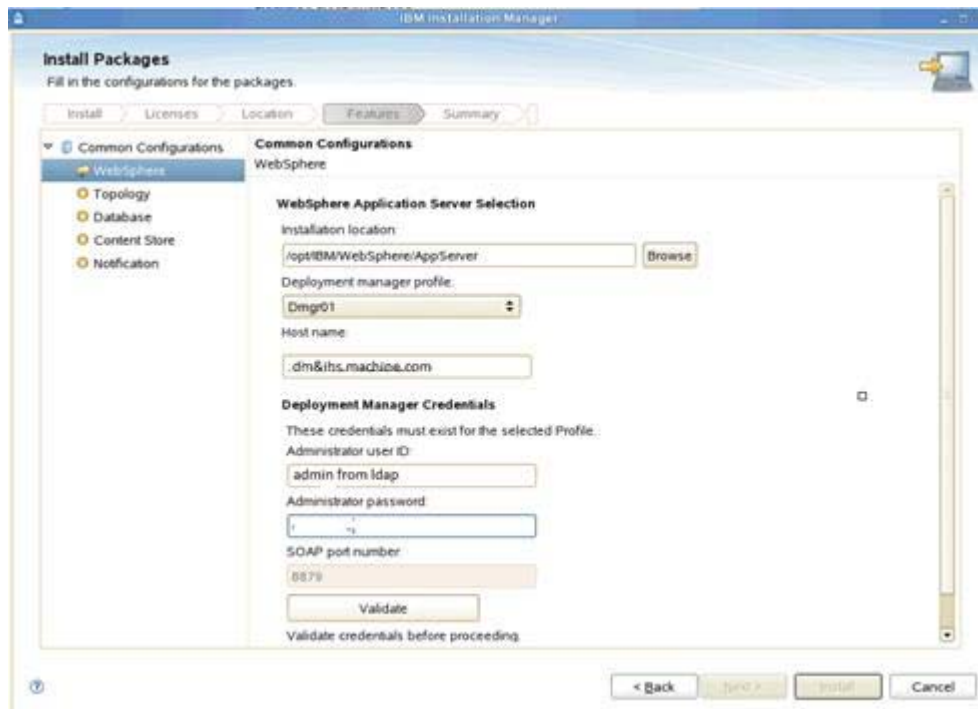


Figure 172. IBM Connections 4.0.0: Configuration for the packages

- ___ 13. The SSL certificate is retrieved from the Deployment Manager. Click **OK**.



Figure 173. Information dialog

14. Click **Topology** on the left side and **Medium: Applications grouped in several clusters**. Then, click **Next** to continue.

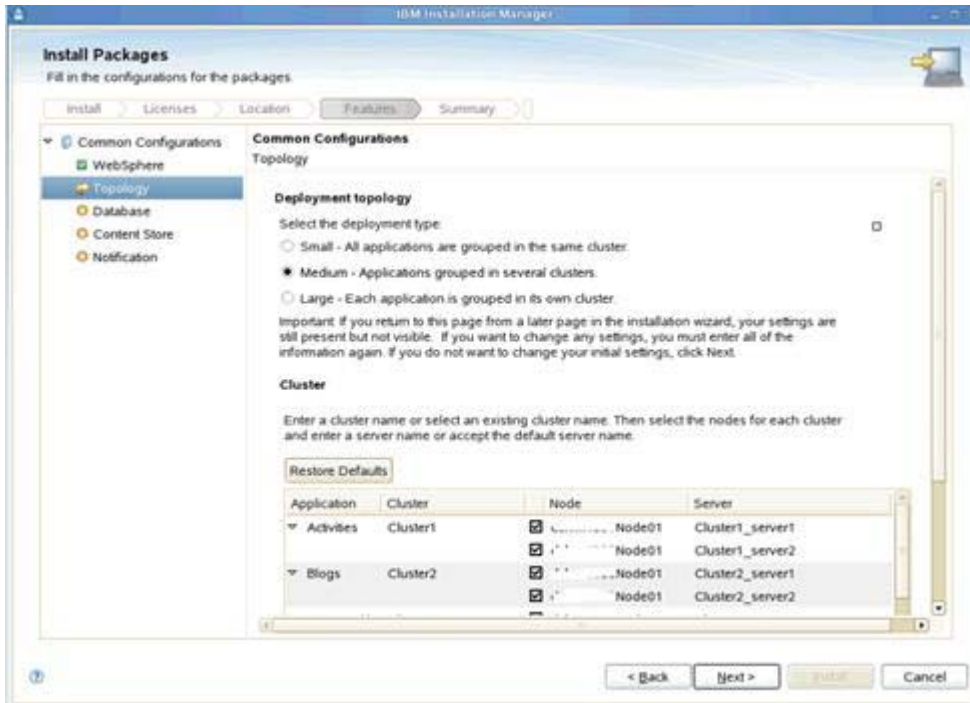


Figure 174. IBM Connections 4.0.0: Topology

15. Next is the database configuration. Ensure that your database server is started. Click **Yes, the applications are on the same database instance**. Enter the host name port of your database server and enter the JDBC driver location as well. In this example, it is `/opt/ibm/db2/V9.7/java`.



Figure 175. IBM Connections 4.0.0: Database configuration

- ___ 16. Then, scroll down. Enter your corresponding user ID and password as well. Then, click **Validate** at the bottom of the panel.

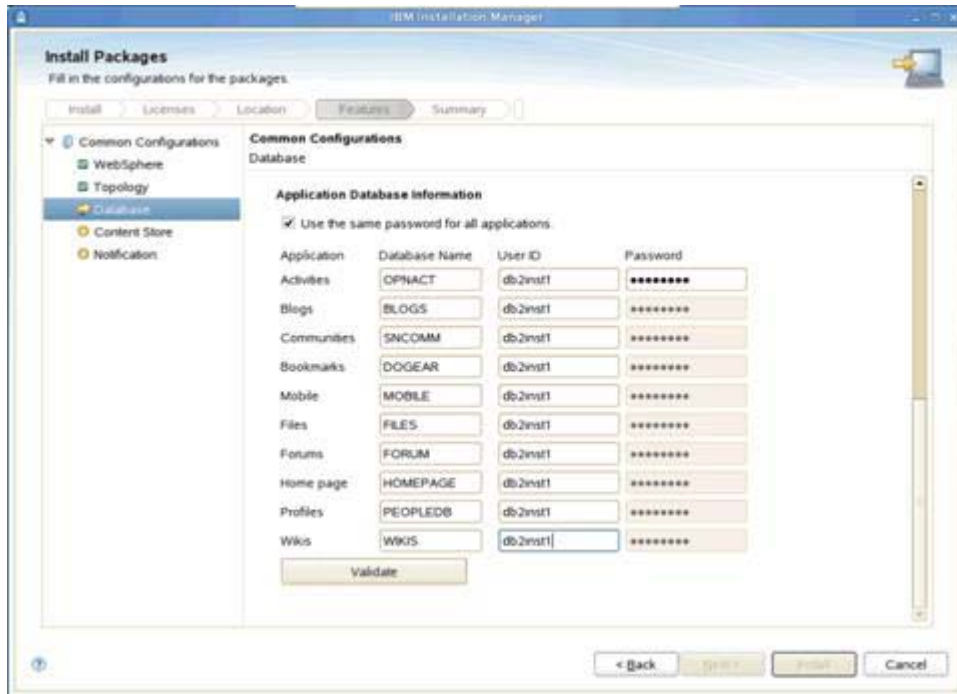


Figure 176. IBM Connections 4.0.0: Database configuration: User ID and password

The following validation message is displayed.



Figure 177. Validation message: Progress Information

- ___ 17. When the validation is complete, click **OK**.

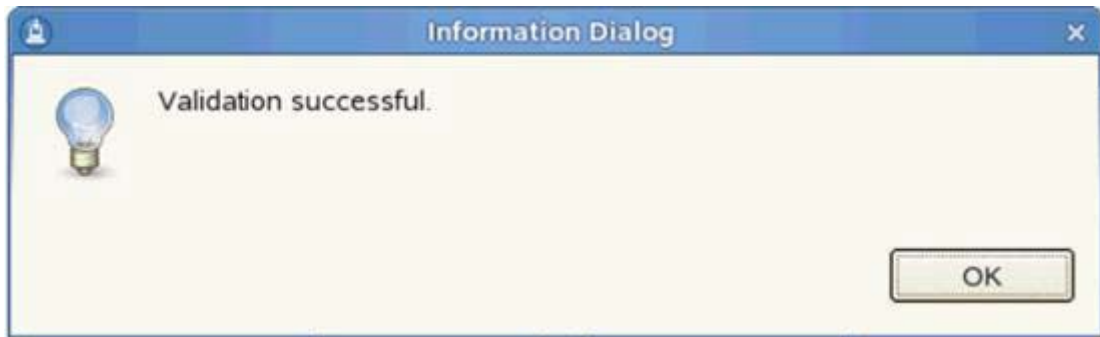


Figure 178. Information dialog: Validation successful

- ___ 18. Click **Next** to continue. Now you are asked about the content store (in a cluster or where the Deployment Manager and Nodes are not installed on the same computer). It should be a shared location where full read/write access is granted. In this example, change the shared content store to `/opt/IBM/SharedArea` which both nodes have access to. Click **OK** when ready.

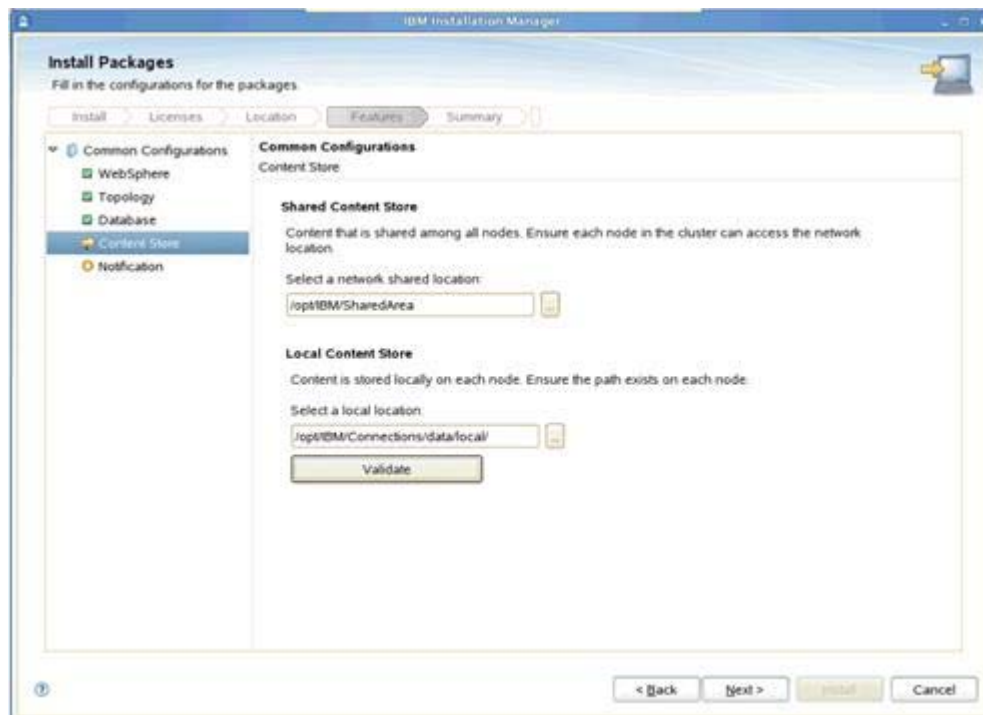


Figure 179. IBM Connections 4.0.0: Content Store

___ 19. Click **Validate**, Click **OK**, and then **Next**.

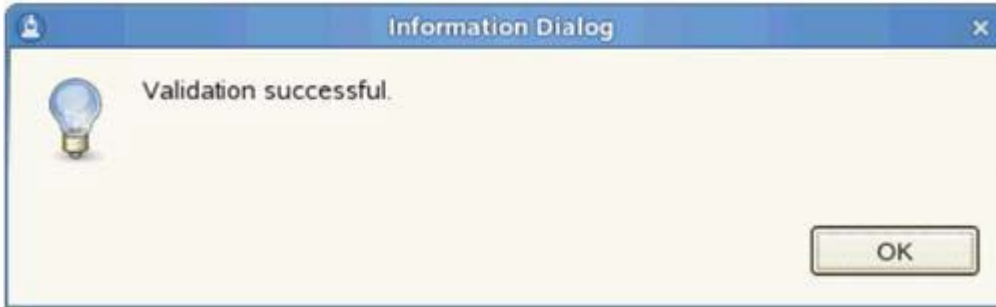


Figure 180. Information dialog: Validation successful

___ 20. Finally, click **None** to not enable notification from the notification configuration screen.

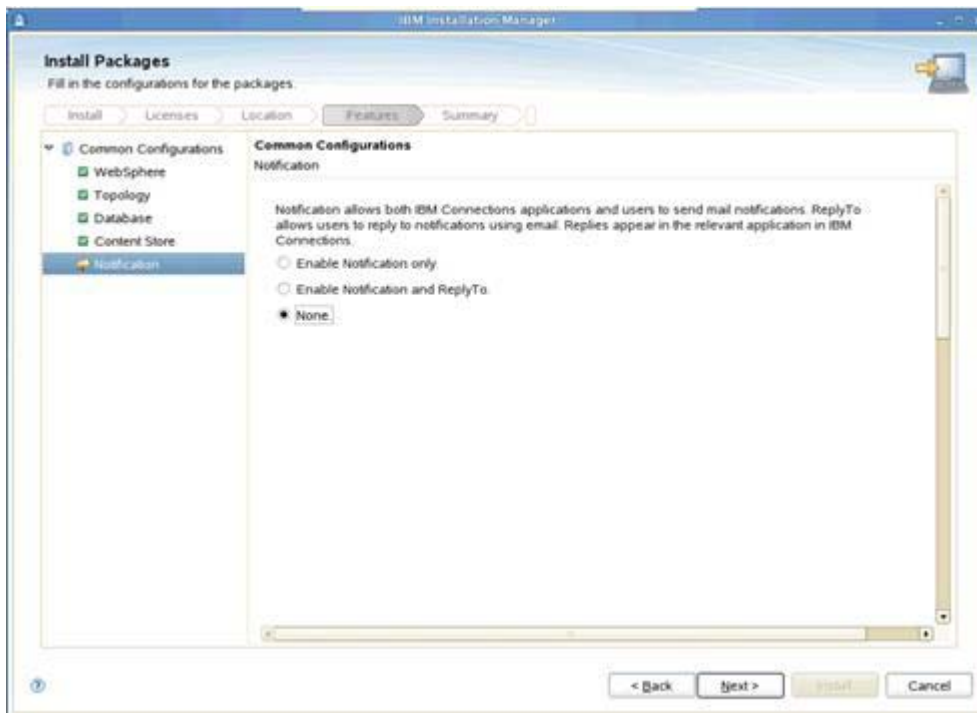


Figure 181. IBM Connections 4.0.0: Notification

___ 21. Check the summary information and click **Install**.

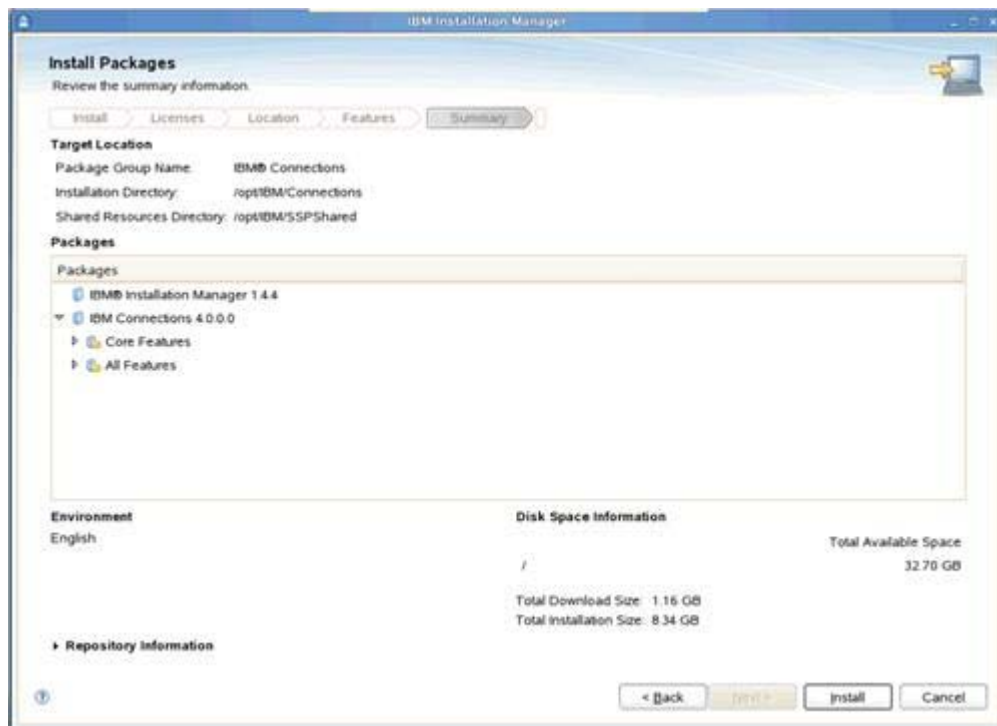


Figure 182. IBM Connections 4.0.0: Summary information

The installation then starts. You see a screen like in the following figure.

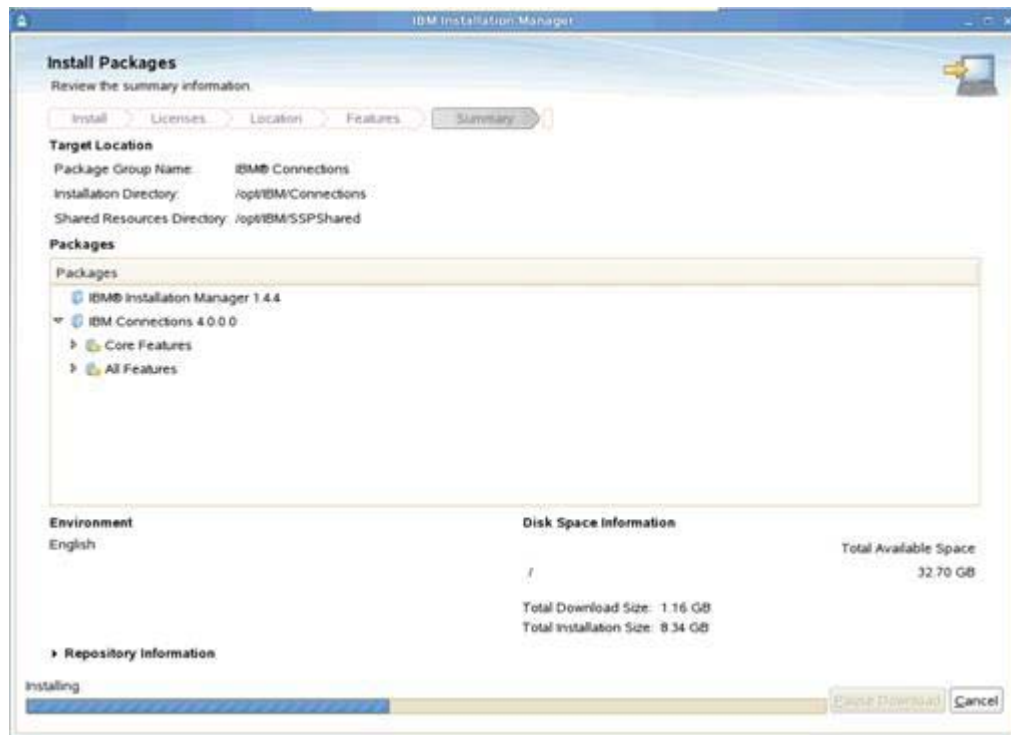


Figure 183. IBM Connections 4.0.0: Installation in progress

- ___ 22. When finished, you should see the following. Review the result of the installation. Click **Finish** to exit the installation wizard.



