

[Home](#) > [Deployment Scenarios](#) > Scenario 1 : Installing Lotus Connections 3.0 - Small Deployment☆☆☆☆☆
(0 ratings)

Scenario 1 : Installing Lotus Connections 3.0 - Small Deployment

► Abstract

[Scroll up for Table of Contents](#)

Overview

This scenario describes how to deploy Lotus Connections 3.0 in a small environment. This type of deployment involves three machines - LDAP, Database and the WebSphere Application Server, which hosts Lotus Connections. This deployment would be typical of a test or pilot deployment. This article is designed as an end-to-end guide to deploying Lotus Connections 3.0, including all prerequisites in a step-by-step process.

To access a PDF version of this content, download the [Scenario1.pdf](#).

Scenario Description

Summary

This scenario is designed as an end-to-end guide to deploying Lotus Connections 3.0 in a single server environment where both the cell and node share the same machine. Full system specifications and a list of software used in this configuration are outlined in the Environment Hardware and Software Specifications topic in this article. The following properties describe the environment in more detail.

Operating system

Microsoft Windows Server 2008 Enterprise Edition x86-64

Database Server

IBM DB2 9.7 FP2

User Directory

IBM Tivoli Directory Server v6.2

Plug-ins Supported

All plug-ins are supported in this environment.

WebSphere Topology

All applications will run under one Java Virtual Machine. This means that all applications will be installed into the same server instance.

Secure Sockets Layer (SSL)

SSL is configured in this scenario; however, SSL communications are not forced by Lotus Connections. This is the default configuration of Lotus Connections, meaning that unless the user inputs "https" manually when accessing Lotus Connections, all traffic will not be encrypted with SSL (with the exception of login). When logging in to Lotus Connections, SSL is always used to encrypt user credentials and after the user is authenticated, they are redirected back to standard HTTP protocol.

Other Product Integration

There is no integration with other IBM products in this scenario.

Mail Integration

A Java mail session is used in this scenario.

Additional Security

There are no additional security layers in this deployment.

Prerequisites Details

The following section describes the prerequisites, which must be completed prior to installing Lotus Connections 3.0. The installation of all these prerequisites is explained in the course of this document, with the exception of the LDAP, which is already configured. As each of the prerequisites is discussed below, links to fix packs are included as well as the names of each machine used in this deployment scenario. Prerequisites are as follows:

- **Installation and configuration of WebSphere Application Server 7.0 Network Deployment (ND) and IBM HTTP Server**

WebSphere Application Server must have the following fix packs and fixes applied:

- 7.0.0-WS-WAS-WinX64-FP0000011.pak
- 7.0.0-WS-WASSDK-WinX64-FP0000011.pak
- 7.0.0.11-WS-WAS-IFPM12828
- 7.0.0.0-WS-WAS-IFPM23410 *
- 7.0.0.0-WS-WASJavaSDK-WinX64-IFPM24384 *
- 7.0.0.11-WS-WAS-IFPM25931 *
- 7.0.0.11-WS-WAS-IFPK54565 *

IBM HTTP Server must have the following fix packs applied:

- 7.0.0-WS-IHS-WinX64-FP0000011.pak
- 7.0.0.0-WS-WASJavaSDK-WinX64-IFPM24384 *

IBM HTTP Server plug-ins for WebSphere has the following fix packs applied:

- 7.0.0-WS-PLG-WinX64-FP000011.pak
 - 7.0.0-WS-WASSDK-WinX64-FP000011.pak
 - 7.0.0.0-WS-WASJavaSDK-WinX64-IFPM24384 *

- The screen shots supplied with this guide for applying fixes do not include the fixes followed by an asterisk (*). However, this list is the definitive list of fixes required for Lotus Connections 3.0 to run correctly in this environment. Hence, all the above listed fixes need to be applied. The screen shots are supplied as a guide on how to do this.

These fix packs can be downloaded from IBM Fix Central at: <http://www.ibm.com/support/fixcentral>.

In this example, Network Deployment and Node 1 are installed on the same machine.

Purpose	Host Name
Deployment Manager, Node1 and HTTP Server	connections.example.com

- Installation and configuration of DB2 Enterprise Edition 9.7**

DB2 must have the following fix pack applied:
 DB2-ntx64-server-9.7.200.358-FP002

DB2 fix packs can be downloaded from this location : <http://www-01.ibm.com/support/docview.wss?uid=swg27007053>

- Installation and configuration of Tivoli Directory Integrator 7.0**

TDI must have the following fix pack applied:
 7.0.0-TIV-TDI-FP0005

This fix pack is available at: <http://www.ibm.com/support/fixcentral>

DB2 and TDI are installed on the same machine:

Purpose	Host Name
Database and TDI	db.example.com

- LDAP Directory:** The LDAP server used is IBM Tivoli Directory Server V6.2. The LDAP is called : ldap.example.com

Environment Hardware and Software Specifications

Machine DNS Name	Purpose	OS	RAM	CPU	Hard Drive Size	Software and Versions Installed
connections.example.com	<ul style="list-style-type: none"> Deployment Manager WebServer Application Server Node IBM HTTP Server 	Windows Server 2008 Enterprise Edition x86-64	8 GB RAM	2 x Intel Xeon X7460 @ 2.66 GHZ	100 GB	<ul style="list-style-type: none"> WebSphere Application Server Network Deployment V7.0.0.11 IBM HTTP Server V7.0.0.11 IBM HTTP Server Plugins for WebSphere V7.0.0.11 IBM WebSphere Update Installer V7.0 Lotus Connections 3.0
db.example.com	<ul style="list-style-type: none"> Database (64-bit) 	Windows Server 2008 Enterprise Edition x86-64	8 GB RAM	2 x Intel Xeon X7460 @ 2.66 GHZ	100 GB	<ul style="list-style-type: none"> IBM DB2 v9.7 FP 2 IBM Tivoli Directory Integrator V7.0 FP 5
ldap.example.com	<ul style="list-style-type: none"> LDAP Directory Server 	Windows Server 2008 Enterprise Edition x86-64	8 GB RAM	2 x Intel Xeon X7460 @ 2.66 GHZ	50 GB	<ul style="list-style-type: none"> IBM Tivoli Directory Server V6.2