Figure 184. IBM Connections 4.0.0: Installation completed

- ___ 23. Restart the Deployment Manager.
- ___ 24. Open a command prompt and change to the `profile_root/Dmgr01/bin` directory. Enter the `./stopManager.sh` command and then enter the `./startManager.sh` command.

```

[redacted]@:/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin # ./stopManager.sh
ADMU0116I: Tool information is being logged in file
           /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/stopServer.log
ADMU0128I: Starting tool with the Dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
Realm/Cell Name: <default>
Username: Aamir_001_077
Password:
ADMU3201I: Server stop request issued. Waiting for stop status.
ADMU4000I: Server dmgr stop completed.

[redacted]@:/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin # ./startManager.sh
ADMU0116I: Tool information is being logged in file
           /opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/logs/dmgr/startServer.log
ADMU0128I: Starting tool with the Dmgr01 profile
ADMU3100I: Reading configuration for server: dmgr
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server dmgr open for e-business; process id is 17274
[redacted]@:/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin #

```

Figure 185. Command prompt to change the directory

- ___ 25. Start all the federated nodes and enter the startNode command.

```

[redacted]:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin # ./startNode.sh
ADMU0116I: Tool information is being logged in file
/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/logs/nodeagent/startServer.log
ADMU0128I: Starting tool with the AppSrv01 profile
ADMU3100I: Reading configuration for server: nodeagent
ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server nodeagent open for e-business; process id is 8350
dslvm1008:/opt/IBM/WebSphere/AppServer/profiles/AppSrv01/bin #

```

Figure 186. Start node command

- ___ 26. Log in to the Integrated Solutions Console on the Deployment Manager to fully synchronize all nodes.
- ___ a. Go to **System administration > Nodes**.
- ___ b. Select the nodes and click **Full Resynchronize**.



Figure 187. Performing a full resynchronize

Nodes

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

Preferences

Add Node Remove Node Force Delete Synchronize Full Resynchronize Stop

Select	Name	Host Name	Version	Discovery Protocol	Status
	CellManager01	.dm&its.machine.com	ND 7.0.0.21	TCP	↔
<input checked="" type="checkbox"/>	Node01	.node1.machine.com	ND 7.0.0.21	TCP	↔
<input checked="" type="checkbox"/>	Node01	.node2.machine.com	ND 7.0.0.21	TCP	↔

Figure 188. Performing a full resynchronize



Note

Wait until the Deployment Manager copies all the application EAR files to the installedApps directory on each of the nodes. This process can take up to 30 minutes. To find out whether the process is complete, log in to each node and go to the installedApps directory and ensure that all the application EAR files are fully extracted. The default path is `app_server_root/profiles/AppSrv01/installedApps`.

```

over/profiles/AppSrv01/installedApps/[redacted]Cell01 # ls
*.ear *.connectionsCommon.ear *.logon.ear *.tiles.ear *.forums.ear *.help.ear *.homepage.ear *.mobileAdministration.ear *.mobile.ear *.moderation.ear *.news.ear *.
over/profiles/AppSrv01/installedApps/[redacted]Cell01 #

```

Figure 189. `app_server_root/profiles/AppSrv01/installedApps`

- ___ 27. Restart the Deployment Manager.
- ___ 28. Start all your IBM Connections clusters:
- ___ a. Log in to the Integrated Solutions Console on the Deployment Manager.

- ___ b. Go to **Servers > Clusters > WebSphere Application Server clusters**.
- ___ c. Select the IBM Connections clusters and click **Start**.

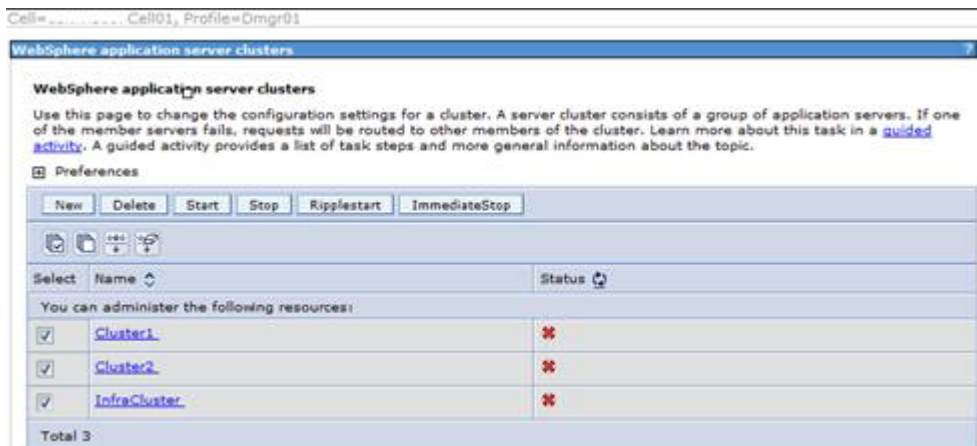


Figure 190. Starting IBM Connections clusters

16. Post-installation tasks

Reviewing JVM heap size

- ___ 1. Log in to the WebSphere® Application Server Integrated Solutions Console and select **Servers > Server Type > WebSphere application servers**.
- ___ 2. Click <server>, where <server> is the name of an IBM Connections server. You might have several servers in your deployment, so you might need to repeat these steps for each server.
- ___ 3. In the Server Infrastructure area, click **Java and Process Management** and then click **Process Definition > Java Virtual Machine**.

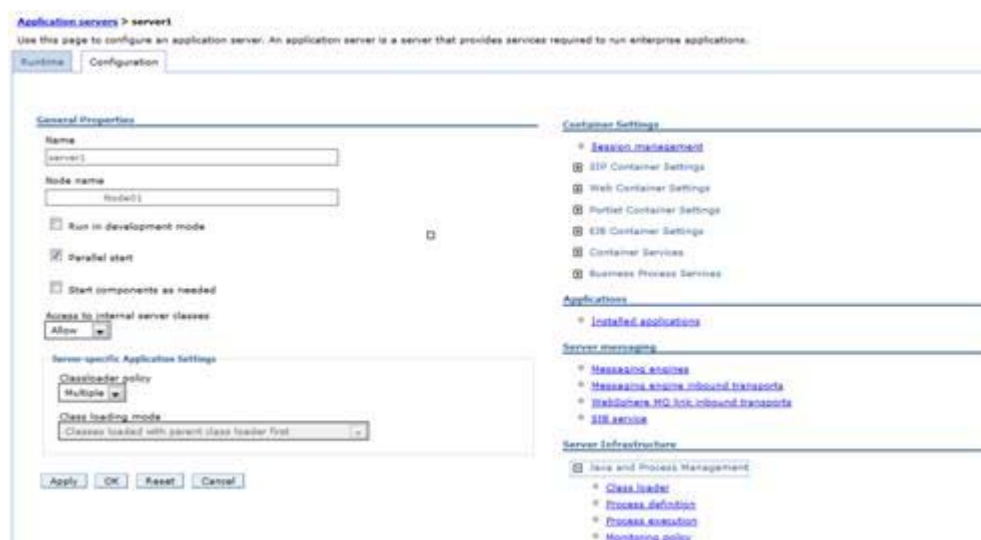


Figure 191. Application servers

- ___ 4. Review the maximum heap size. IBM Installation Manager sets the following values for Small and Medium deployments. Make sure that the Maximum Heap Size is set to 2506.



Note

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

- 5. Adjust the current values of the heap size up or down to suit the needs of your deployment and your hardware capabilities.

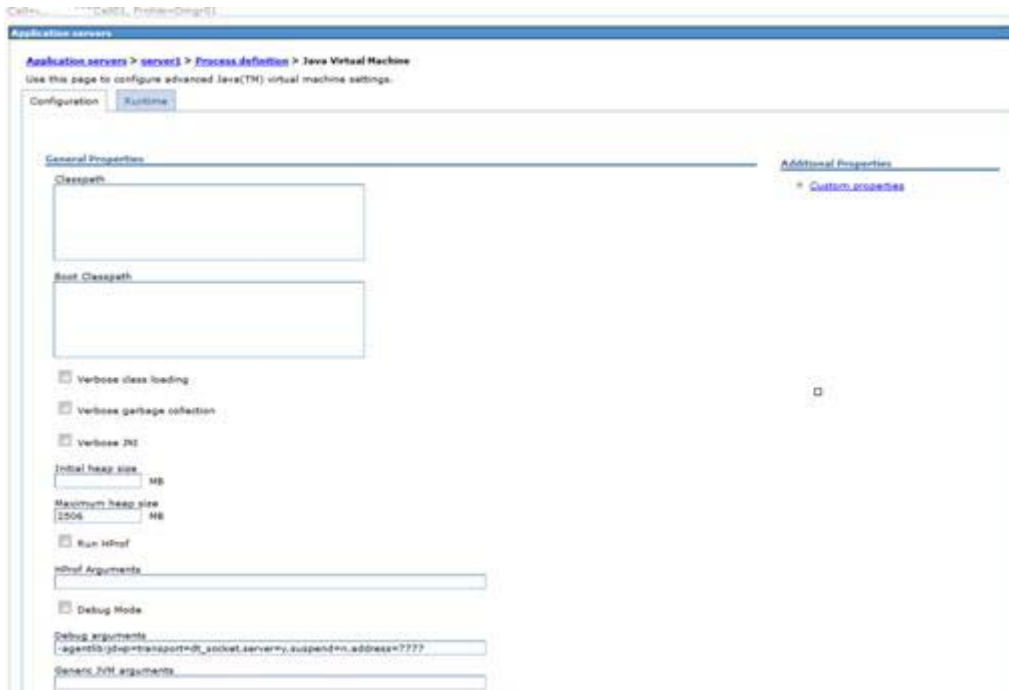


Figure 192. Java virtual machine

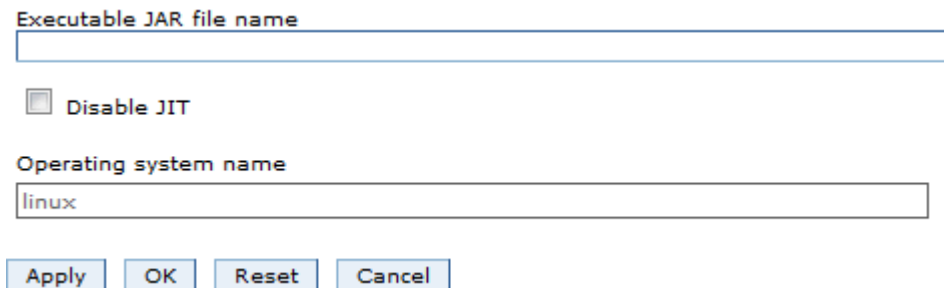


Figure 193. Adjusting the values of the heap size

- 6. Click **OK** and then click **Save**.
- 7. Repeat these steps for any additional servers in your deployment.

The next section is about HTTP configuration and must be completed as HTTP is required for Login by default on Connections.

Configuring IBM HTTP Server

Add web server as unmanaged node

- ___ 1. After the administration server is started, open the Deployment Manager and add the web server to the cell as an unmanaged node. Open the administrative console at <https://dm&IBM HTTP Server.machine.com:9043/admin>.
- ___ 2. Go to **System Administration: Nodes** and click **Add Node**.



Figure 194. System Administration: Nodes

- ___ 3. Select the Unmanaged node option and click **Next**.



Figure 195. Selecting the Unmanaged node option

- ___ 4. Provide a name and host name of the HTTP server and click **OK**.



Figure 196. Providing a host name for the HTTP server

___ 5. Click **Save**.

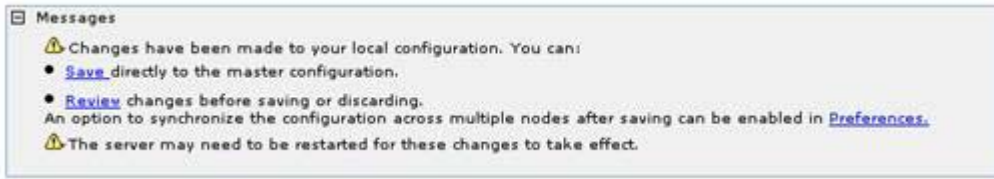


Figure 197. Saving directly to the master configuration

On the nodes panel, the web server is displayed in the list.



Figure 198. Nodes panel

Add web server as a server

Next, add the web server as a server in the configuration. To do so, follow these steps:

- ___ 1. From **Servers: Server Types: Web Servers**, click **New**.

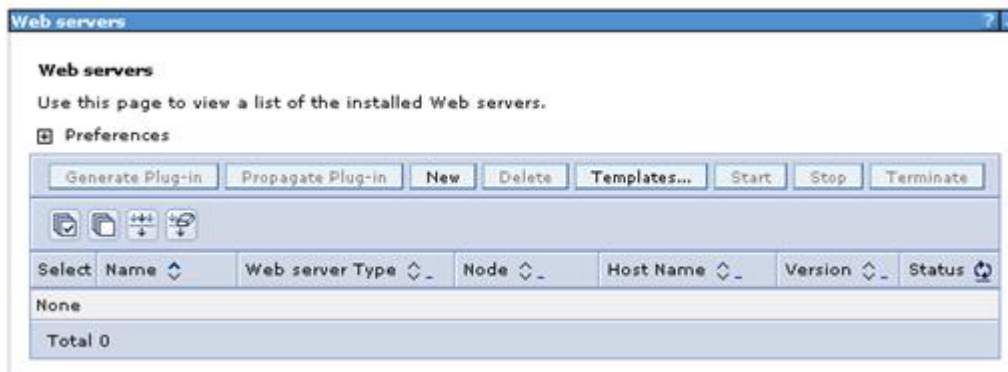


Figure 199. Adding a web server as a server in the figuration

- ___ 2. Select the web server node and provide the name of this server, `webserver1`. It is the same name that is provided during the plug-ins installation on the web server. Click **Next** to continue.



Figure 200. Selecting a node for the web server and selecting the web server type

- ___ 3. The IBM HTTP Server option is selected. Click **Next** to continue.

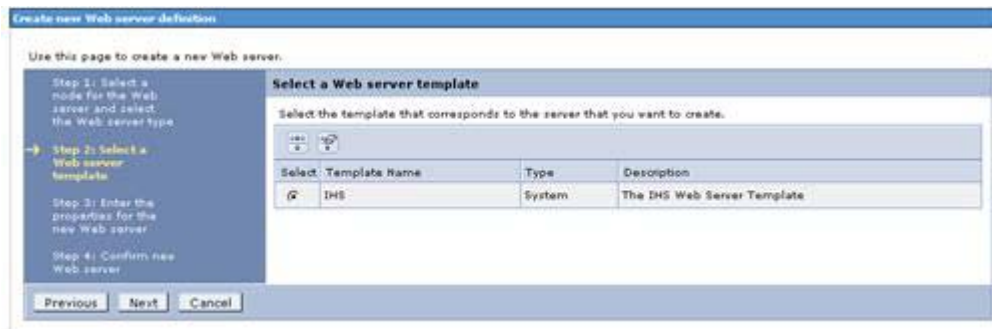


Figure 201. Selecting a web server template

4. Provide all of the web server details as shown in the following figure and click **Next**.

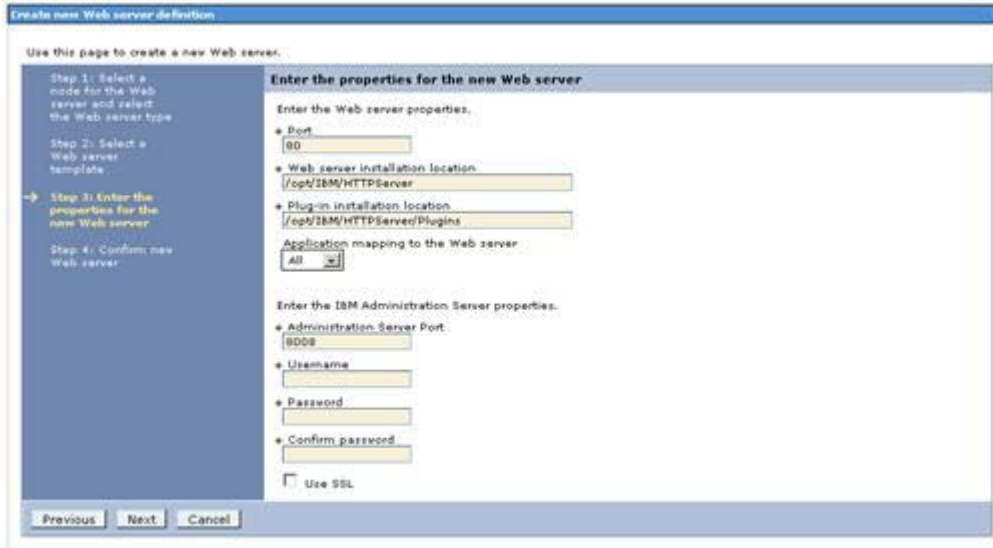


Figure 202. Entering the properties for the new web server

5. Confirm the new web server and click **Finish**.

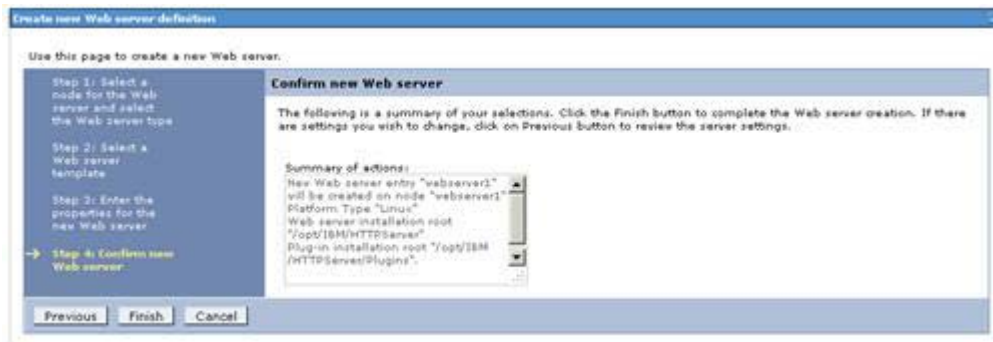


Figure 203. Confirming new web server

6. Save this change. Before proceeding, do a full synchronize between nodes in the deployment.

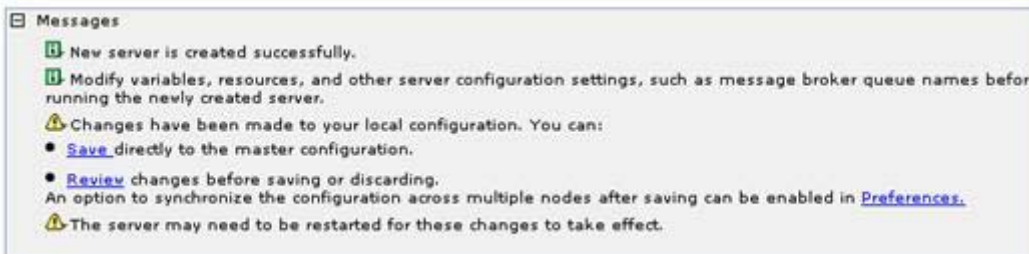


Figure 204. Saving the new web server

- ___ 7. Return to **Servers > Server Types > Web Servers**. Generate and propagate the plug-in file to the web server.



Figure 205. Generating and propagating the plug-in

- ___ 8. To do so, select the check box beside `webserver1` and click **Generate Plug-in**.

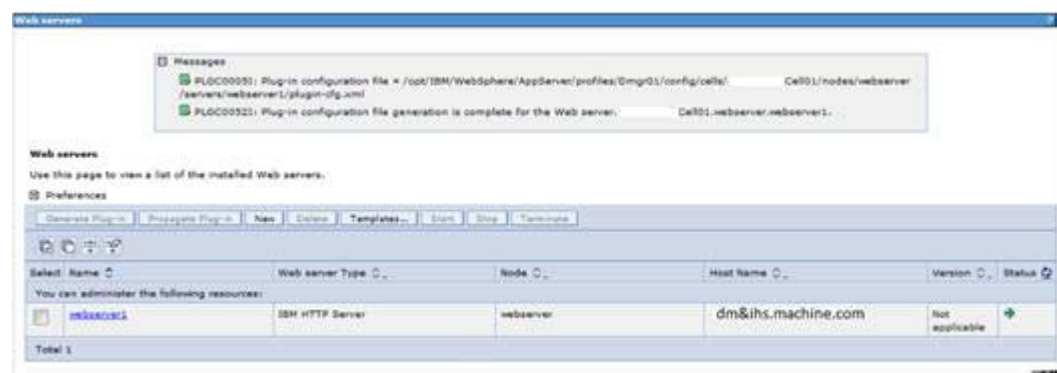


Figure 206. Generating plug-in

- ___ 9. Select the check box again and click **Propagate Plug-in**.



Figure 207. Propagating plug-in

___ 10. Click `webserver1` and then click the **Plug-in properties**.

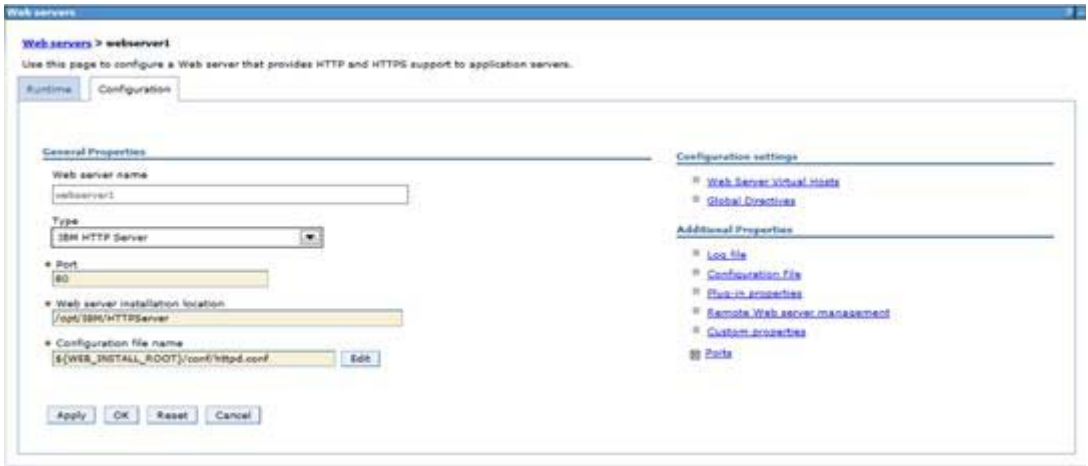


Figure 208. Plug-in properties

___ 11. From the repository copy of web server plug-in files section, click **Copy to Web server key store directory**.



Figure 209. Repository copy of Web server plug-in files

The following message is displayed to indicate the successful copying of these keys. Again, restart the web server for the plug-in changes to take effect.



Figure 210. Message indicating that keys were successfully copied

Configuring IBM HTTP Server for SSL

To support SSL, create a self-signed certificate and then configure IBM HTTP Server for SSL traffic. If you use this certificate in production, users might receive warning messages from their browsers. In a typical production deployment, you would use a certificate from a trusted certificate authority.

1. The first step is to create a key file. Start the iKeyman utility by `ikeyman.sh` from `/opt/IBM/HTTPServer/bin`.



Figure 211. Starting the iKeyman utility

The following panel is displayed when you start this utility.

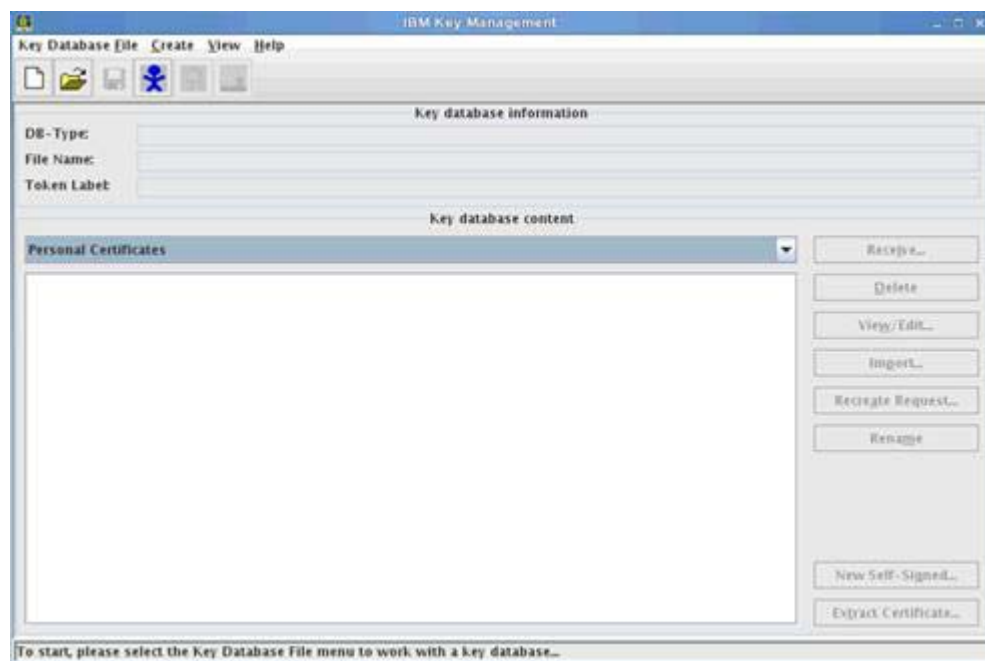


Figure 212. IBM Key Management

2. Click **Key Database File > New...**

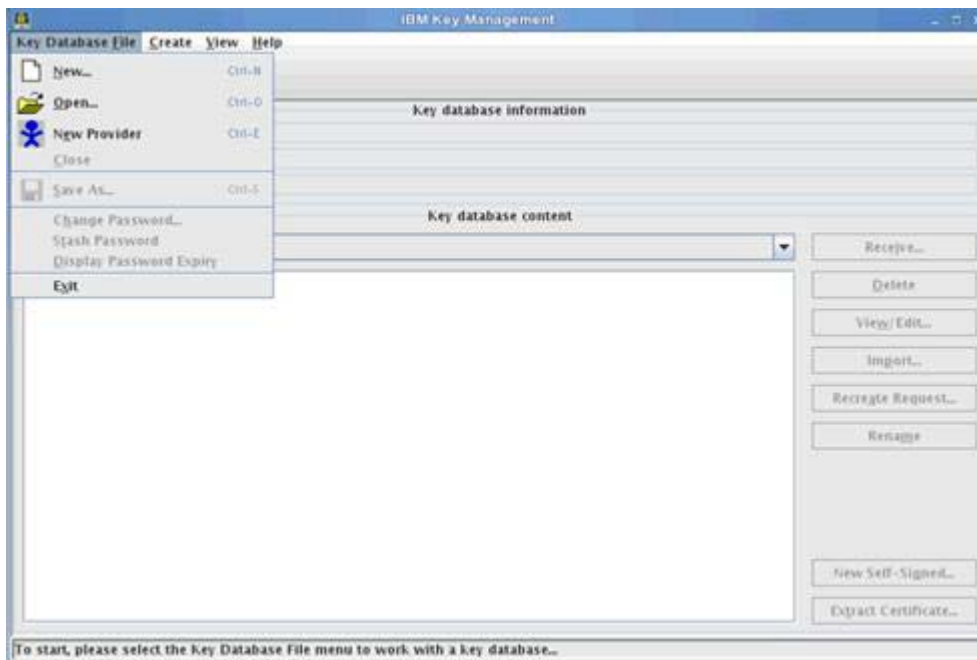


Figure 213. Key Database File: Creating a new key file

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

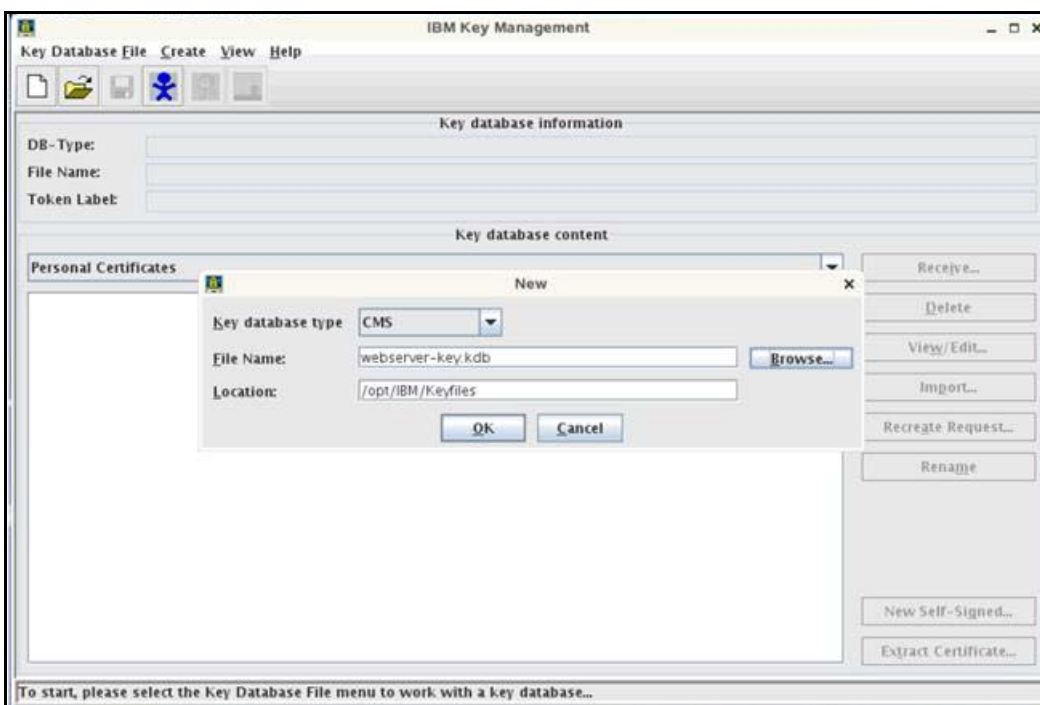


Figure 214. Selecting database type, entering a new name and location for the key file

- ___ 4. Enter a password and click **Stash password to a file**.

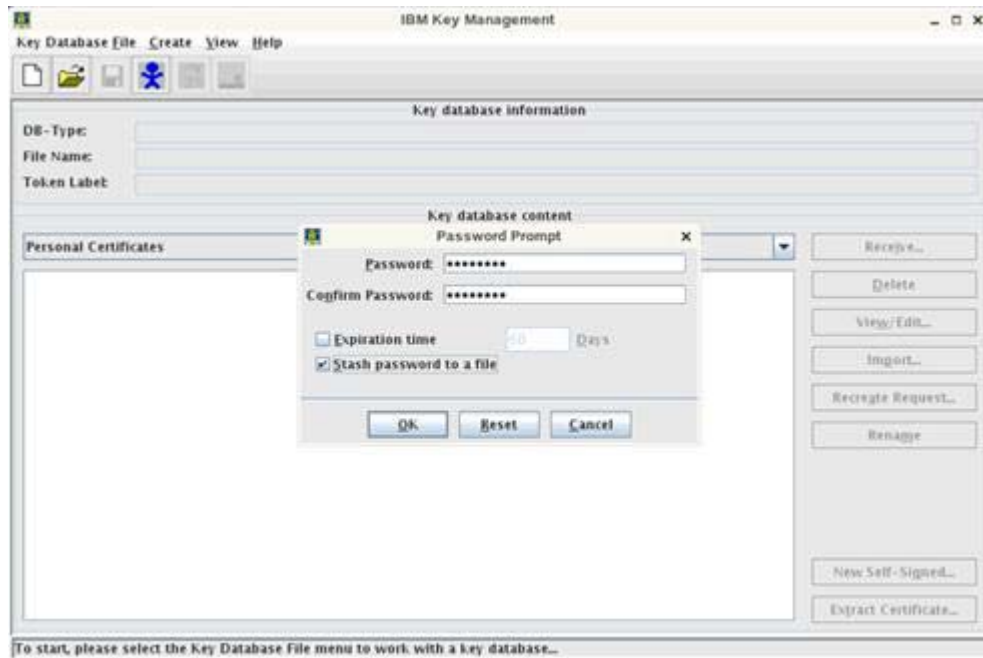


Figure 215. Password prompt: Stash password to a file

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

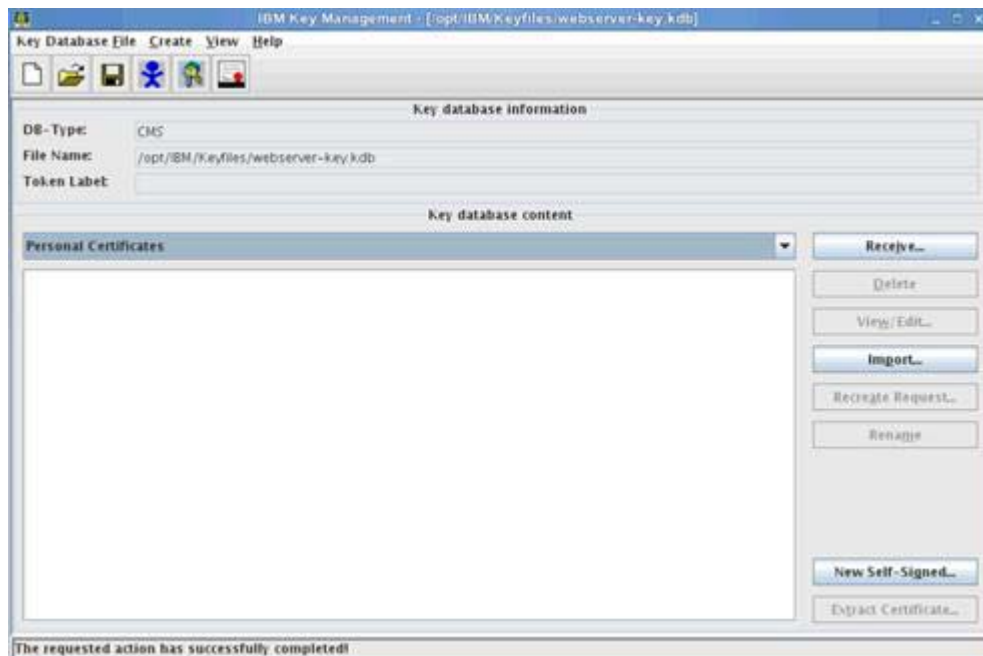


Figure 216. IBM Key Management

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

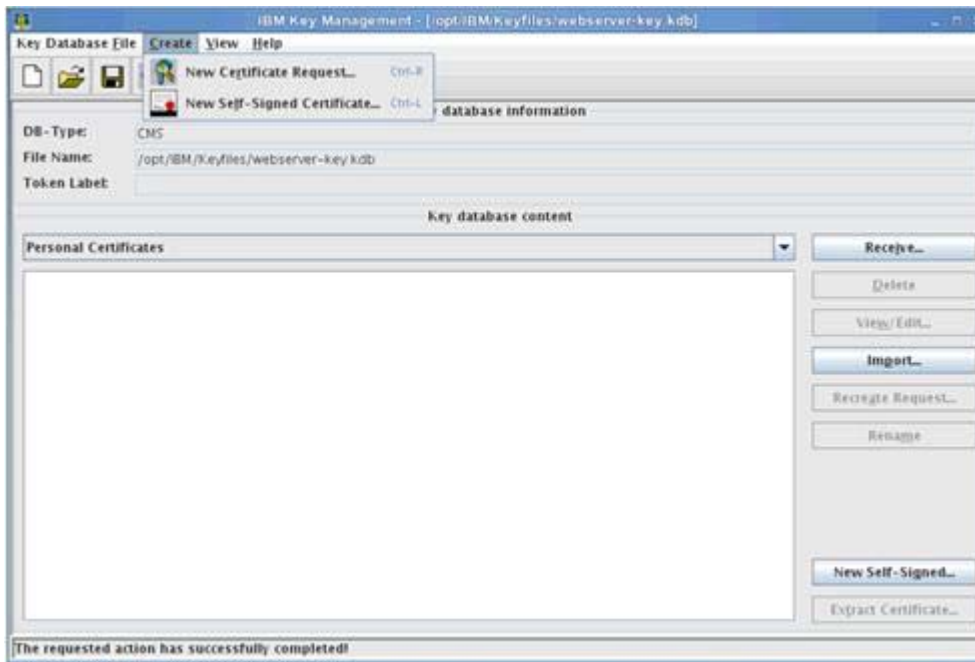


Figure 217. iKeyman: Creating a self-signed certificate

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

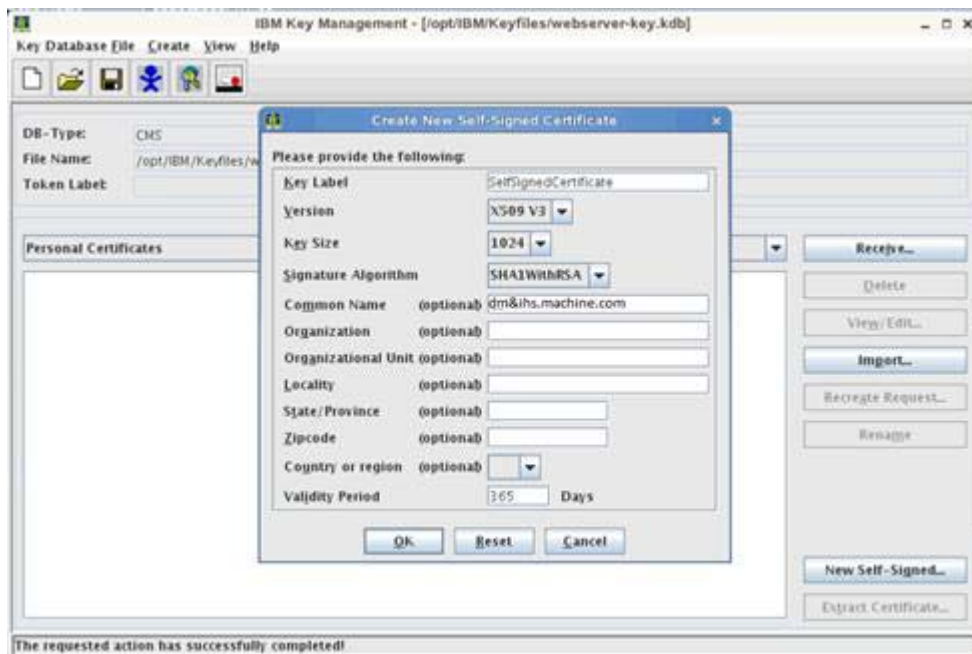


Figure 218. Entering the properties for the certificate

- ___ 7. The certificate now appears in the key file, as in the following figure. Stop the IBM HTTP Server, if started. When you verified that it is stopped, log in to the administrative console and configure the web server for SSL.

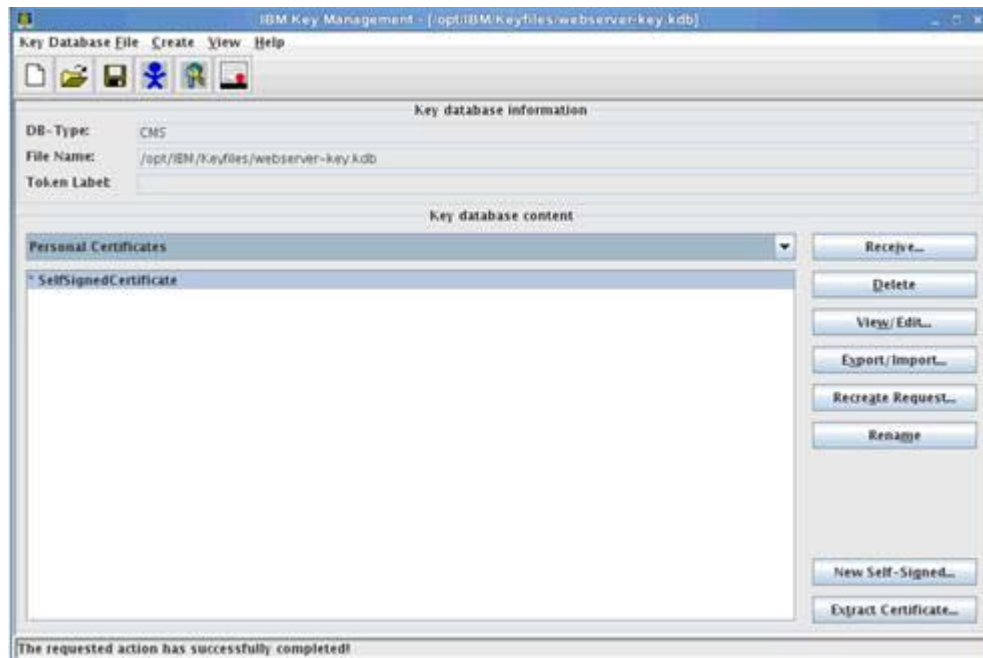


Figure 219. Stopping the IBM HTTPS Server

- ___ 8. From the Web servers panel, click webserver1.