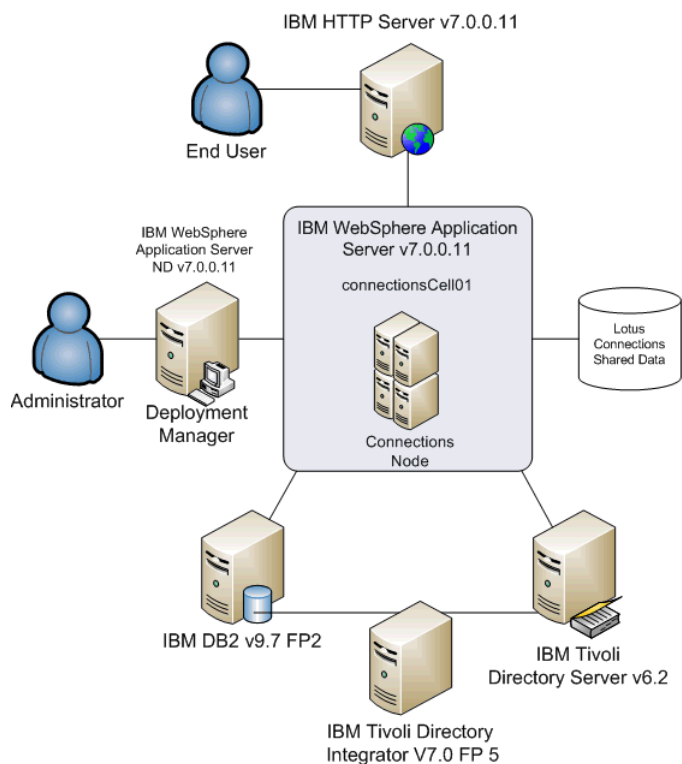
Configuration Diagrams

The following diagrams demonstrate the topology used in this deployment scenario. The topology below affords both good performance and the opportunity to scale up in the future, if required. It is a solid base for a test or pilot system and is contained on only two machines.

Overall System Topology

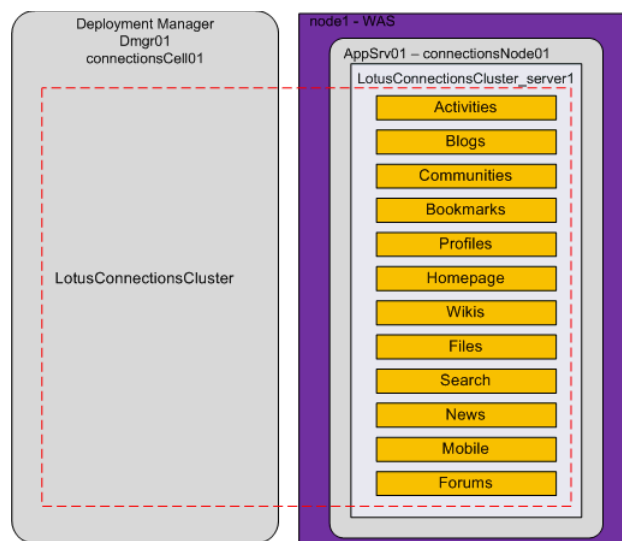
The following topology diagram illustrates a single node cluster of Lotus Connections. In this scenario, the LDAP and database servers communicate with the cell controlled by the Deployment Manager. The Tivoli Directory Integrator server sits between the database and LDAP maintaining the synchronization between both. Lotus Connections is installed onto the Deployment Manager machine and, from here, is pushed out to the nodes in the cell (in this case, the single node below). The data store shown on the right is a shared space accessible from all nodes in the configuration (in this case, the single node). This shared space is actually a directory on the same machine as the cell.

Sitting in front of the entire configuration is the Web server. From here, the end user accesses Lotus Connections 3.0.



WebSphere Application Server Topology

In the overall system topology diagram above, the relationships between the various components in the deployment is clear. However, this did not illustrate the WebSphere Application Server topology (shown below). In this scenario, there is a single cluster containing a single server on the node below. Within this server, all of the features of Lotus Connections 3.0 are installed.



Deployment Considerations

When planning a deployment of Lotus Connections, there are a number of things to consider. Here is a brief discussion on some of the key points.

System Requirements

- Lotus Connections 3.0 is supported only on 64 bit versions of Linux or AIX with the exception of SLES10 31 bit on System Z. While it is supported on 32 bit versions of Windows, it is highly recommended to move to a 64 bit operating system to achieve better performance from the overall system.
- It is recommended to have at least 8 GB RAM on your node machine in this scenario.
- In this scenario, the system hosting WebSphere Application Server and Lotus Connections has a total of 100 GB, approximately 70 GB hard disk space is free on the system after the installation. This is sufficient for a test system and a good starting base for a pilot install. When planning the installation, it is important to consider how many users will use the system and how much data each user might generate. The file system

should be big enough to handle this, or else expanded over time to cope with the space requirements.

Resource Planning

While this scenario covers a specific deployment situation, it can be used as a guide to deploying other slightly different topologies. It is possible to customize the number of clusters and applications that are installed into each cluster. Where there are resource constraints, any number of the Lotus Connections applications can be combined onto a cluster.

It is also possible to combine one or more databases onto any number of DB2 instances to achieve the performance required.

Future Planning

It is crucial to plan for the future when deploying Lotus Connections. While this configuration is an excellent starting configuration, over time, demands on the system may grow and additional nodes may need to be added to the system. This topology offers this option by allowing additional nodes to be added to the cell, as and when required in the future.

Integration with Other Products and Single Sign On

While neither product integration or Single Sign On (SSO) are covered in this scenario, you may need to consider the implications of integrating other products with Lotus Connections or SSO between a security product and Lotus Connections when planning your installation.

- Enabling SSO with another IBM product involves exchanging LTPA tokens, sharing realms and users who can access the system, as well as the machines being in close synchronization with each other's system clocks.
- If you plan to deploy a system where a third party security suite, such as SiteMinder, Tivoli Access Manager, or SPNEGO, will be deployed, it is crucial that an LDAP user be configured as a WebSphere Application Server administrator and be specified as the user to connect to WebSphere Application Server during the installation.