Figure 220. Web servers panel

9. Click **Configuration File** to open the `httpd.conf` from the administrative console.

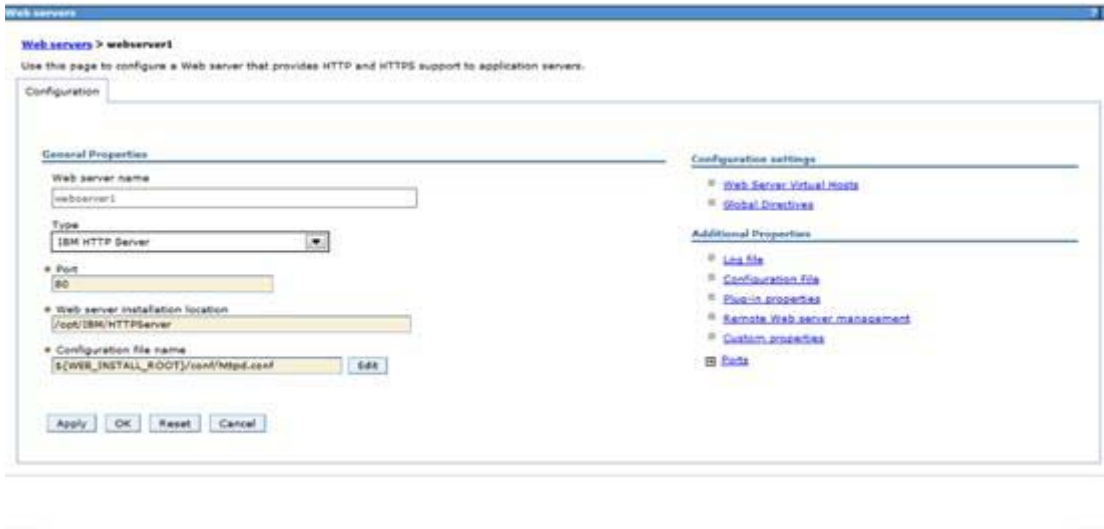


Figure 221. Configuration file

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



Figure 222. Editing the `http.conf` file

___ 10. At the bottom of the configuration, add the following lines to the http.conf file:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName connections.example.com
SSLEnable
AllowEncodedSlashes On

</VirtualHost>
</IfModule>
SSLDisable

Keyfile "/opt/IBM/Keyfiles/webserver-key.kdb"
SSLStashFile "/opt/IBM/Keyfiles/webserver-key.sth"
```

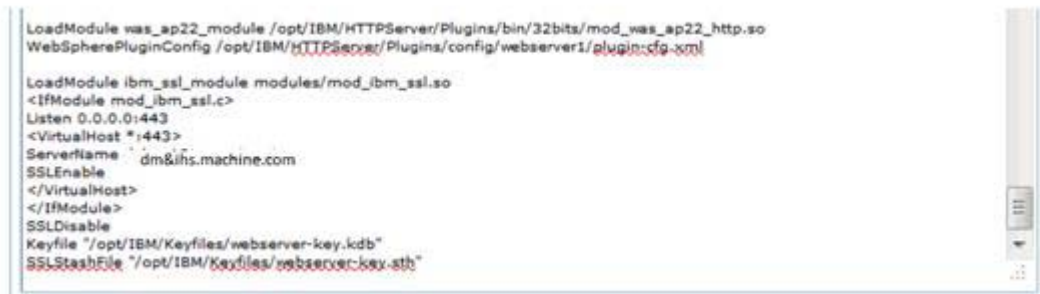


Figure 223. http.conf file

___ 11. Click **OK** to save this change.

12. Next, start the IBM HTTP Server. To verify that the SSL settings took effect correctly, type `https://dm&IBM HTTP Server.machine.com` into a browser. If the IBM HTTP Server page appears over https, then this step was successful. You might need to accept the certificate to your browser as it is not signed.

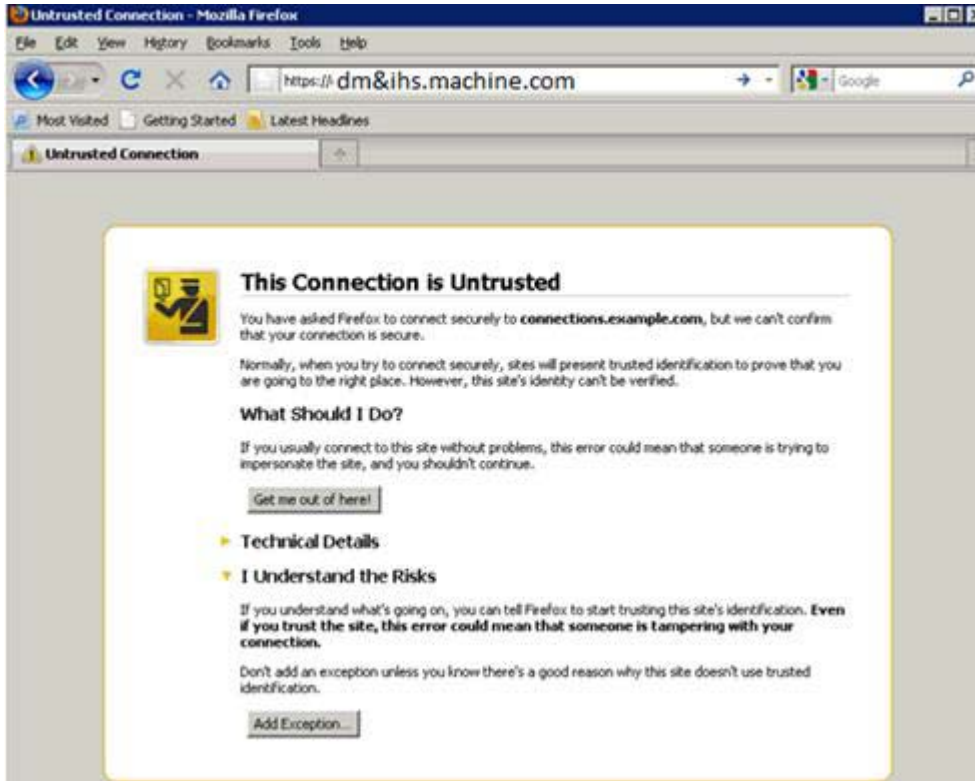


Figure 224. Untrusted connection: Accepting the certificate of the browser

13. Click **Confirm Security Exception**.

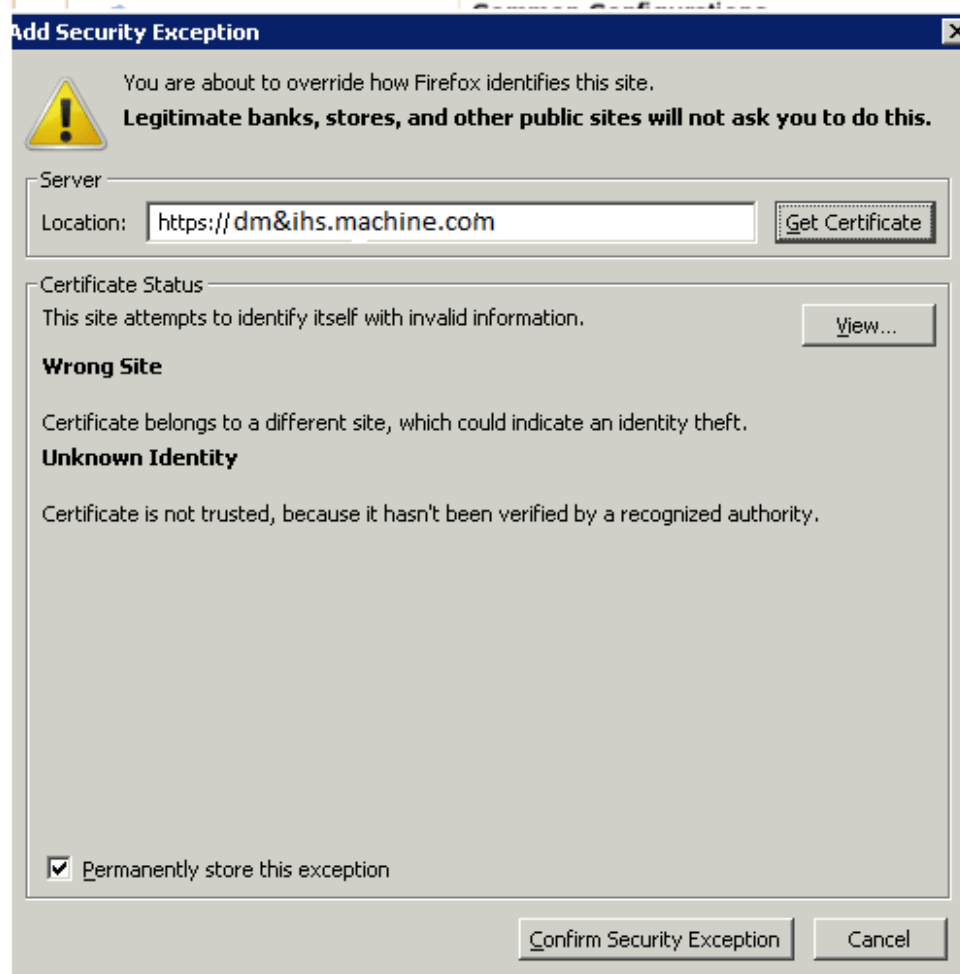


Figure 225. Adding security exception

The IBM HTTP Server home page is displayed.



Figure 226. WebSphere software: IBM HTTP Server Version 7.0

Adding Certificates to the WebSphere truststore

1. On the administrative console, go to **Security > SSL Certificate and Key Management**. Click **Key Stores and certificates**.



Figure 227. SSL certificate and key management

___ 2. Click **CellDefaultTrustStore** as shown in the following figure.

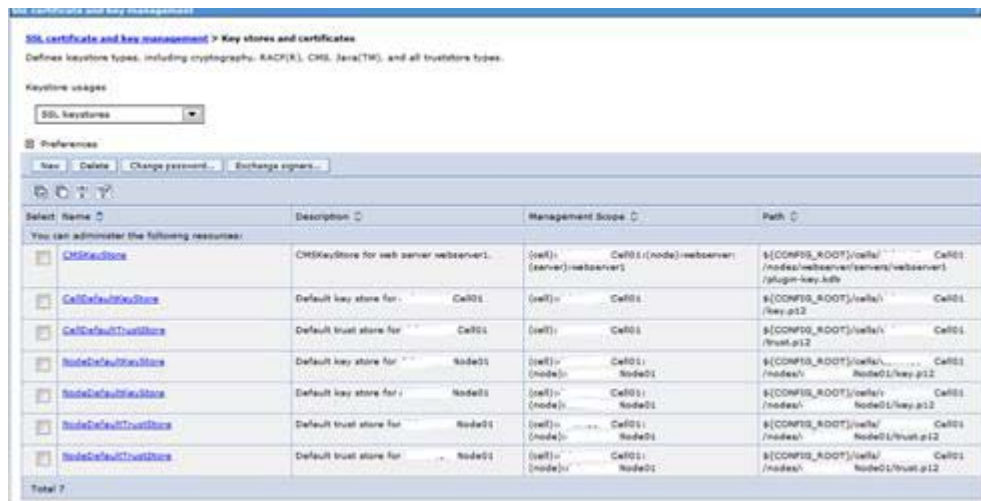


Figure 228. Key stores and certificates

___ 3. From within CellDefaultTrustStore, click **Signer certificates** from the right side.

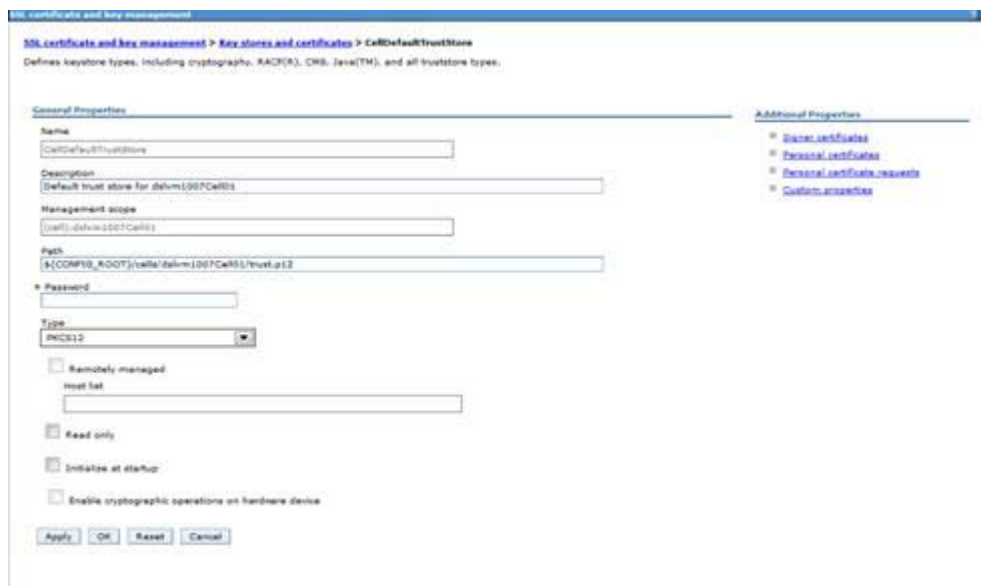


Figure 229. CellDefaultTrustStore

4. To add the web server signer to the truststore, click the **Retrieve from Port**.

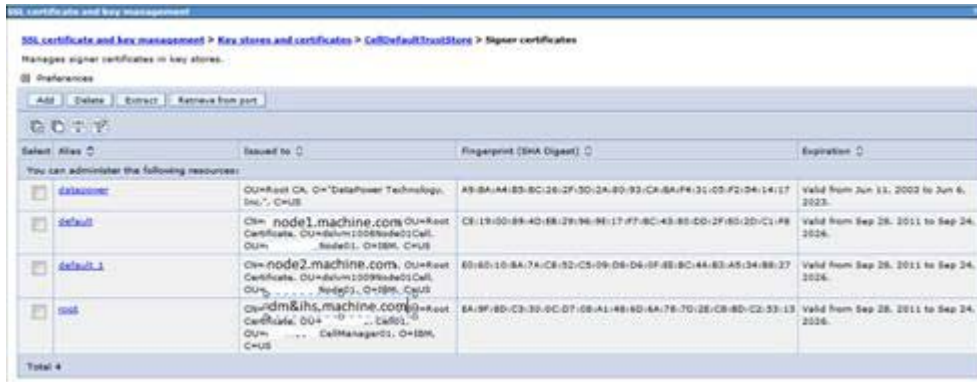


Figure 230. Retrieving from Port

5. 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.

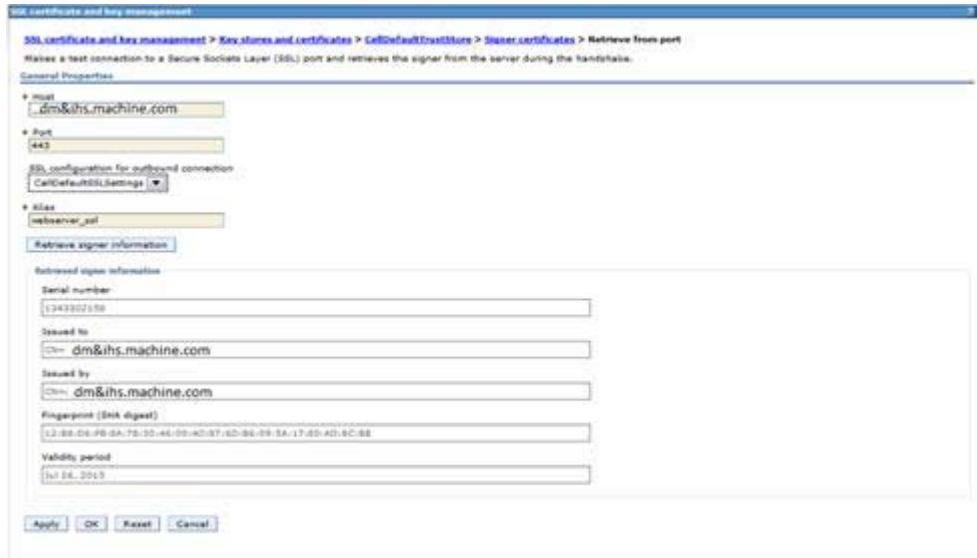


Figure 231. SSL certificate and key management: Retrieving signer information

6. Save this change and restart the HTTP server to apply the changes.

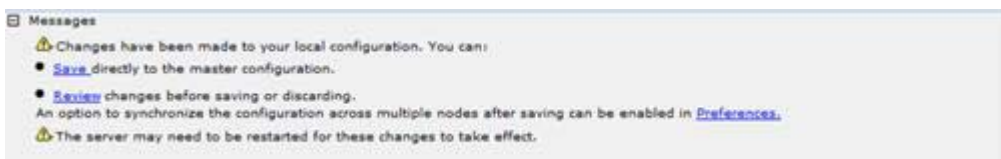


Figure 232. Saving the changes and restarting the HTTP server

Update web addresses used by Lotus Connections to access content

- 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.

```

Terminal
File Edit View Terminal Tabs Help
/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin # ./wsadmin.sh -lang
jython -username Aamir_001_077 -password . -port 8879
WASX7209I: Connected to process "dmgr" on node (.....)CellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/bin_lc_admin/connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("/temp", "(.....)Cell01")
Connections configuration file successfully checked out
wsadmin>

```

Figure 233. wsadmin client

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

The first screenshot shows the original XML configuration with href values pointing to a specific IP and port:

```

<xsi:type="xsd:string" href="http://dm&ihs.machine.com:9090" ssl_href="http://dm&ihs.machine.com:9090"/>

```

The second screenshot shows the updated XML configuration where the href and ssl_href values have been changed to use the domain name and omit the port number:

```

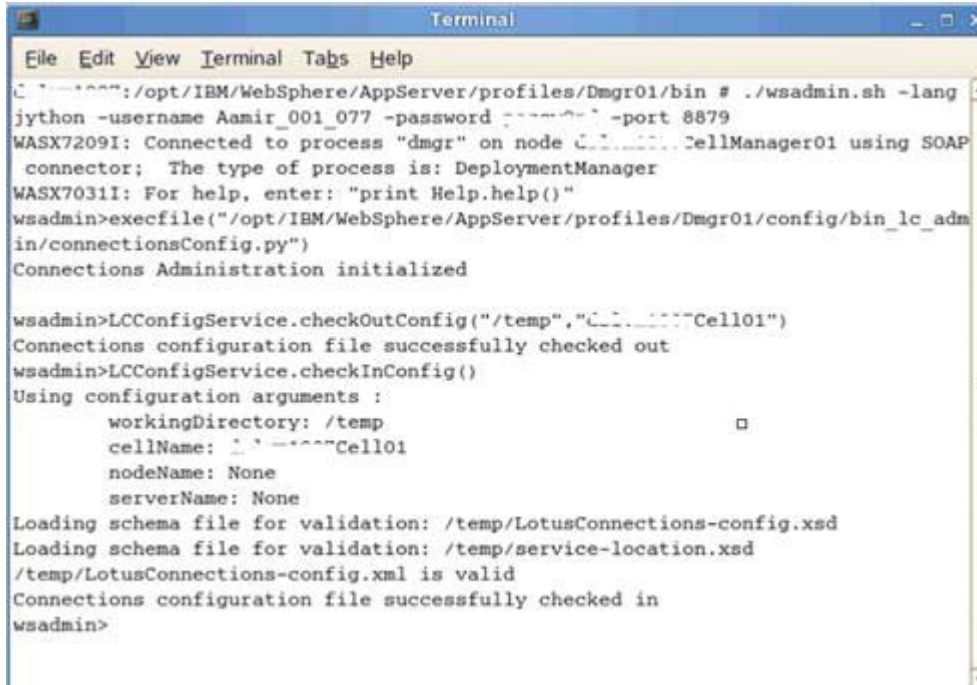
<xsi:type="xsd:string" href="http://dm&ihs.machine.com" ssl_href="http://dm&ihs.machine.com"/>

```

Figure 234. Resynchronizing the node

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

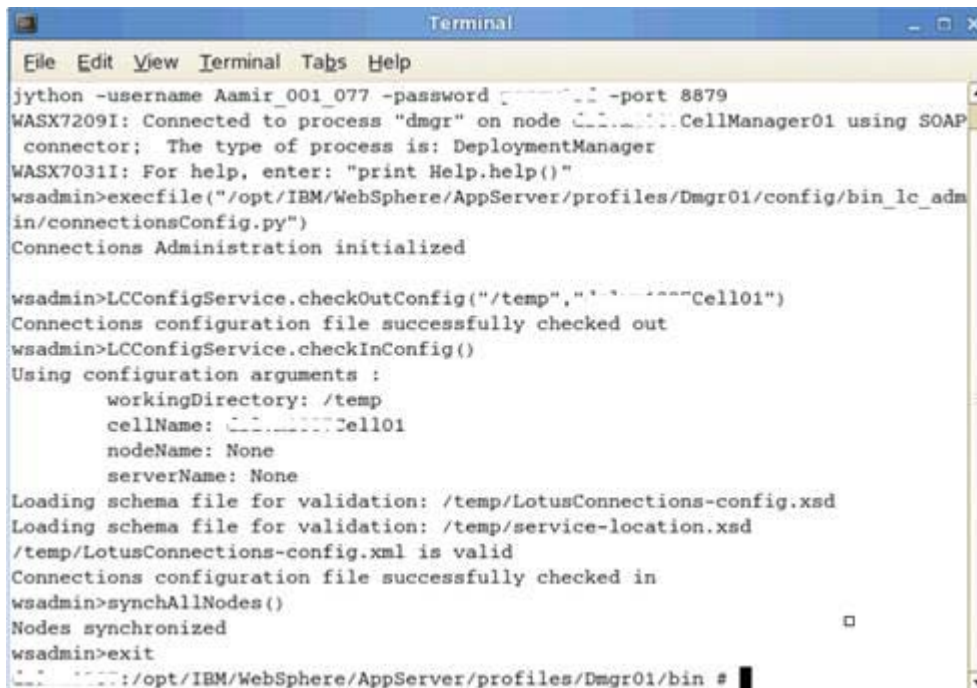
3. The commands to do all of the above are shown below (the above updates take place after the check out command).



```
Terminal
File Edit View Terminal Tabs Help
C:\...: /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin # ./wsadmin.sh -lang
jython -username Aamir_001_077 -password [REDACTED] -port 8879
WASX7209I: Connected to process "dmgr" on node C... CellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/bin_lc_admin/connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("/temp","...Cell01")
Connections configuration file successfully checked out
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
    workingDirectory: /temp
    cellName: ...Cell01
    nodeName: None
    serverName: None
Loading schema file for validation: /temp/LotusConnections-config.xsd
Loading schema file for validation: /temp/service-location.xsd
/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>
```

Figure 235. Check out commands



```
Terminal
File Edit View Terminal Tabs Help
jython -username Aamir_001_077 -password [REDACTED] -port 8879
WASX7209I: Connected to process "dmgr" on node C... CellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("/opt/IBM/WebSphere/AppServer/profiles/Dmgr01/config/bin_lc_admin/connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("/temp","...Cell01")
Connections configuration file successfully checked out
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
    workingDirectory: /temp
    cellName: ...Cell01
    nodeName: None
    serverName: None
Loading schema file for validation: /temp/LotusConnections-config.xsd
Loading schema file for validation: /temp/service-location.xsd
/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>synchAllNodes()
Nodes synchronized
wsadmin>exit
C:\...: /opt/IBM/WebSphere/AppServer/profiles/Dmgr01/bin # █
```

Figure 236. Check out commands

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

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

Configuring an administrator user for blogs and home page

Next, you need to add an admin user for blogs. Follow these steps:

- ___ 1. Log in to your admin console at <http://dm&IBM HTTP Server.machine.com:9060/admin>.
- ___ 2. Select **Application > Application Types > WebSphere Enterprise Applications** and then select **Blogs**. Next, click **Security role to user/group mapping**.



Figure 237. Enterprise Applications: Blogs

___ 3. Click **Admin role** and then the **Map Users**.



Figure 238. Search and Select Users

___ 4. Search for the user, `Aamir_001_077` in this example, and add them.

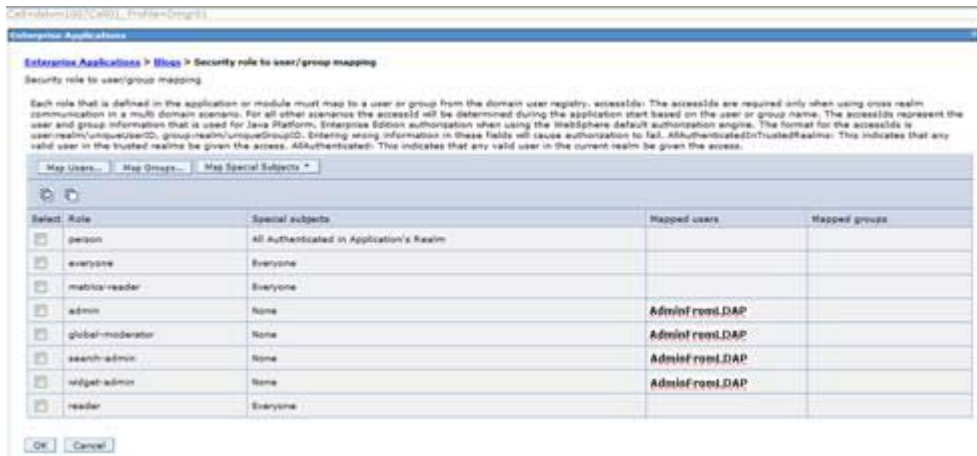


Figure 239. Select role to user/group mapping

___ 5. Click **OK** and then save the changes.

- ___ 6. For the home page, follow the same steps as above and you should be able to see the following panel:

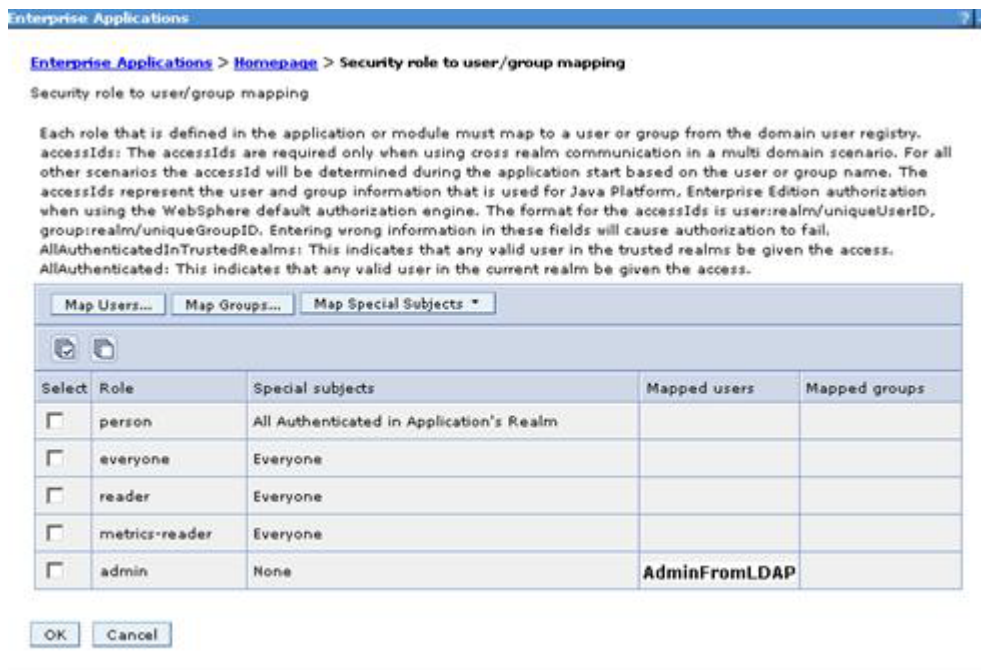


Figure 240. Select role to user/group mapping

Enabling fast downloads for files and wikis

The last item is to enable fast download for files and wikis. This is an optional step for customers but it is suggested to run all SVT systems with it.

- ___ 1. On your deployment manager, go to `/opt/IBM/LotusConnections/plugins/IBM HTTP Server/mod_ibm_local_redirect/linux_ia32-ap22`. You see a file that is called `mod_ibm_local_redirect.so` located there.
- ___ 2. Copy this file to your HTTP Server under `/opt/IBM/HTTPServer/modules/`.
- ___ 3. Now edit the `httpd.conf` under `/opt/IBM/HTTPServer/conf`:

```
LoadModule ibm_local_redirect_module modules/mod_ibm_local_redirect.so
```

```
LoadModule env_module modules/mod_env.so (it might already exist to check your existing file).
```

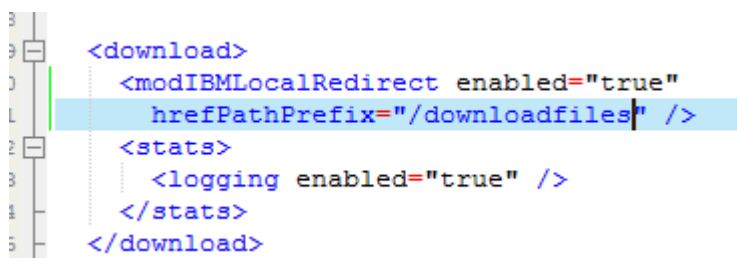
- ___ 4. Also, add the following sections. Paths need to change based on installation.

```

Alias /downloadfiles /opt/IBM/SharedArea/files/upload/
Alias /downloadwikis /opt/IBM/SharedArea/wikis/upload/
<Directory /opt/IBM/SharedArea/files/upload/>
  Order Deny ,Allow
  Deny from all
  Allow from env=REDIRECT_FILES_CONTENT
</Directory>
<Directory /opt/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>

```

- ___ 5. Finally, edit the `files-config.xml` and `wikis-config.xml` files under `/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/config/cells/dmCell01/LotusConnections-config/` on your deployment manager and change.



```

3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000

```

Figure 241. Editing files-config.xml

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

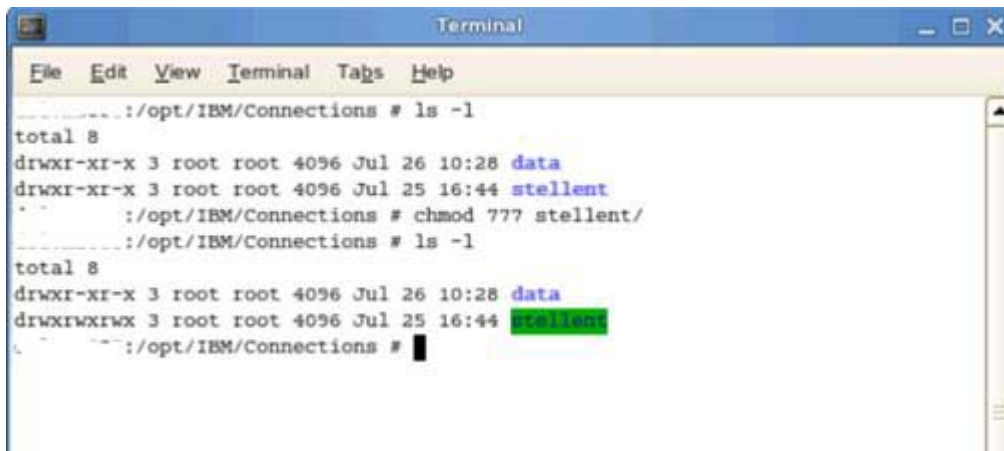
Figure 242. Editing wikis-config.xml

- ___ 6. When you made the changes, make sure to synch the changes to your nodes.
- ___ 7. Restart the HTTP server and the Connections cluster servers, and you are finished.

Setting path variables for search

During the installation, you set `/opt/IBM/SharedArea` which then set `/opt/IBM/SharedArea/search/stellent/dcs/oiexport` as the location for the `stellent` converters. In a multi-node cluster it is recommended to run this on the nodes themselves and not the shared area.

- ___ 1. Copy the folder `/opt/IBM/SharedArea/search/stellent` to `/opt/IBM/Connections/stellent` on both nodes in your cluster. Change the rights on the folder to `777`.
 - ___ a. In `/opt/IBM/Connections/stellent`, run `cp -rf /opt/IBM/SharedArea/search/stellent/*`.
 - ___ b. Run `chmod 777 -R *`



```

Terminal
File Edit View Terminal Tabs Help
.....:/opt/IBM/Connections # ls -l
total 8
drwxr-xr-x 3 root root 4096 Jul 26 10:28 data
drwxr-xr-x 3 root root 4096 Jul 25 16:44 stellent
.....:/opt/IBM/Connections # chmod 777 stellent/
.....:/opt/IBM/Connections # ls -l
total 8
drwxr-xr-x 3 root root 4096 Jul 26 10:28 data
drwxrwxrwx 3 root root 4096 Jul 25 16:44 stellent
.....:/opt/IBM/Connections #
  
```

Figure 243. Copying the `stellent` file on both nodes in the cluster

- ___ 2. Set up that share and then go to **Environment > WebSphere Variables and FILE_CONTENT_CONVERSION**. Change the path from the shared area to the local area on your nodes. It should be the same across both nodes.



Figure 244. Changing the path from the shared area to the local area

- ___ 3. Then, add `/opt/IBM/Connections/stellent/dcs/oiexport` to your `PATH` variable in `.profile` for the root user.

-
- ___ 4. Either add `export LD_LIBRARY_PATH=/opt/IBM/Connections/stellent/dcs/oiexport` to `/opt/IBM/WebSphere/AppServer/bin/set-upCmdLine.sh` and run `../set-upCmdLine.sh` before you start the nodes or add `export LD_LIBRARY_PATH=/opt/IBM/Connections/stellent/dcs/oiexport` and add the line to the PATH in `.profile`.

```
export PATH=$PATH:/opt/IBM/Connections/stellent/dcs/oiexport
export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/opt/IBM/Connections/stellent/dcs/oiexport
```

Figure 245. PATH variable in `.profile`

- ___ 5. Restart the computer. Then, to make sure that the variables take effect or in `/root/` folder, run `.profile`.

SiteMinder integration

How SiteMinder Works

The following diagram explains how SiteMinder Integration works when used with WebSphere TAI and a Web Agent on the IBM HTTP Server.

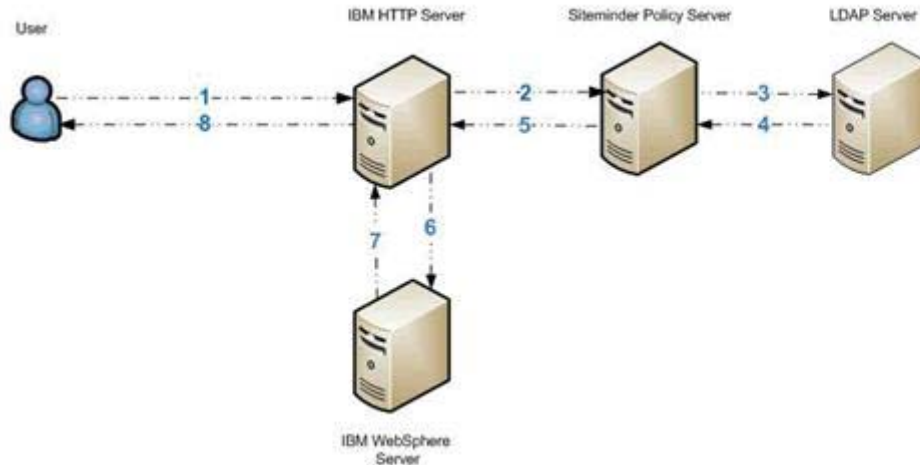


Figure 246. SiteMinder integration

The following step numbers correspond to each of the previous communications:

1. User access protected resource.
2. SiteMinder Web Agent on HTTP Server intercepts the request and prompts for Authentication.
3. User enters user name and password.
4. SiteMinder Web Agent Passes user name and password to SiteMinder Policy Server.
5. SiteMinder Policy Server attempts to Authenticates the user against the LDAP.
6. Policy Server uses the User Directory Object Details that are specified in the SiteMinder Administration Console.
7. After successful authentication, the Policy Server Authorizes the user.
8. SiteMinder checks the users and Groups assigned access in the Policy.
9. SiteMinder checks the Rules for the Requested methods and urls.
10. SiteMinder adds SMSESSION cookie to the request.
11. Request is returned to the HTTP Server.
12. SiteMinder Web Agent on the IBM HTTP Server checks for valid SMSESSION cookie.
13. Request is sent to the WebSphere Server.
14. SiteMinder ASA Agent on the WebSphere Server checks for valid SMSESSION cookie.
15. ASA Agent asserts user details to the WebSphere Server.
16. WebSphere performs its own internal authorization.
17. Allows access to the requested resource.
18. Response is returned to the HTTP Server.
19. Response sent to user with the requested resource.

Installing the SiteMinder agents

This document describes a configuration that uses SiteMinder Policy Server 6.0 SP6, SiteMinder ASA 6.0 Agent for WebSphere Application Server with CR00011 test fix, and SiteMinder Web Agent with v6qmr6-cr007. The following sections detail how to install the web agent on the HTTP Server and the application server agents on all of the nodes in your configuration.

Preparing WebSphere Application Server for SiteMinder

- ___ 1. If not already done, you must ensure that single sign-on is enabled on the Deployment Manager. On the deployment manager, go to Security > Global Security > Web and SIP Security > Sign Sign-On (SSO). Ensure that the following is set:

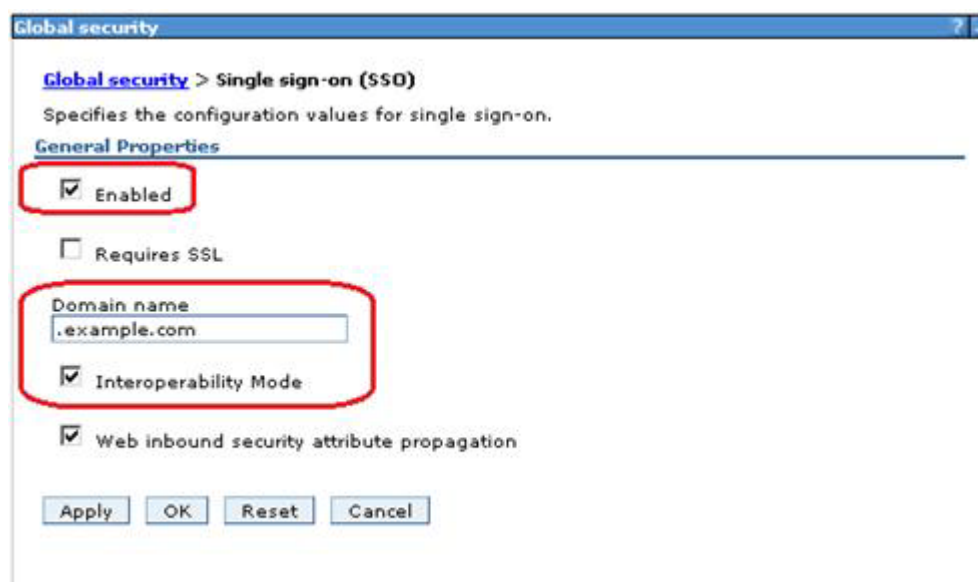


Figure 247. Specifying the configuration values for single sign-on

Copy unrestricted JCE policy files to WebSphere Application Server

- ___ 1. You must copy the unrestricted JCE policy files to the Application Server nodes and Deployment Manager computers. The `unrestricted.zip` contains:
 - * `US_export_policy.jar`
 - * `local_policy.jar`.
- ___ 2. On the two nodes and deployment manager computer, go to the following location and take a backup of the existing files and then copy in the new unrestricted versions to this location.

All servers, node agents, and deployment managers must be restarted for this change to take effect.



Figure 248. /opt/IBM/WebSphere/AppServer/java/jre/lib/security

Set up SiteMinder policy server

- ___ 1. Create agents on the SiteMinder Policy Server, including Web Agents for IBM HTTP Server and an Application Server Agent for WebSphere Application Server.
 - ___ a. Open the SiteMinder Administration console.
 - ___ b. Right-click **Agents** and click **Create Agent**.
 - ___ c. Enter details of the name and description of the Web Agent for IBM HTTP Server.
 - ___ d. Repeat these steps for the Application Server Agent.
- ___ 2. Create Agent Configuration Objects on the SiteMinder Policy Server. In the SiteMinder Administration Console, open the Agent Configuration Objects pane and complete the following steps:
 - ___ a. Configure the Web Agent for IBM HTTP Server:
 - Right-click **Apache Default Settings Agent** and select **Duplicate Configuration Object**.
 - Enter the name and description of the Agent Configuration Object.
 - Update the following parameters to match your environment:
 - **DefaultAgentName**: Name of the Apache Agent that was created earlier
 - **CookieDomain**: your_domain
where your_domain is your IBM Connections domain. If, for example, the URL is `http://activities.example.com/activities`, your host name is `activities.example.com` and your domain is `example.com`. In this example, you would set `CookieDomain=example.com`.
 - **RequireCookies**: NO
This parameter configures the Web Agent to support basic authentication but without requiring all API client programs to support cookies.
 - **BadCSSChars**: <,>
This parameter enables the Invite colleagues function in Profiles.
 - **LogOffUri**: URI
Configure SiteMinder to recognize only one web address as the logout web address.

Uncomment one of the following URLs by removing the number sign (#) character:

```
#LogOffUri="/activities/service/html/ibm_security_logout"  
#LogOffUri="/blogs/ibm_security_logout"  
#LogOffUri="/communities/communities/ibm_security_logout"  
#LogOffUri="/dogear/ibm_security_logout"  
#LogOffUri="/files/ibm_security_logout"  
#LogOffUri="/forums/ibm_security_logout"  
#LogOffUri="/homepage/web/ibm_security_logout"  
#LogOffUri="/moderation/ibm_security_logout"  
#LogOffUri="/news/ibm_security_logout"  
#LogOffUri="/profiles/ibm_security_logout"  
#LogOffUri="/search/ibm_security_logout"  
#LogOffUri="/wikis/ibm_security_logout"
```

- ___ b. Under the System tab, update the Agent Configuration Object with the following value:
FCCCompatMode: NO.
- ___ c. Configure the Application Server Agent:
 - Right-click Apache Default Settings Agent and select Duplicate Configuration Object.
 - Enter the Name and description of the Agent Configuration Object.
 - Update the following parameters to match your environment:
 - **DefaultAgentName:** Name of the Apache Agent that was created earlier
 - **CookieDomain:** your_domain
where your_domain is your IBM Connections domain. If, for example, the URL is `http://activities.example.com/activities`, your host name is `activities.example.com` and your domain is `example.com`. In this example, you would set `CookieDomain=example.com`.
 - **AssertionAuthResource:** /siteminderassertion
 - **AssertbyUserID:** True



Note

When activated, the `LogOffUri` parameter clears the `SMSESSION` cookie and ensures that the user is logged out of all IBM Connections browser sessions.

To add parameters, edit the Agent Configuration Object on the SiteMinder Policy Server. Alternatively, you can edit the `LocalConfig.conf` file on the HTTP server if the Web Agent is configured to use it.

If you are editing the SiteMinder configuration file directly, you must surround the values of SiteMinder configuration parameters with quotation marks (""); for example: `BadCSSChars="<, >".` If you are changing these parameters within the SiteMinder Policy Server, do not use quotation marks.

- ___ 3. Specify your SiteMinder Authentication Scheme configuration:
 - ___ a. Open the SiteMinder Administration Console and go to the Authentication Scheme Properties dialog box.
 - ___ b. From the Authentication Scheme type list, select Windows Authentication template.
 - ___ c. Clear the Use Relative Target check box.
 - ___ d. Complete the User DN Lookup field with the appropriate information for your domain. For example (sAMAccountName=%{UID}).
- ___ 4. On the SiteMinder Policy Server, create a domain for the IBM HTTP Server web agent.
- ___ 5. Create protected realms under the IBM HTTP Server Web Agent domain:
 - ___ a. Using the IBM HTTP Server Agent Object and Windows Authentication Scheme that you created earlier, create SiteMinder realms that Windows forms authentication protects.
 - ___ b. Realms that require forms authentication

Table 1: Realms that require forms authentication

Application	Protected URL resource
ConnectionsDefaultRealm	/
Activities	/activities/follow/atomfba /activities/service/atom2/forms /activities/service/atom2/communityEvent /activities/service/download/forms /activities/service/getnonce/forms
Blogs	/blogs/api_form /blogs/atom_form /blogs/follow/atomfba /blogs/roller-ui/blog /blogs/roller-ui/feed_form /blogs/roller-ui/rendering/api_form /blogs/roller-ui/rendering/feed_form /blogs/services/atom_form
Bookmarks	/dogear/atom_fba
Common resources	/connections/opensocial/rest
Communities	/communities/calendar/atom_form /communities/follow/atomfba /communities/forum/service/atom/forms /communities/recomm/ajax /communities/recomm/atom_form /communities/service/atom/forms
Files	/files/follow/atomfba /files/form/cmris/repository
Forums	/forums/atom/forms /forums/follow/atomfba
Metrics	/metrics /cognos

Profiles	/profiles/atom/forms /profiles/atom2/forms /profiles/follow/atomfba
Wikis	/wikis/follow/atomfba

___ 6. Using the IBM HTTP Server Agent Object that you created earlier, create SiteMinder realms that basic authentication protects.

Table 2: Realms that require basic authentication

Application	Protected URL resource
Activities	/activities/follow/atom /activities/service/download /activities/service/html/autocompleteactivityname /activities/service/html/autocompleteentryname /activities/service/html/autocompletemembers /activities/service/atom /activities/service/getnonce
Blogs	/blogs/api /blogs/atom /blogs/follow/atom /blogs/issuecategories /blogs/roller-ui/BlogsWidgetEventHandler.do /blogs/roller-ui/feed /blogs/roller-ui/rendering/api /blogs/roller-ui/rendering/feed /blogs/services/atom
Bookmarks	/dogear/api/app /dogear/api/deleted /dogear/api/notify /dogear/atom
Common resources	/connections/opensocial/basic/rest
Communities	/communities/calendar/atom /communities/calendar/handleEvent /communities/calendar/ical /communities/follow/atom /communities/forum/service/atom /communities/recomm/atom /communities/recomm/handleEvent /communities/service/atom /communities/service/json
Files	/files/basic/api /files/basic/cmis /files/basic/opensocial /files/follow/atom
Forums	/forums/atom /forums/follow/atom
Home page	/homepage/atom/search /homepage/atom/mysearch
News	/news/atom/service /news/atom/stories/newsfeed /news/atom/stories/public /news/atom/stories/saved /news/atom/stories/statusupdates /news/atom/stories/top /news/atom/watchlist /news/atomfba/stories/public

Profiles	/profiles/atom /profiles/atom2 /profiles/audio.do /profiles/follow/atom /profiles/json /profiles/photo.do /profiles/vcard
Wikis	/wikis/basic/api /wikis/follow/atom



Optional

Protect login credentials with encryption: Using the Basic over SSL Template scheme, create a SiteMinder Authentication Scheme and apply the new Authentication Scheme to all the SiteMinder realms that require basic authentication.

- ___ 7. Create Delete and Head actions for the Web Agent. By default, the Web Agent has only the Get, Post, and Put actions available. To add the Delete and Head actions, complete the following steps:
 - ___ a. In the SiteMinder Administration Console, click **View** and click **Agent Types**.
 - ___ b. Click **Agent Types** in the Systems pane.
 - ___ c. Double-click **Web Agent** in the Agent Type list.
 - ___ d. In the Agent Type Properties dialog box, click **Create**.
 - ___ e. Enter "Delete" in the New Agent Action dialog box and click **OK**.
 - ___ f. Enter "Head" in the New Agent Action dialog box and click **OK**.
 - ___ g. Click **OK** again to save the new action.
- ___ 8. Create the following rules for each realm:

Table 3: Rules for the IBM HTTP Server realmsGetPostPutDelHead rule

GetPostPutDelHead rule	OnAuthAccept rule
Realm: CurrentRealm	Realm: CurrentRealm
Resource: * (not /*)	Resource: * (not /*)
Action: Web Agent actions -> Get,Post,Put,Delete,Head	Action: Authentication events -> OnAuthAccept
When this Rule fires: Allow Access	When this Rule fires: Allow Access
Enable or Disable this Rule: Enabled	Enable or Disable this Rule: Enabled

- ___ 9. Create a policy and add the users who can access the server to the policy. You can allow all users in the LDAP directory or a subset of users; for example: an LDAP branch, individual users, or groups of users.
- ___ 10. Add the new rules to the new policy.
- ___ 11. Specify realms that SiteMinder does not protect.

**Note**

You must configure notification templates and some Atom feeds as unprotected URLs. The Blogs footer page must also be unprotected because Blogs uses the Velocity template to extract footer pages.

Table 4: Realms that do not require authentication

Application	Unprotected URL resource
Activities	/activities/auth /activities/images /activities/oauth /activities/service/html/images /activities/service/html/mainpage /activities/service/html/styles /activities/service/html/themes /activities/service/html/servermetrics /activities/service/html/serverstats /activities/serviceconfigs /activities/static/
Blogs	/blogs/oauth /blogs/serviceconfigs /blogs/static/
Bookmarks	/dogear/oauth /dogear/peoplelike /dogear/serviceconfigs /dogear/static/
Common resources	/connections/bookmarklet/tools/blet.js /connections/bookmarklet/tools/discussThis.js /connections/bookmarklet/tools/rlet.js /connections/core/oauth /connections/oauth /connections/resources/ic /connections/resources/socmail-client /connections/resources/socpim /connections/resources/web /nav/common
Communities	/communities/calendar/Calendar.xml /communities/calendar/oauth /communities/comm.widget /communities/images /communities/nav /communities/recomm/oauth /communities/resourceStrings.do /communities/service/atom/oauth /communities/service/html/communityview /communities/service/html/community/autoCompleteMembers.do /communities/service/html/singleas /communities/service/opensocial/oauth /communities/serviceconfigs /communities/static/ /communities/stylesheet /communities/tools/embedAS.html /communities/widgets

Files	/files/app /files/basic/anonymous/api /files/basic/anonymous/cmisis /files/basic/anonymous/opensocial /files/form/anonymous/api /files/form/anonymous/cmisis /files/form/anonymous/opensocial /files/oauth /files/static/
Forums	/forums/oauth /forums/serviceconfigs /forums/static/
Home page	/homepage/oauth /homepage/search /homepage/serviceconfigs /homepage/static/ /homepage/web/updates/
Metrics	/metrics/service/eventTracker /metrics/service/oauth /cognos/servlet
Moderation	/moderation/app /moderation/oauth /moderation/static
News	/help /news/microblogging/isPermitted.action /news/follow/oauth /news/oauth /news/serviceconfigs /news/sharebox/config.action /news/static/
OAuth Provider	/oauth2
Profiles	/profiles/atom/forms/connections.do /profiles/images /profiles/oauth /profiles/serviceconfigs /profiles/static/
Search	/search/atom/search /search/oauth /search/static/
Widget container	/connections/opensocial/anonymous/rest /connections/opensocial/common /connections/opensocial/gadgets /connections/opensocial/ic /connections/opensocial/oauth /connections/opensocial/rpc /connections/opensocial/social /connections/opensocial/xrds /connections/opensocial/xpc
Wikis	/wikis/basic/anonymous/api /wikis/form/anonymous/api /wikis/home /wikis/js /wikis/oauth /wikis/static/

___ 12. On the SiteMinder Policy Server, create a domain for the Application Server Agent.

___ 13. Add the following realm to the new WebSphere Application Server domain:

Table 5: SiteMinder realms for WebSphere Application Server

Realm name	Protected resource
SM TAI Validation	/siteminderassertion

**Note**

You must configure the Protected Resource of this realm to match the AssertionAuthResource parameter that you configured earlier for the Application Server Agent.

- __ 14. Set the timeout value of the session for each realm.
 - __ a. In the SiteMinder Policy Server, open the **Realm Dialog** and click **Session**.
 - __ b. In the Session Timeouts Group Box, enter timeouts for each realm. Enter the following values, if they are not already present:
 - **Maximum Timeout Enabled:** 2 Hours 0 Minutes.
 - **Idle Timeout Enabled:** 1 Hours 0 Minutes.

**Note**

The maximum timeout and the idle timeout must be longer than the LTPA token timeout, which is defined in WebSphere Application Server. The LTPA token timeout is set to 120 minutes by default.

Install the Web Agent on the IBM HTTP Server

- __ 1. Extract all files from the compressed file that the CS SiteMinder contact provides.
- __ 2. Run the WebAgent executable file (usually named in the following format:
 nete-wa-6qmrX-platform.exe for example, nete-wa-6qmr5-rhel130.bin.

```

Terminal
File Edit View Terminal Tabs Help
~/Siteminder/sm # ls -l
total 91476
-rw-r--r-- 1 root root 93569656 Sep  7  2011 nete-wa-6qmr6-cr007-rhel130.bin
~/Siteminder/sm # chmod 777 nete-wa-6qmr6-cr007-rhel130.bin
~/Siteminder/sm # ls -l
total 91476
-rwxrwxrwx 1 root root 93569656 Sep  7  2011 nete-wa-6qmr6-cr007-rhel130.bin
~/Siteminder/sm # ./nete-wa-6qmr6-cr007-rhel130.bin
Preparing to install...
Extracting the JRE from the installer archive...
Unpacking the JRE...
Extracting the installation resources from the installer archive...
Configuring the installer for this system's environment...