Security Considerations

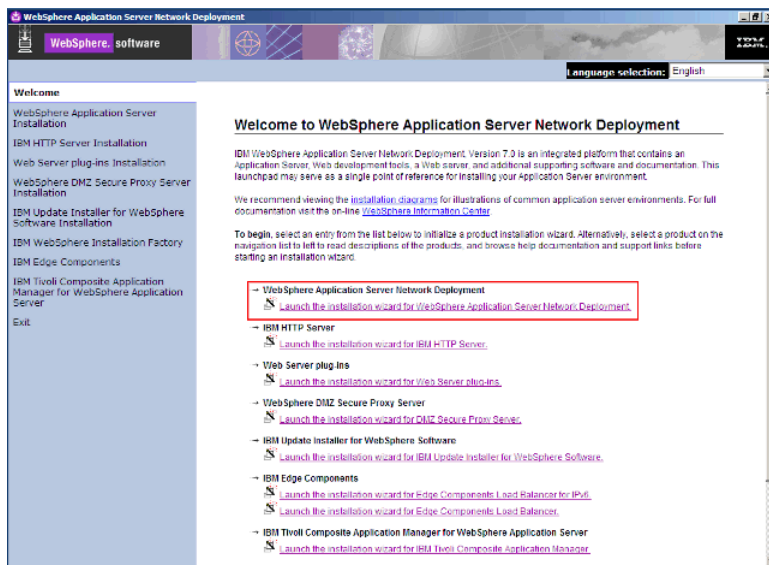
- The proxy-config.tpl file allows the proxy to work with self-signed certificates. This is true out-of-the-box, but for improved security, set the value of the unsigned_ssl_certificate_support property to false when your deployment is ready for production. This file can be checked out and edited by following the *Configuring the AJAX proxy* section of the Lotus Connections product documentation.

Pre-Installation Tasks

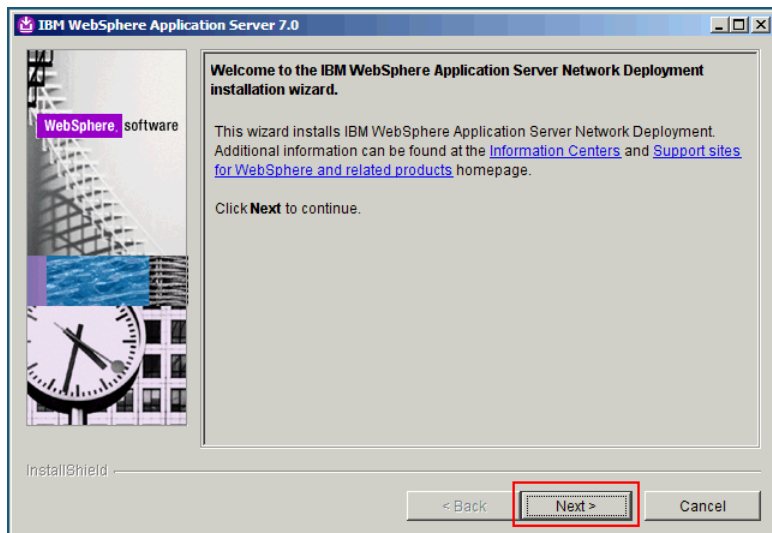
The following prerequisite software must be installed in advance of installing Lotus Connections 3.0. The following sections detail how to achieve this.

Installing WebSphere Application Server 7.0 Network Deployment

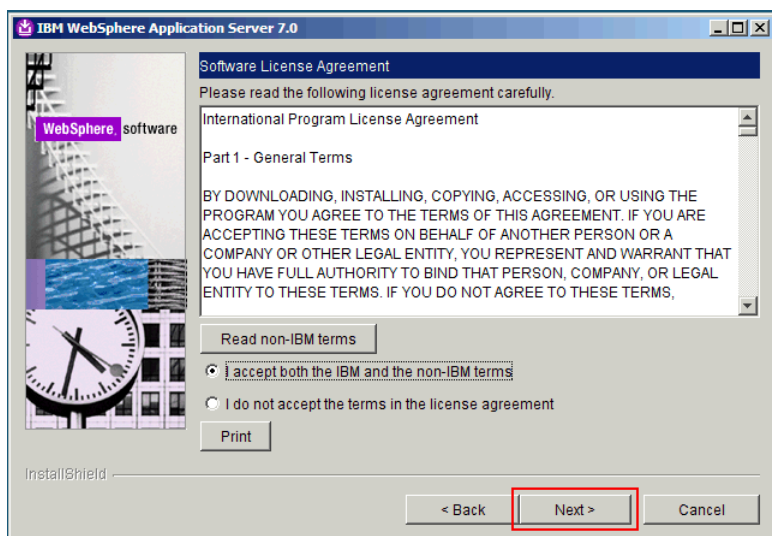
Unzip the file that you have downloaded in a directory on your hard disk. Change to the directory and run **launchpad.exe**. The following panel is displayed:



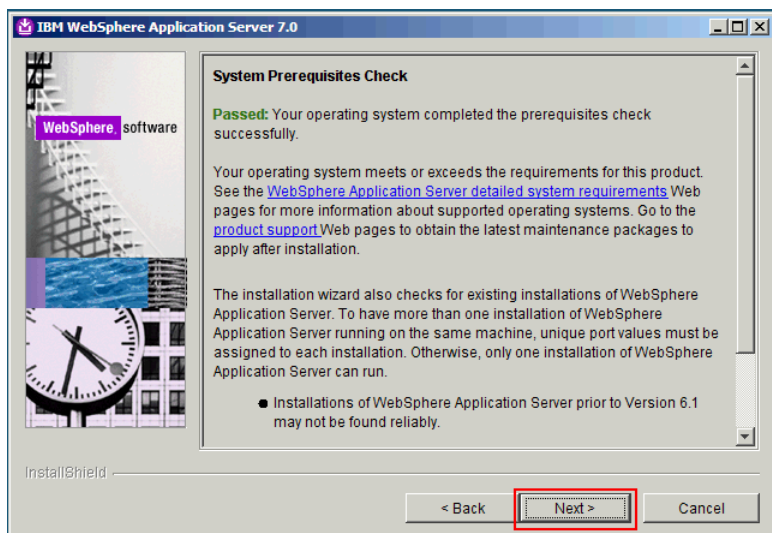
Click **Launch the installation wizard for WebSphere Application Server Network Deployment**. The following panel is displayed.