Launching installer...
  
```

Figure 249. WebAgent

- ___ 3. The Introduction screen is displayed. Click **Next**.

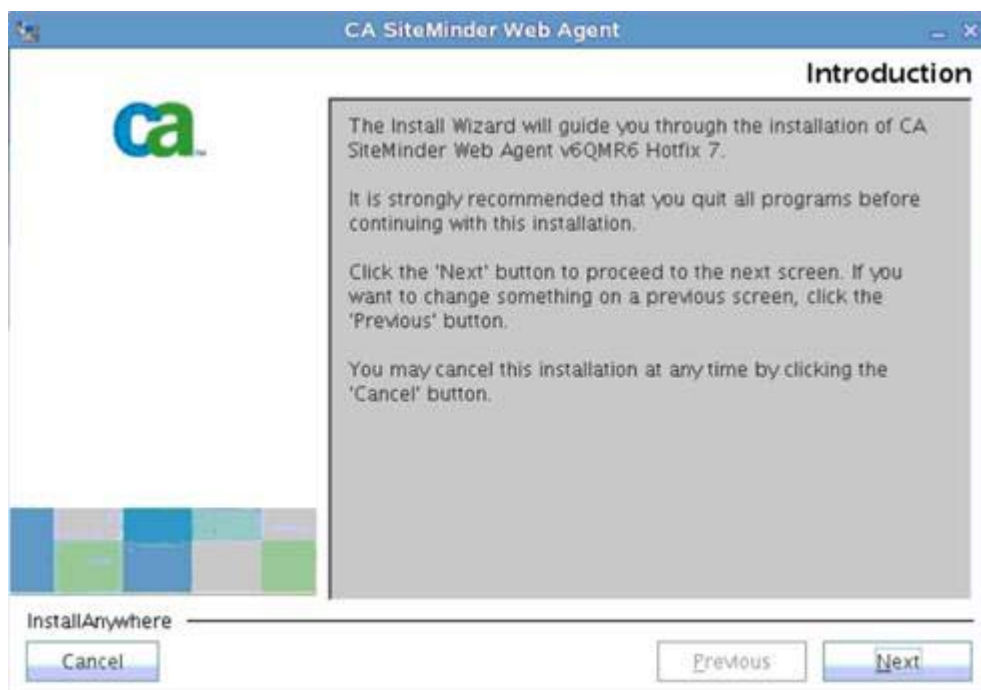


Figure 250. CA SiteMinder Web Agent: Introduction

- ___ 4. Accept the license agreement and click **Next** to continue.



Figure 251. CA SiteMinder Web Agent: License Agreement

5. On the Important Information screen, click **Next** to continue.

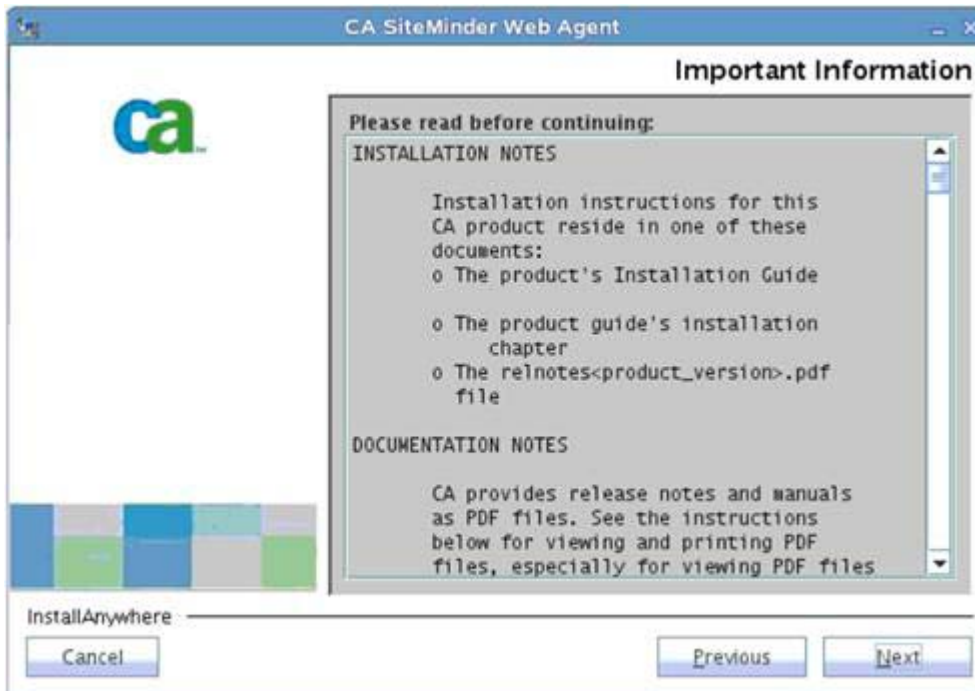


Figure 252. CA SiteMinder Web Agent: Important Information

6. On the Choose Install Location screen, select the default location for the installation of the WebAgent (/opt/netegrity/webagent) or click **Choose** to select a location of your choice. When selected, click **Next**.



Figure 253. CA SiteMinder Web Agent: Choose Install Location

- ___ 7. Review the pre-installation summary screen and click **Install**.



Figure 254. CA SiteMinder Web Agent: Pre-Installation Summary

The installation begins.



Figure 255. CA SiteMinder Web Agent: Installation in progress

- ___ 8. On the Install Complete screen, accept the defaults and click **Done**.



Figure 256. CA SiteMinder Web Agent: Install Complete

- ___ 9. Start the web agent configuration wizard.

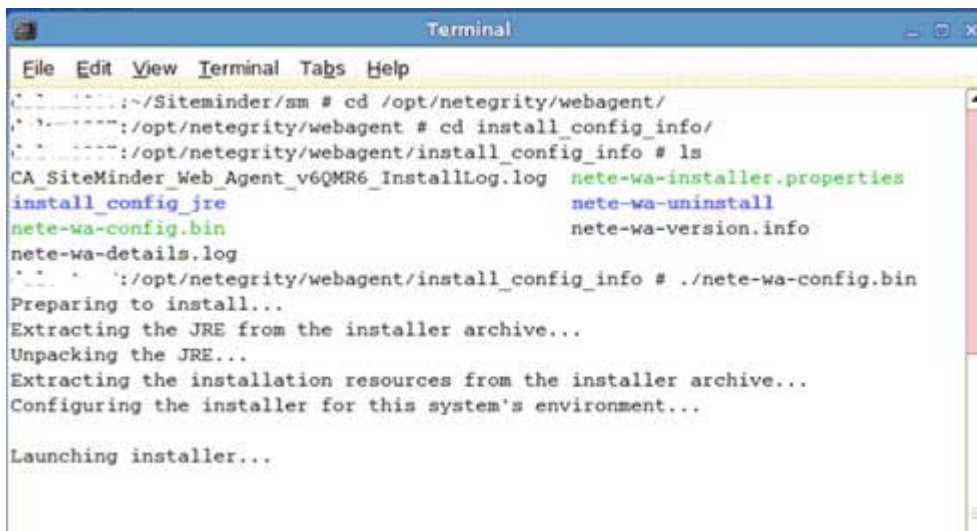


Figure 257. Starting the web agent configuration wizard

- ___ 10. The Web Agent Configuration wizard then starts. On the Host Registration screen, select “Yes, I would like to do Host Registration now”. Then, click **Next**.



Figure 258. CA SiteMinder Web Agent: Host Registration

- ___ 11. On the Admin Registration screen, enter the SiteMinder Administrator name and password that the CS SiteMinder Contact supplies. Do not select “Enable Shared Secret Rollover”. Then, click **Next**.



Figure 259. CA SiteMinder Web Agent: Admin Registration

- 12. On the “Trusted Host Name and Configuration Object” screen, enter the Trusted Host Name and Host Configuration Object that the CS SiteMinder Contact supplies. Then, click **Next**.

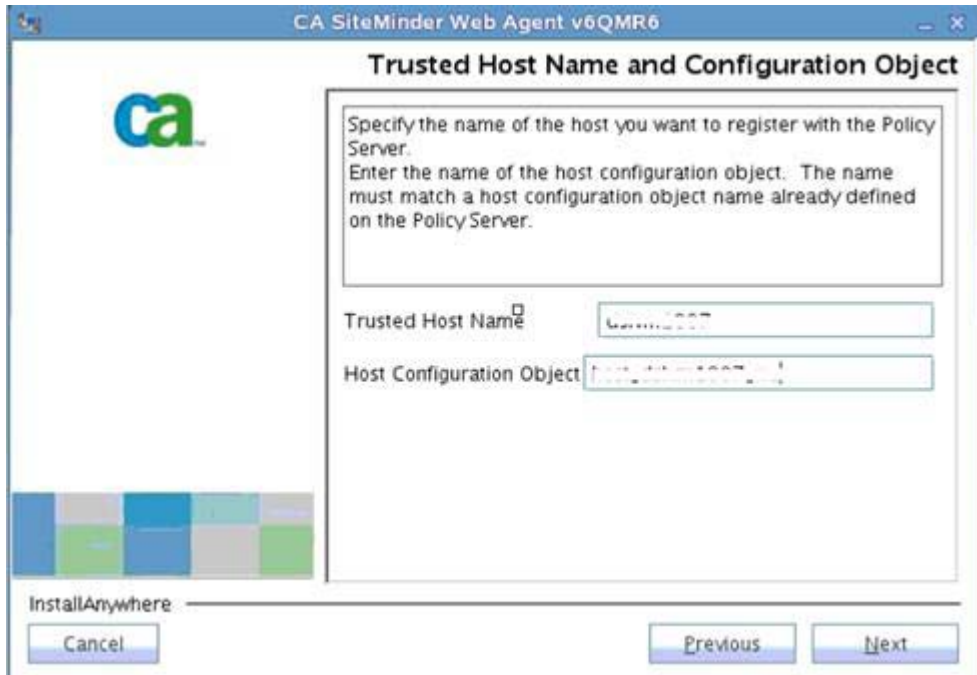


Figure 260. CA SiteMinder Web Agent: Trusted Host Name and Configuration Object

- 13. On the Policy Server IP Address screen, enter the SiteMinder Policy Server IP address that the CS SiteMinder Contact supplies and click **Add**. Then, click **Next**.



Figure 261. CA SiteMinder Web Agent: Policy Server IP Address

- ___ 14. On the Host Configuration file location screen, accept the default file name and location and click **Next**.

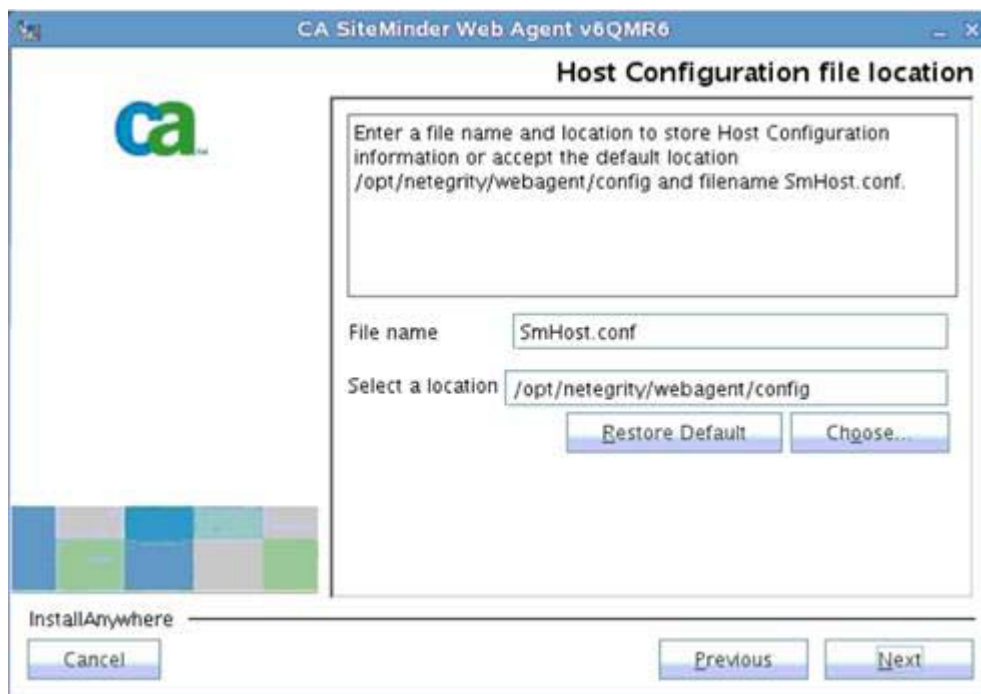


Figure 262. CA SiteMinder Web Agent: Host Configuration file location

- ___ 15. On the Select Web Server(s) screen, select the Apache server that you want to configure with the WebAgent from the available listing by selecting it in the list and then click **Next**.

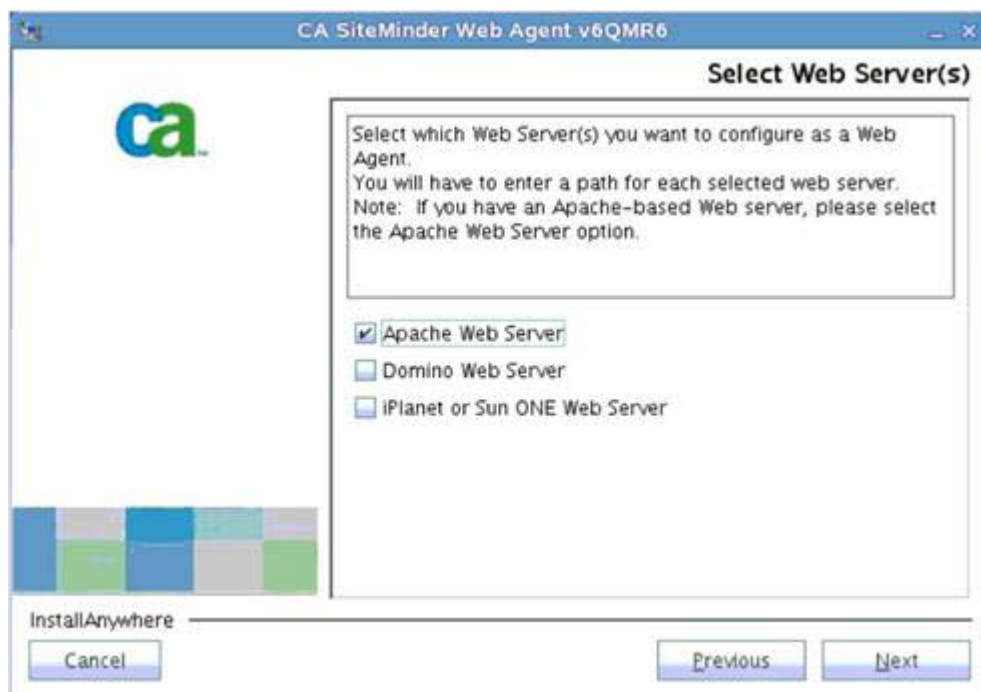


Figure 263. CA SiteMinder Web Agent: Select Web Server(s)

__ 16. Enter the Apache Web server path and click **Next**.

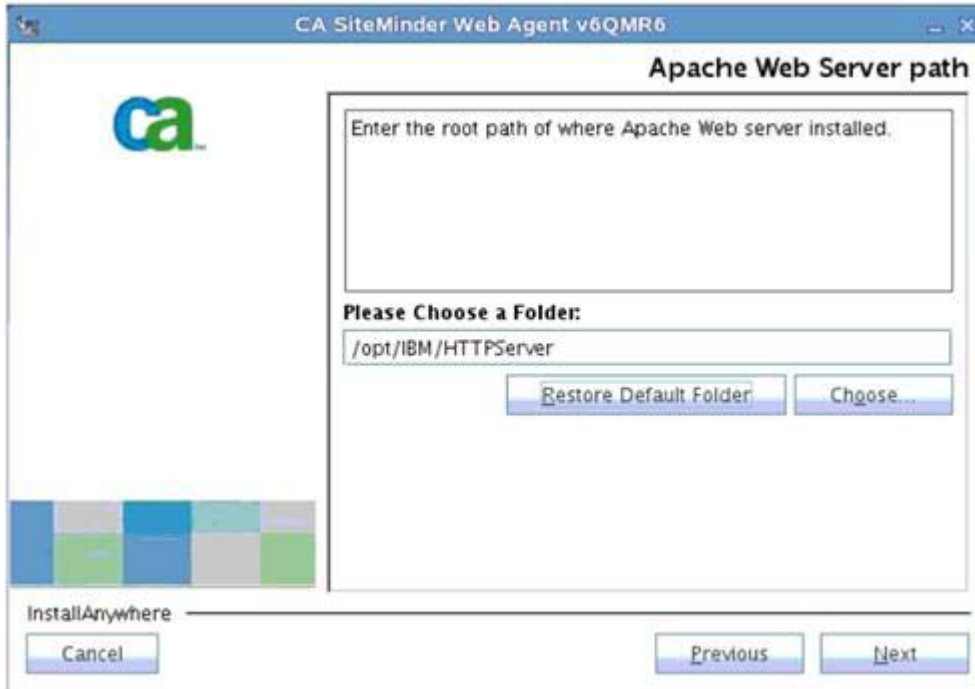


Figure 264. CA SiteMinder Web Agent: Apache Web Server path

__ 17. Choose “I would like to enter a specific configuration path.” Click **Next** to continue.



Figure 265. CA SiteMinder Web Agent: Apache Web Server Failure

___ 18. Choose the Apache server path and click **Next** to continue.



Figure 266. CA SiteMinder Web Agent: Apache Web Server path

___ 19. Select the Apache version and click **Next** to continue.

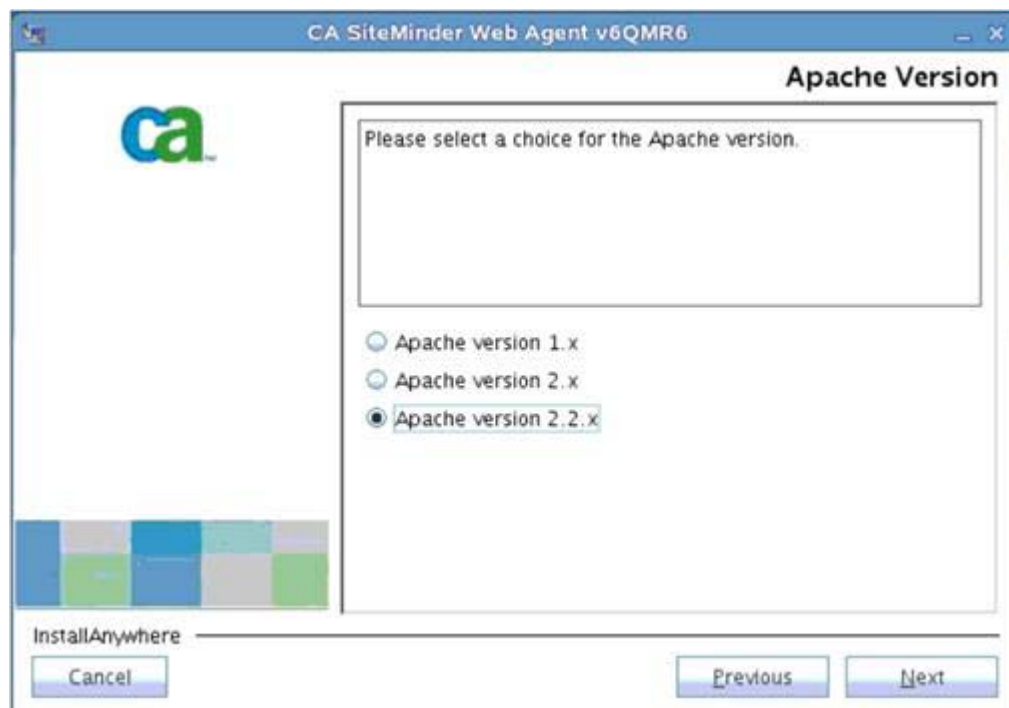


Figure 267. CA SiteMinder Web Agent: Apache version

___ 20. Select the Apache Server Type and click **Next**.



Figure 268. CA SiteMinder Web Agent: Apache Server Type

___ 21. Select the Web Server that you want to configure as web agent and click **Next**.



Figure 269. CA SiteMinder Web Agent: Select Web Server(s)

___ 22. Input the Agent Configuration Object and click **Next**.



Figure 270. CA SiteMinder Web Agent: Agent Configuration Object

___ 23. Select the advanced authentication to use depending on your requirements and click **Next**.

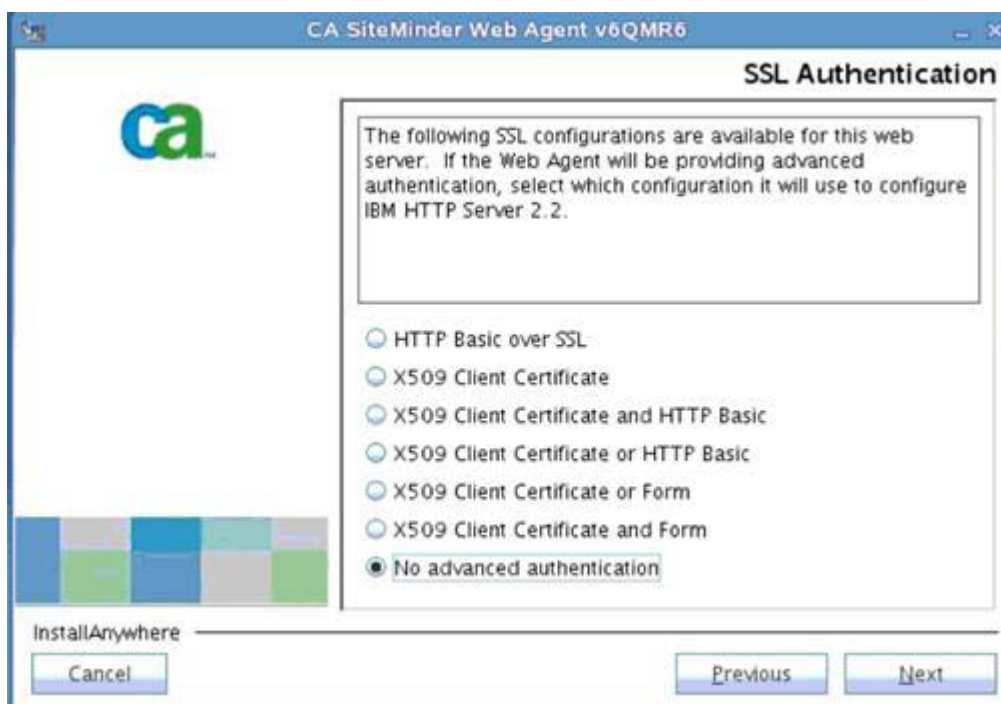


Figure 271. CA SiteMinder Web Agent: SSL Authentication

___ 24. At the following panel click “No, I don't want to configure Self Registration” and click **Next**.



Figure 272. CA SiteMinder Web Agent: Self Registration

___ 25. Review the web agent configuration options and click **Install**.



Figure 273. CA SiteMinder Web Agent: Web Server Configuration Summary

- __ 26. The WebAgent is then configured and then the Configuration Complete screen displays. Click **Done** to complete the configuration process.



Note

You can ignore any message about warnings that occurred during the installation. These warnings appear by default during the installation.

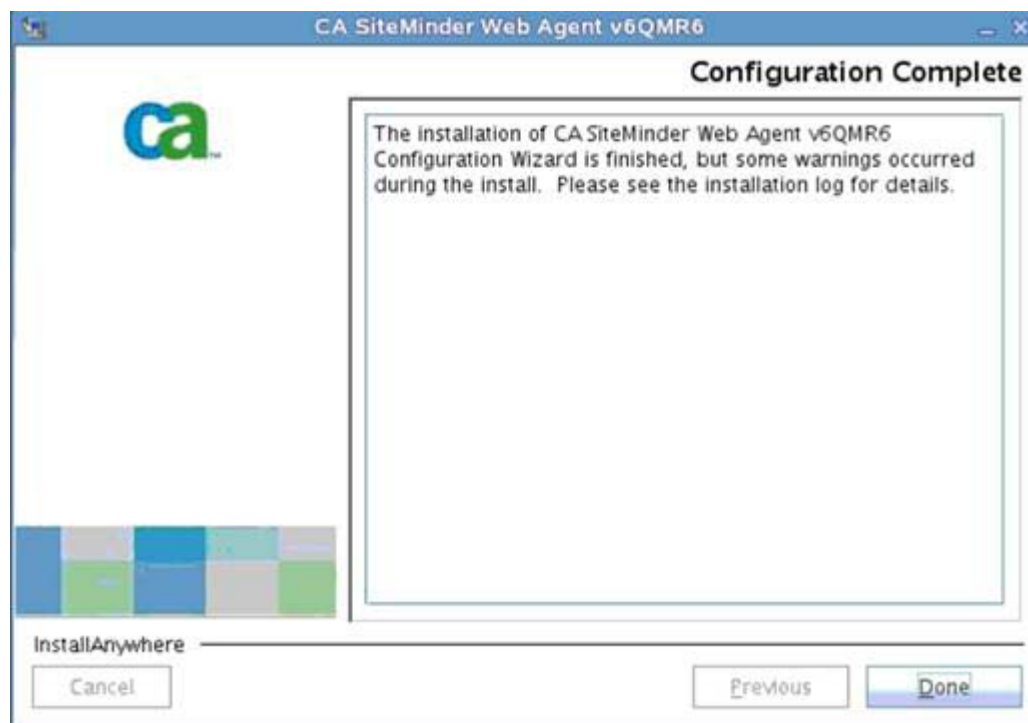


Figure 274. CA SiteMinder Web Agent: Configuration Complete

- __ 27. Check the `Install.log`. You should see something like this screen:

```

/opt/netegrity/webagent/install_config_info # tail -f CA_SiteMinder_Web_Agent_
v6QMR6_InstallLog.log

Install Action:          InstallAnywhere Variable
                        Status: SUCCESSFUL

Modify Text File - Single File:  New File /root/netegrity/install-info/nete-install-his
tory.log
                        Status: SUCCESSFUL

Modify Text File - Single File:  No Target Chosen
                        Status: SUCCESSFUL

```

Figure 275. Installation log

- __ 28. Registration:
- __ a. CD to `/opt/netegrity/webagent`.
 - __ b. Run `./nete_wa_env.sh`.

- ___ c. Register the web agent with the policy server where `< ./smreghost -i SM policy server -u admin_id -p admin_pwd -hn webagent_hostname -hc hostconfig_object>` for example `< ./smreghost -i SM_Policy_Server -u RegHost -p RegHost -hn connections -hc host_connections>`.
- ___ d. Check the `webagent.config` file in `/opt/IBM/HTTPServer/conf` that `EnableWebAgent="YES"`.
- ___ e. Start the HTTP server.
- ___ f. run `./envvars-std`.
- ___ g. `./apachectl start`.

SiteMinder should prompt you to go to the HTTP web server page.

- ___ 29. After configuring the web agent as explained, find the `WebAgent.conf` in the `HTTPServer/conf` directory. Open this file and edit it so `EnableWebAgent=YES`.
- ___ 30. Now restart your HTTP Server. When attempting to access the HTTP Server root, you should now see the SiteMinder login screen and be able to log in to get the IBM HTTP Server splash screen. This screen indicates that SiteMinder is set up correctly with the WebAgent. Enter your user name and password.



Figure 276. SiteMinder login screen

The WebSphere software home page is displayed.



Figure 277. WebSphere software home page

Install Application Server Agent

Install the Application Server Agent on both nodes: `node1.machine.com` and `node2.machine.com` in the example.



Important

You must set the session to point to the WebSphere Java path. For example, in `.profile`, add `<PATH=/opt/IBM/WebSphere/AppServer/java/bin:$PATH:$HOME/bin:/opt/IBM/Connections/s tellent/dcs/oiexport:/opt/IBM/WebSphere/AppServer/java>`.

1. Start the TAI agent installation by using the following `jar` command: `<java: jar ca-asa-6.0-cr11-was.jar>` for the application server agent. The eTrust SiteMinder Application Server Agent v6.0 for WebSphere opens.



Figure 278. CA eTrust SiteMinder Agent v6.0 for WebSphere: Introduction

2. You see an introduction screen. Click **Next** to continue.



Figure 279. CA eTrust SiteMinder Agent v6.0 for WebSphere: Introduction

3. Accept the license agreement. Click **Next** to continue.



Figure 280. CA eTrust SiteMinder Agent v6.0 for WebSphere: License Agreement

- ___ 4. Choose an installation folder and click **Next** to continue.



Figure 281. CA eTrust SiteMinder Agent v6.0 for WebSphere: Choose Install Folder

- ___ 5. Choose an installation folder for WebSphere and click **Next** to continue.



Figure 282. CA eTrust SiteMinder Agent v6.0 for WebSphere: Choose WebSphere Folder

___ 6. Select “Yes, create trusted host” and click **Next** to continue.



Figure 283. CA eTrust SiteMinder Agent v6.0 for WebSphere: Host registration

___ 7. Enter the information of the SiteMinder server and click **Next** to continue.



Figure 284. CA eTrust SiteMinder Agent v6.0 for WebSphere: Host registration

- ___ 8. Enter the agent configuration object name and click **Next**.



Figure 285. CA eTrust SiteMinder Agent v6.0 for WebSphere: Agent Configuration

- ___ 9. Review any errors messages in the installation log. In this case, they are benign errors. Click **Done** to exit the wizard.
- ___ 10. Check the installation log reports like in the following figure and make sure that there are no unrecoverable errors.

```

[redacted]:/opt/smwasa # cd log
[redacted]:/opt/smwasa/log # ls
CA_eTrust_SiteMinder_Agent_v6.0_for_WebSphere_InstallLog.log
dslvm1008:/opt/smwasa/log # tail -f CA_eTrust_SiteMinder_Agent_v6.0_for_WebSphere_InstallLog.log

Modify Text File - Single File: AsaAgent-az.conf
                        Status: SUCCESSFUL

Modify Text File - Single File: smagent.properties
                        Status: SUCCESSFUL

Modify Text File - Multiple Files: conf
                        Status: SUCCESSFUL

```

Figure 286. Installation log

Post-agent installation actions

When you installed the various SiteMinder agents on your nodes and web server, turn your attention to the following tasks. You must enable the trust association interceptor from the deployment manager and set up various rules on the web server to handle logging out from SiteMinder correctly. Also, you must configure the SiteMinder custom authenticator.

Actions on WebSphere Application Server post-agent installation

1. When the Application Server Agent is configured ensure to copy `smagent.properties` from the agent installation directory: `smwasasa\conf` to `AppServer\profiles\AppSrv01\properties` on each node.

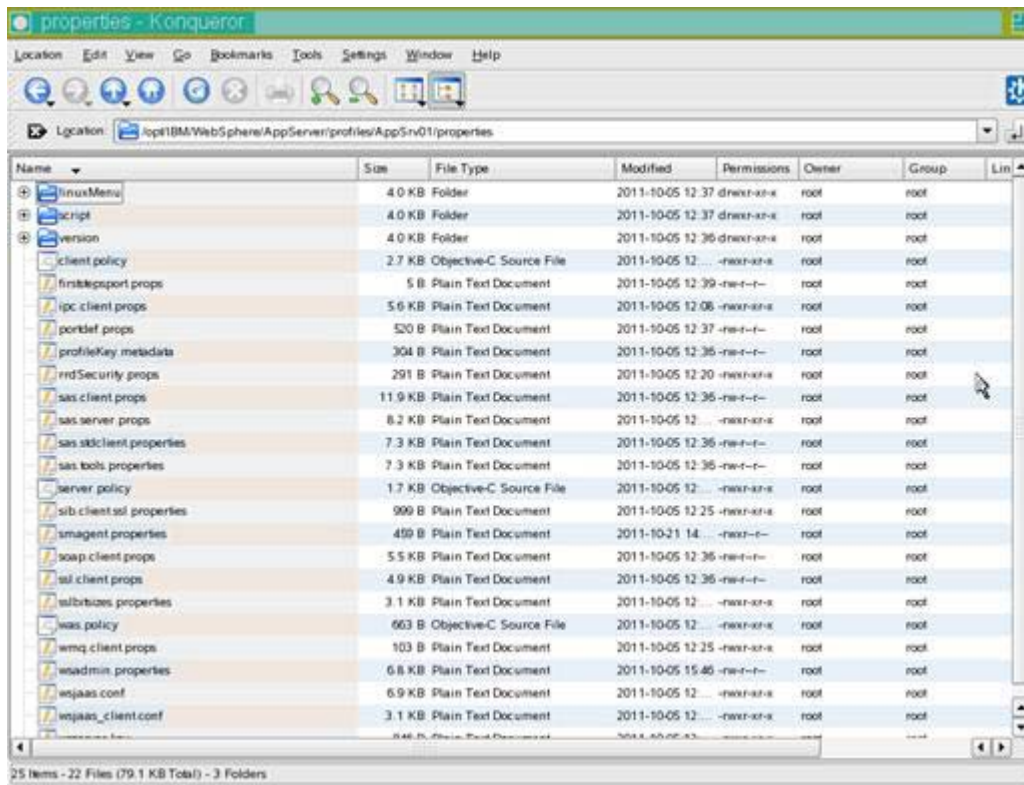


Figure 287. Properties: Konqueror

2. Next, on the Deployment Manager configure Trust Association Interceptor on WebSphere Application Server. From the deployment manager administrative console for WebSphere Application Server, click **Security > Global security > Web and SIP security**, click **Trust association**. Click **Enable Trust Association** and then click **Save**.



Figure 288. Global Security

3. Next, back in the trust association screen, click **Interceptors**, click **New**, and add an interceptor with the following name (com.netegrity.siteminder.websphere.auth.SmTrustAssociationInterceptor). Click **OK** and save the change.

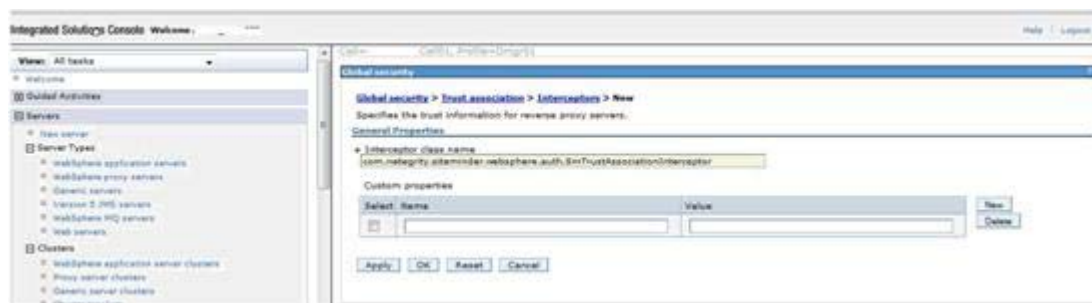


Figure 289. Interceptors: General properties

4. It is OK to delete any unused interceptors. Leaving these interceptors in place causes no issues but results in error messages in the logs during startup so it makes sense to delete these interceptors. Click **Delete** and save this change. You must not delete the `oauth` interceptor (`com.ibm.ws.security.oauth20.tai.OAuthTAI`). It is required for `oauth` to work properly. After this step, you have two interceptors for `oauth` and for SiteMinder.

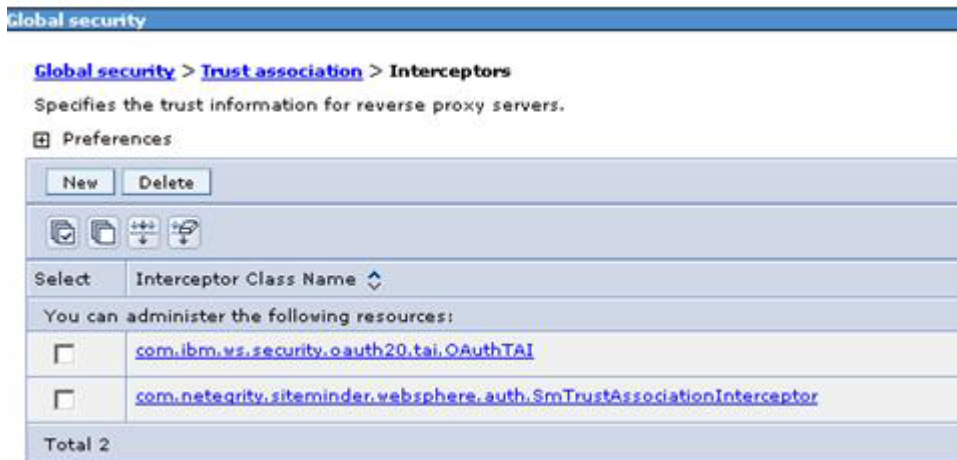


Figure 290. Interceptors: Preferences

Actions on HTTP Server after the agent installation

1. Create rewrite rules to remap Atom API requests and to redirect URLs when users log out of Lotus Connections. Open the IBM HTTP Server `httpd.conf` configuration file. The file is stored in the `/opt/IBM/HTTPServer/conf` directory on the web server computer. The following extracted section of the `httpd.conf` shows these rules that are implemented in both the HTTP and HTTPS sections of this file. In this extract, the logout rules redirect users to the home page logout screen, and when they are logged out they are redirected to the page at `home.example.com`.
2. When this change is made save and close the `httpd.conf` file. Restart the IBM HTTP Server.



Note

Uncomment `LoadModule rewrite_module modules/mod_rewrite.so` line in the `httpd.conf` file. This line is commented out by default. When the line is commented out, the web server does not start.

```
RewriteEngine on
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteCond %{QUERY_STRING} !=logoutExitPage=http://home.example.com
RewriteRule /(.*)/ibm_security_logout(.*)
/homepage/web/ibm_security_logout?logoutExitPage=http://home.example.com
[noescape,L,R]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/api/(.*) /blogs/roller-ui/rendering/api/$1/api/$2
```



```

[R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/tags/atom(.*)
/blogs/roller-ui/rendering/feed/$1/tags/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/entries/atom(.*)
/blogs/roller-ui/rendering/feed/$1/entries/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/comments/atom(.*)
/blogs/roller-ui/rendering/feed/$1/comments/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/blogs/atom(.*)
/blogs/roller-ui/rendering/feed/$1/blogs/atom/ [R,L]
#Connections Config for SSL
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName connections.example.com
SSLEnable

RewriteEngine on
RewriteCond %{REQUEST_URI} /(.*)/ibm_security_logout(.*)
RewriteCond %{QUERY_STRING} !=logoutExitPage=http://home.example.com
RewriteRule /(.*)/ibm_security_logout(.*)
/homepage/web/ibm_security_logout?logoutExitPage=http://home.example.com
[noescape,L,R]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/api/(.*) /blogs/roller-ui/rendering/api/$1/api/$2
[R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/tags/atom(.*)
/blogs/roller-ui/rendering/feed/$1/tags/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/entries/atom(.*)
/blogs/roller-ui/rendering/feed/$1/entries/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/comments/atom(.*)
/blogs/roller-ui/rendering/feed/$1/comments/atom/ [R,L]
RewriteCond %{REQUEST_URI} !^/blogs/roller-ui/rendering/(.*)
RewriteRule ^/blogs/(.*)/feed/blogs/atom(.*)
/blogs/roller-ui/rendering/feed/$1/blogs/atom/ [R,L]
</VirtualHost>
</IfModule>
SSLDisable

```

Configure IC Custom Authenticator for SiteMinder

The `customAuthenticator` element in the `LotusConnections-config.xml` file defines some key parameters of your single sign-on (SSO) solution. The configuration settings that you can specify in this XML element affect only back-end inter-service communication in an SSO environment. The attributes for the `customAuthenticator` element can differ, depending on the SSO solution that you implemented. Most attributes are optional, but some might be mandatory in the context of your SSO solution.



Information

For more information, see the relevant topics for your authentication solution and the information center topic that is dedicated to this subject.

1. Add a SiteMinder authenticator property to the Lotus Connections configuration by editing the `LotusConnections-config.xml` file. Start the `wsadmin` client and check out the Lotus Connections configuration file.

```

[redacted]:/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin # ./wsadmin.s
h -lang jython -username Aamir_001_077 -password [redacted]
WASX7209I: Connected to process "dmgr" on node [redacted] CellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"

```

Figure 291. LotusConnections-config.xml

```

wsadmin>execfile("connectionsConfig.py")
Connections Administration initialized
wsadmin>

```

Figure 292. LotusConnections-config.xml

```

wsadmin>LCConfigService.checkOutConfig("/opt/temp", "[redacted] Cell01") 1.3
Connections configuration file successfully checked out
wsadmin>print AdminControl.getCell() 0AP
[redacted] Cell01
WASX7031I: For help, enter: "print Help.help()"

```

Figure 293. LotusConnections-config.xml

2. Update the custom authenticator values by running the following commands and configure the custom authenticator to support server-to-server authentication for SiteMinder.

```

wsadmin>LCConfigService.updateConfig("customAuthenticator.name", "SiteminderAuthenticator")
Changing name from DefaultAuthenticator to SiteminderAuthenticator
Loading schema file for validation: /opt/temp/LotusConnections-config.xsd
Loading schema file for validation: /opt/temp/service-location.xsd
/opt/temp/LotusConnections-config CHANGED .xml is valid

```

Figure 294. Updating and configuring the custom authenticator values

3. Set the value of the `custom.authenticator.cookieTimeout` parameter to be equal to or less than the maximum timeout and idle timeout values already configured. To do so, you

must open the `LotusConnections-config.xml` from the `/opt/temp` directory and apply the change manually. As the key `CookieTimeout` is not yet part of this file. Specify the timeout value in minutes. In this case 60 minutes is the specified timeout value.



Note

When your production environment is ready, set the `AllowSelfSignedCerts` property to `false`. In a similar fashion to adding `CookieTimeout`, you must do it manually on the checked out `LotusConnections-config.xml` before checking it back in.

4. The following line is a snippet of the content of the XML as it should look when updated with the previous values:

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

Check the `LotusConnections-config.xml` file back in by running the following command:

```
wsadmin>LCConfigService.checkOutConfig("/opt/temp", "Cell01")
Connections configuration file successfully checked out
wsadmin>
```

Figure 295. Checking the `LotusConnections-config.xml` file

```
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
  workingDirectory: /opt/temp
  cellName: Cell01
  nodeName: None
  serverName: None
Loading schema file for validation: /opt/temp/LotusConnections-config.xsd
Loading schema file for validation: /opt/temp/service-location.xsd
/opt/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>
```

Figure 296. Checking the `LotusConnections-config.xml` file

- ___ 5. Update the reauthenticate property in the files-config.xml file. When this property is set to false, and when a Lotus Connections application detects a session timeout, users must log in again through the SSO authentication mechanism. To update the reauthenticate property, complete the following steps:
 - ___ a. Log in to the wsadmin client.
 - ___ b. Run the following command to load files administration: `execfile("filesAdmin.py")`.

```
wsadmin>execfile("/opt/IBM/WebSphere/DeploymentManager/profiles/Dmgr01/bin/filesAdmin.py")
1: WebSphere:name=FilesSchedulerMBean,process=Cluster2_server1,platform=dynamicproxy,node=dslvm1008Node01,version=7.0.0.19,type=LotusConnections,mbeanIdentifier=FilesSchedulerMBean,cell=Cell01,spec=1.0
Which service do you want to connect to?
1
2: WebSphere:name=FilesSchedulerMBean,process=Cluster2_server2,platform=dynamicproxy,node=dslvm1008Node01,version=7.0.0.19,type=LotusConnections,mbeanIdentifier=FilesSchedulerMBean,cell=Cell01,spec=1.0
Which service do you want to connect to?
1
Connecting to WebSphere:name=FilesAdminService,type=LotusConnections,cell=Cell01,node=Node01,*
Files Administration initialized.
wsadmin>
```

Figure 297. Loading file administration

- ___ 6. Run the following command to check out the files configuration file:
`FilesConfigService.checkOutConfig("/opt/temp","Cell01"):`

```
wsadmin>FilesConfigService.checkOutConfig("/opt/temp","Cell01")
Files configuration files successfully checked out.
wsadmin>
```

Figure 298. Checking out the files configuration files

- ___ 7. Update the reauthenticate property by running the following command:
`FilesConfigService.updateConfig("security.reauthenticateAndSaveSupported", "false")`.

```
wsadmin>FilesConfigService.updateConfig("security.reauthenticateAndSaveSupported", "false")
/opt/temp/files-config.xml
Changing reauthenticateAndSaveSupported from false to false
Loading schema file for validation: /opt/temp/files-config.xsd
/opt/temp/files-config_CHANGED.xml is valid
wsadmin>
```

Figure 299. Updating the reauthenticate property

- ___ 8. Finally, check in the files-config.xml file by running the following command:
FilesConfigService.checkInConfig().

```
wsadmin>FilesConfigService.checkInConfig()
Using configuration arguments :
  workingDirectory: /opt/temp
  cellName: [REDACTED]Cell101
  nodeName: None
  serverName: None
Loading schema file for validation: /opt/temp/files-config.xsd
/opt/temp/files-config.xml is valid
Loading schema file for validation: /opt/temp/mime-files-config.xsd
/opt/temp/mime-files-config.xml is valid
Files configuration files successfully checked in.
wsadmin>
```

Figure 300. Checking the files-config.xml file