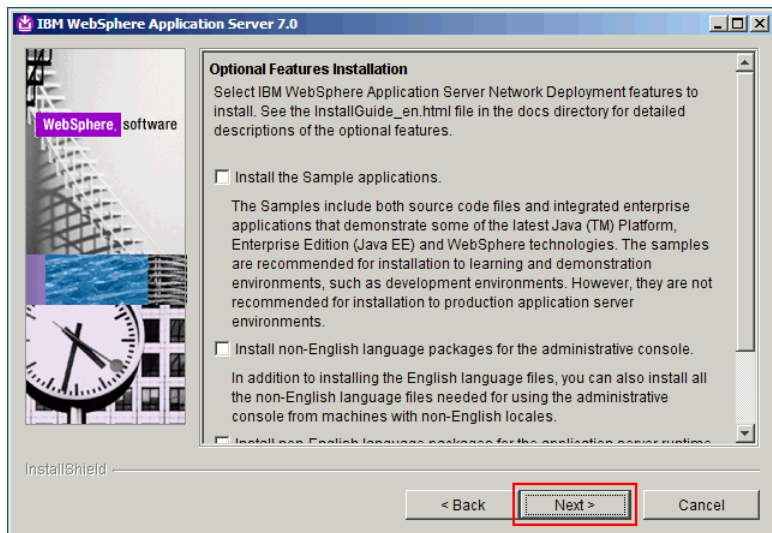
Click **Next**. The following panel is displayed.



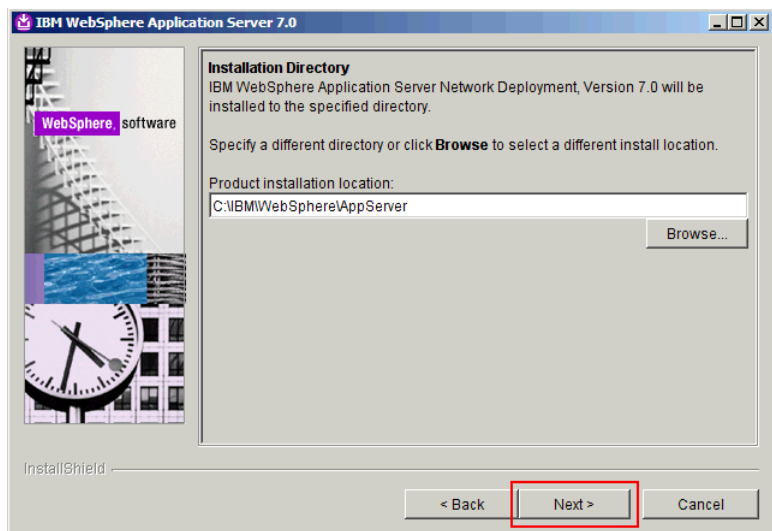
Accept the IBM and non-IBM terms and click **Next**. The following panel is displayed.



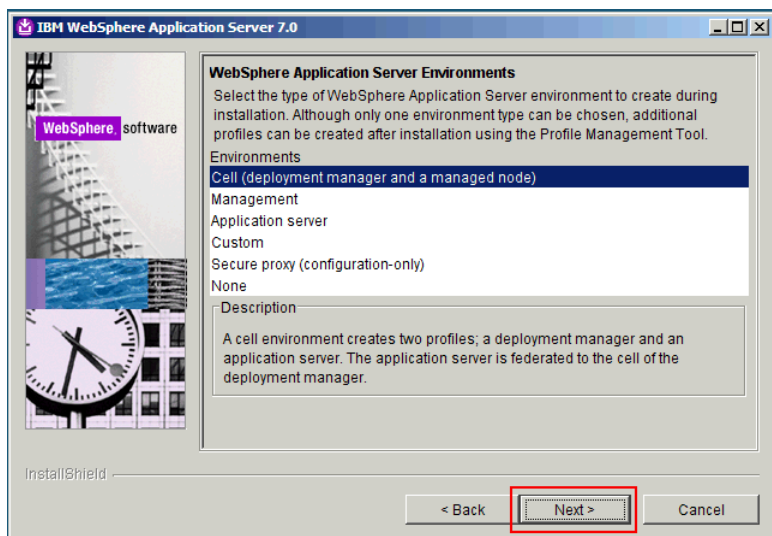
If the prerequisites check is successful, click **Next**. The following panel is displayed.



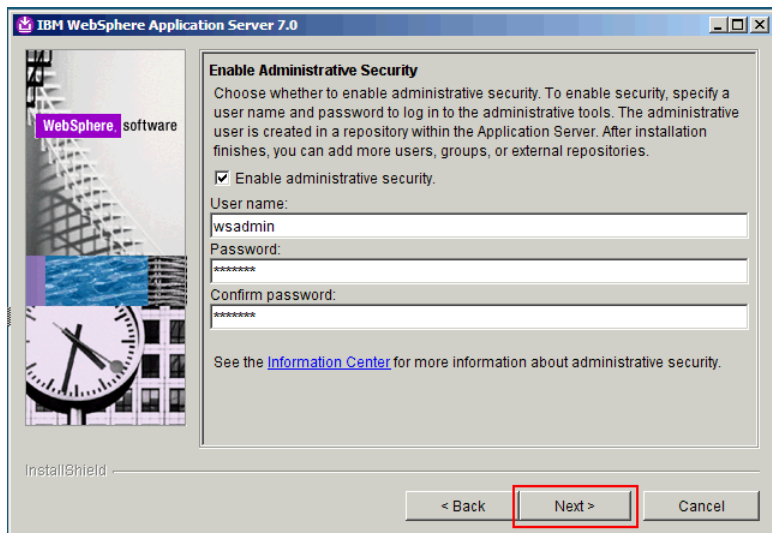
Leave all the check boxes unselected and click **Next**. The following panel is displayed.



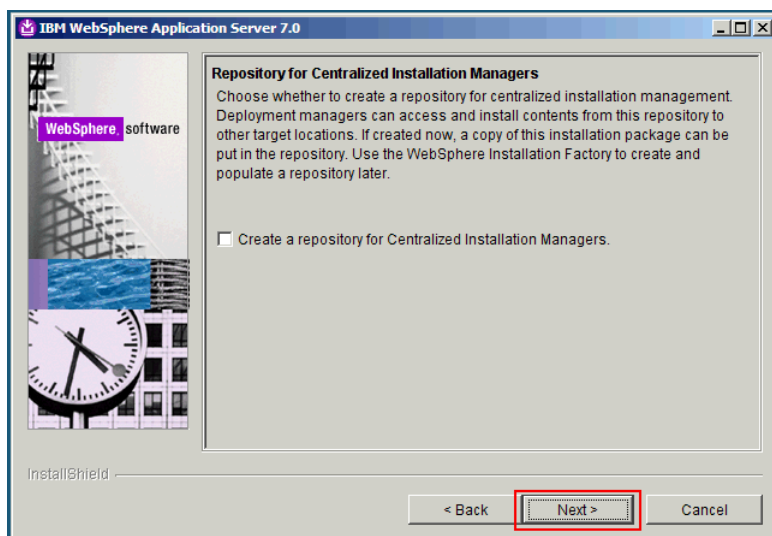
Select an installation directory, preferably not in C:\Program Files, and click **Next**. The following panel is displayed.



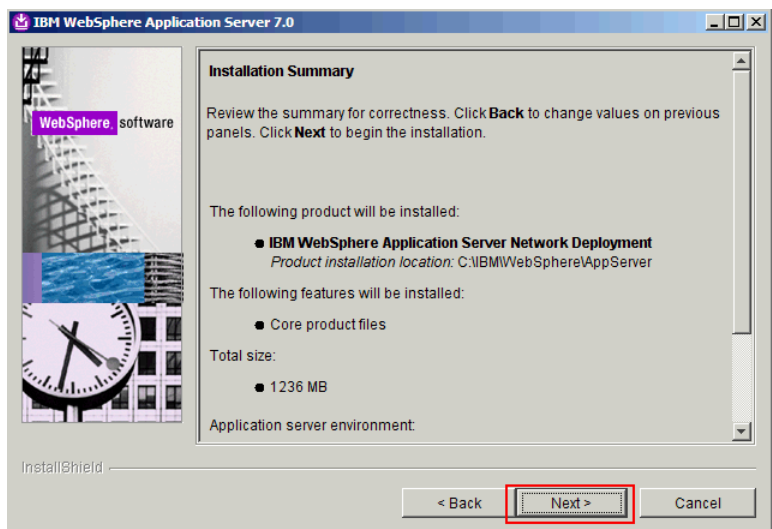
Select **Cell** as the environment to install, and then click **Next**. The following panel is displayed.



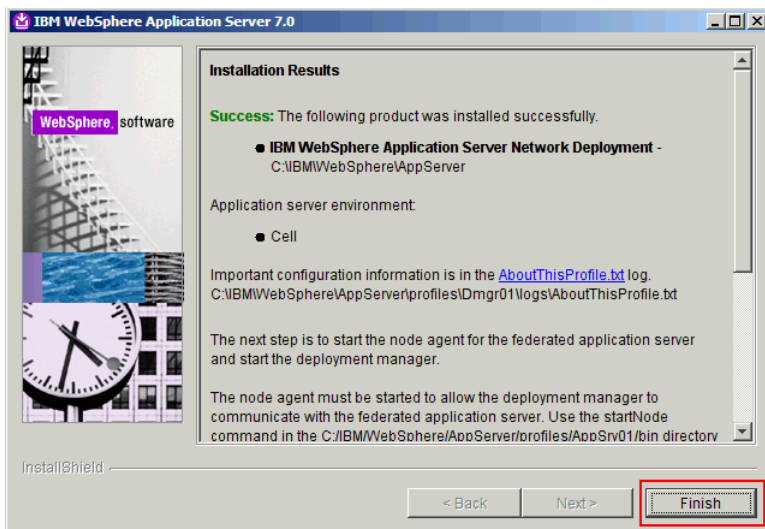
Choose a user name and a password for the administrative user of WebSphere Application server and click **Next**. The following panel is displayed.



Leave the check box unselected and click **Next**. The following panel is displayed.



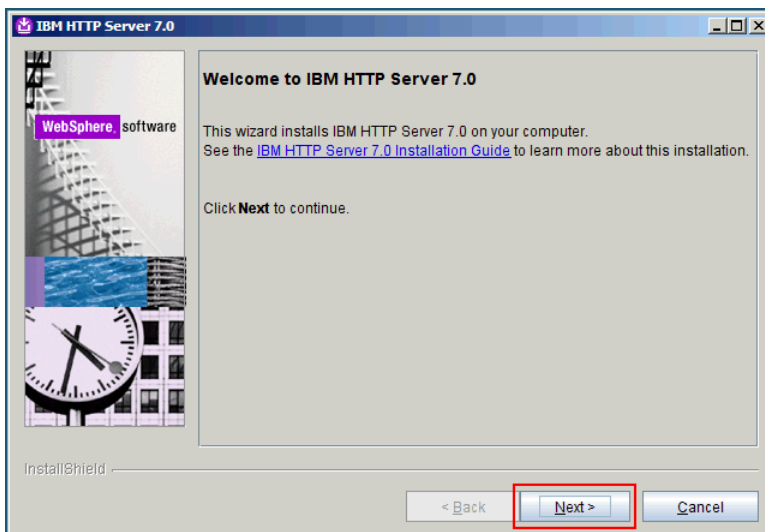
Click **Next**. The following panel is displayed.



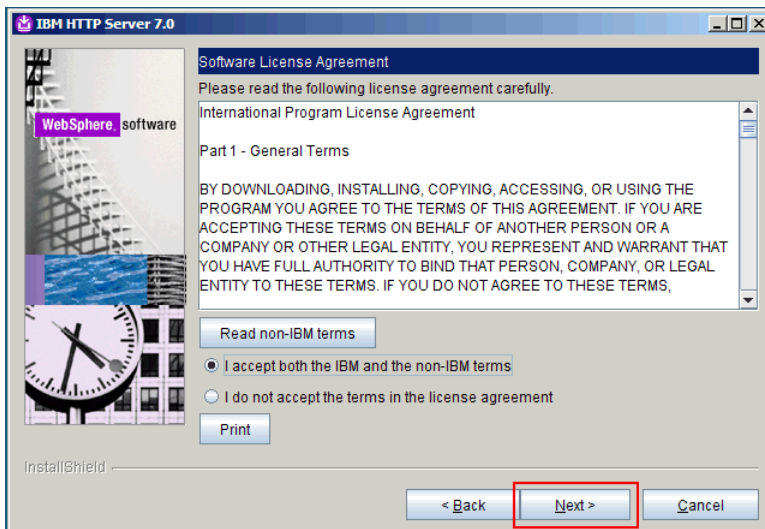
Click **Finish**.

Installing IBM HTTP Server V7.0 and WebSphere Plugins

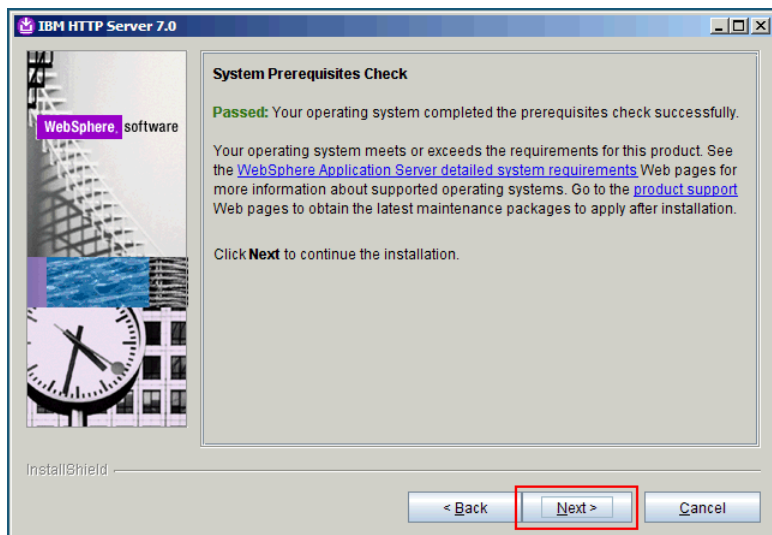
Unzip the WebSphere Application Server Supplements file in a directory on your hard disk. Go to the IHS subdirectory and run **install.exe**. The following panel is displayed.



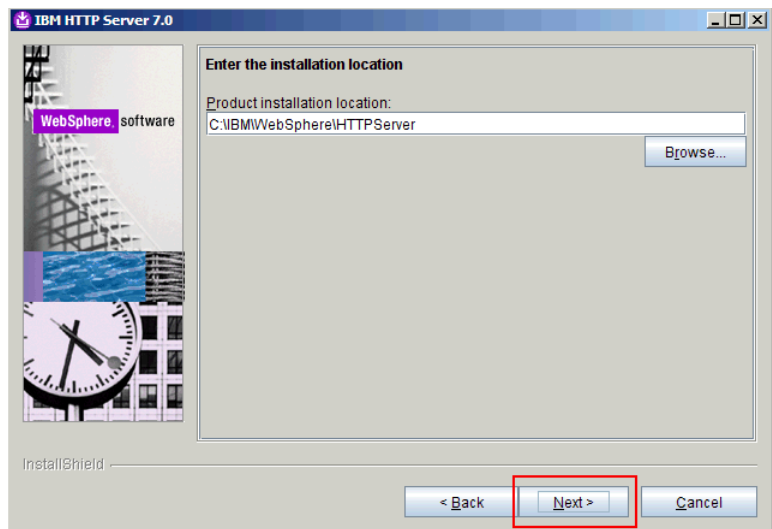
Click **Next**. The following panel is displayed.



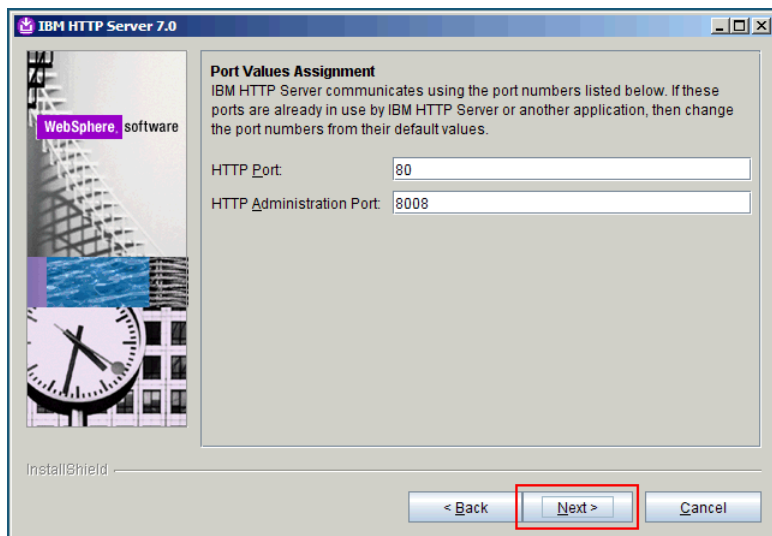
Accept the IBM and non-IBM terms and click **Next**. The following panel is displayed.



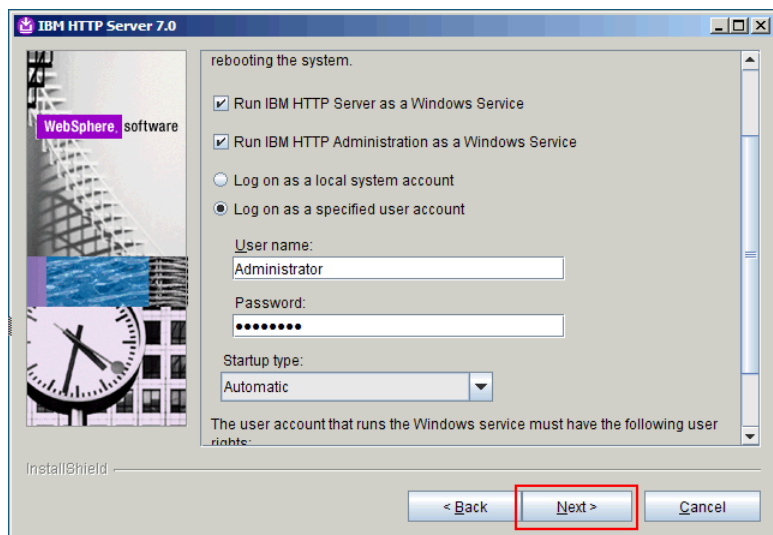
If the prerequisites check is successful, click **Next**. The following panel is displayed.



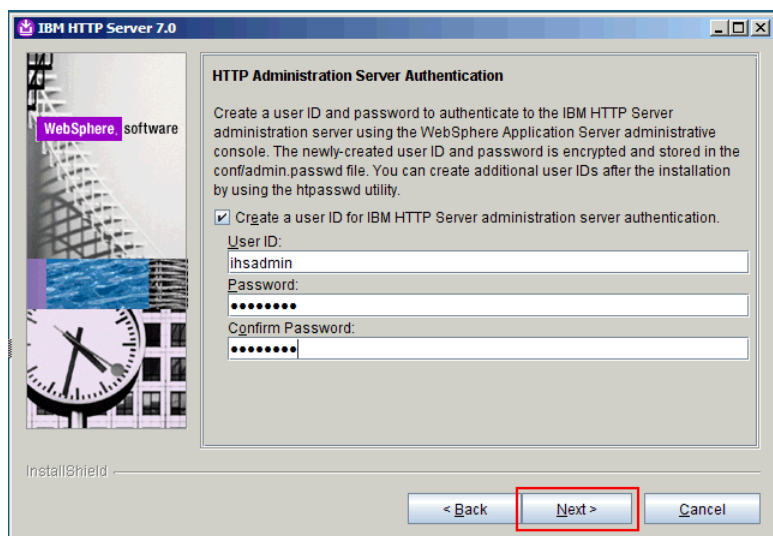
Select an installation directory, preferably not in C:\Program Files, and click **Next**. The following panel is displayed.



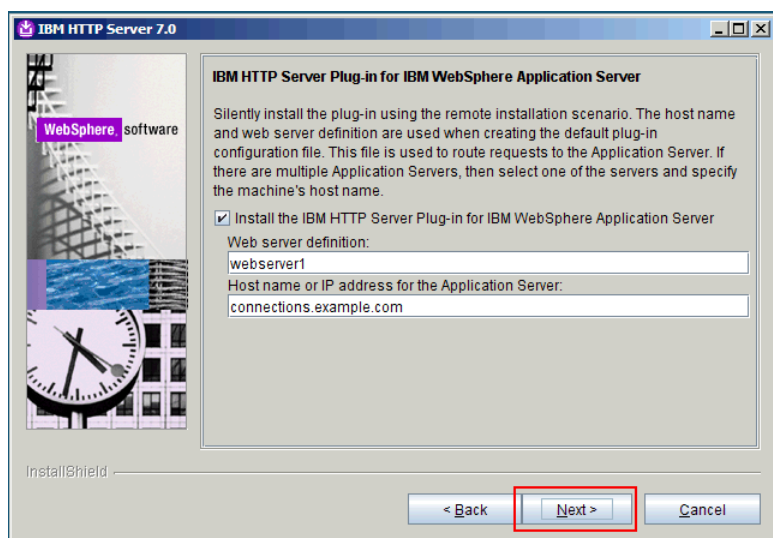
Leave the default values and click **Next**. The following panel is displayed.



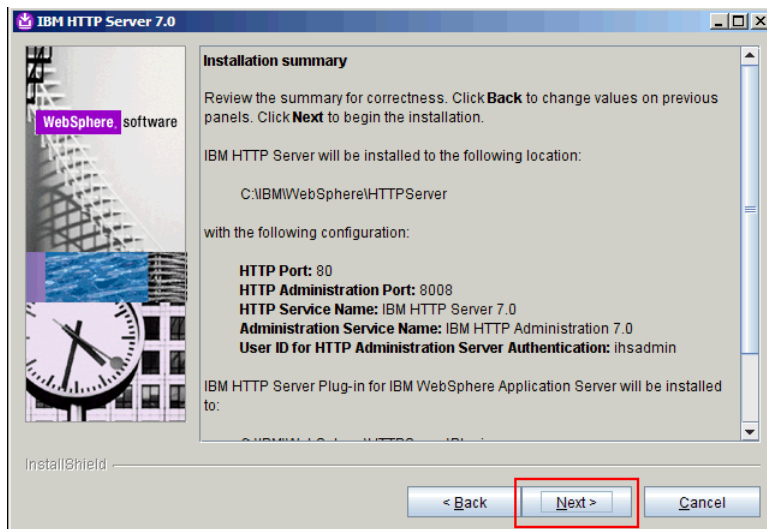
Select the two check boxes, select to "Log on as a specified user account," and then enter a user name and a password for that account. Click **Next**. The following panel is displayed.



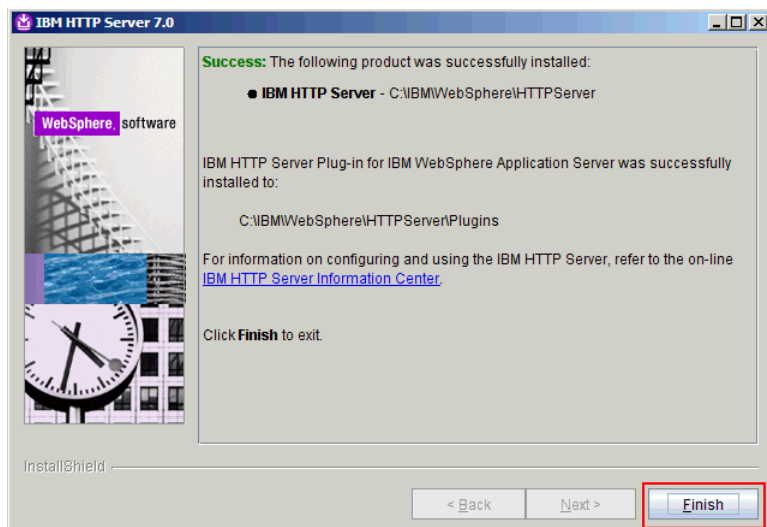
Select "Create a user ID for IHS administration server authentication," and then select a user name and a password. Click **Next**. The following panel is displayed.



Select "Install the IBM HTTP Server Plug-in for IBM WebSphere Application Server." The two fields are already filled. Leave the defaults and click **Next**. The following panel is displayed.

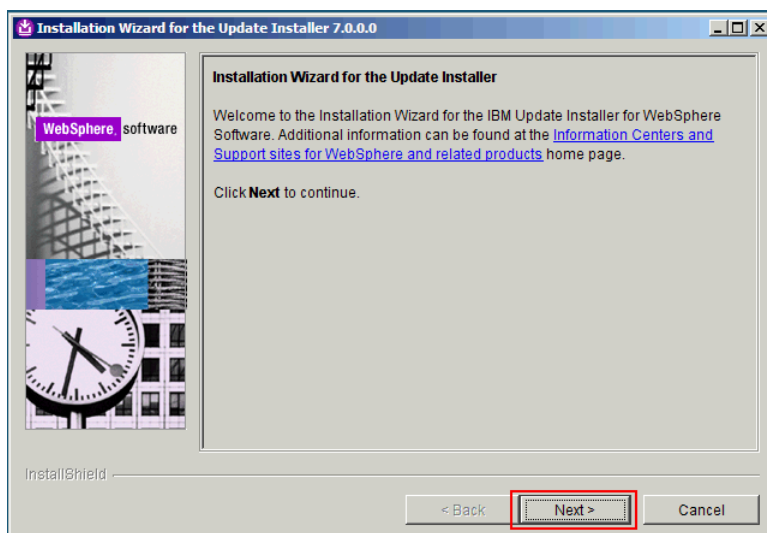


Review the installation summary and click **Next**. The following panel is displayed.

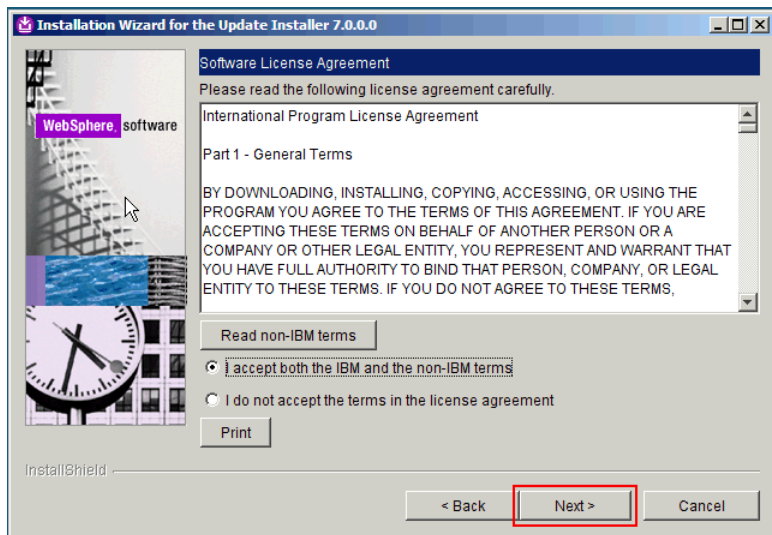


Upgrading WebSphere Application Server, HTTP Server and WebSphere Plug-ins to Correct Fix pack Level

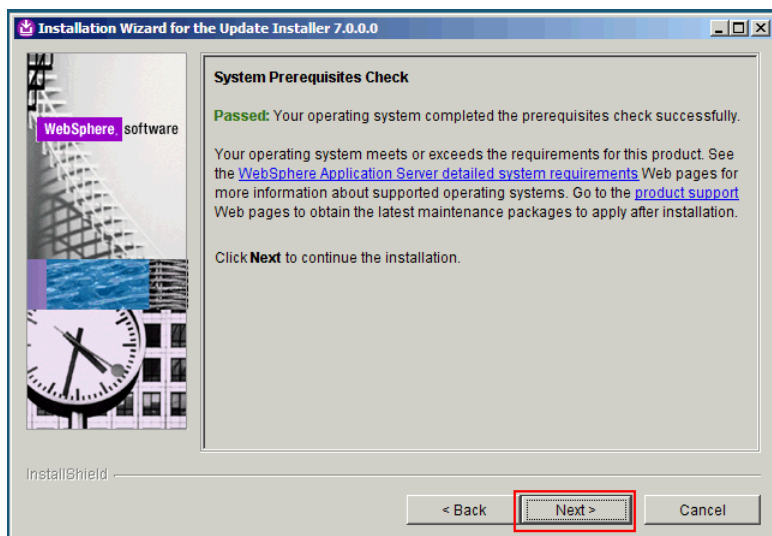
Locate the directory where you unzipped the WebSphere Application Server supplements. Go to the UpdateInstaller directory and run **install.exe**. The following panel is displayed.



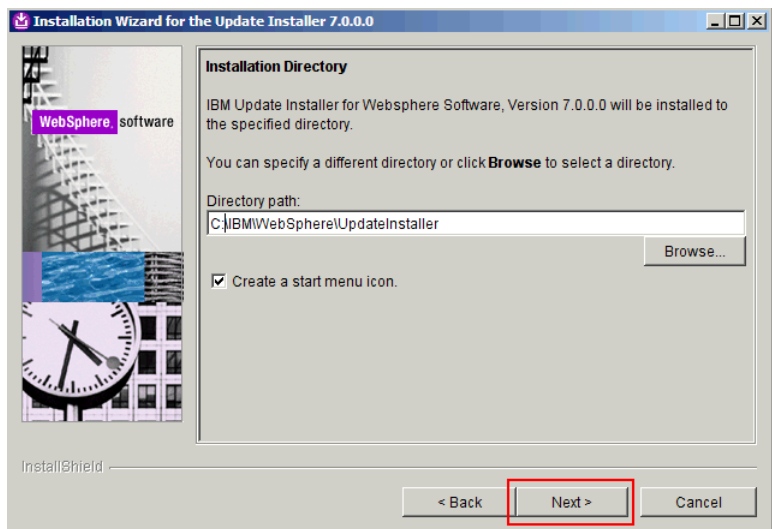
Click **Next**. The following panel is displayed.



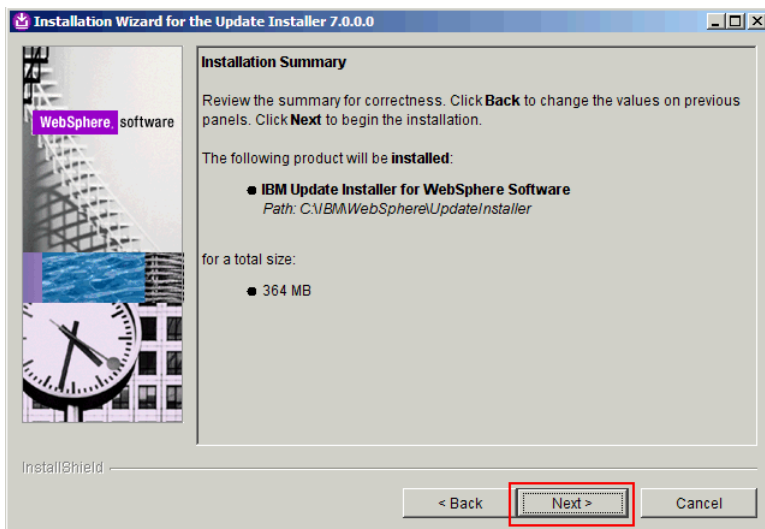
Accept the IBM and non-IBM terms and click **Next**. The following panel is displayed.



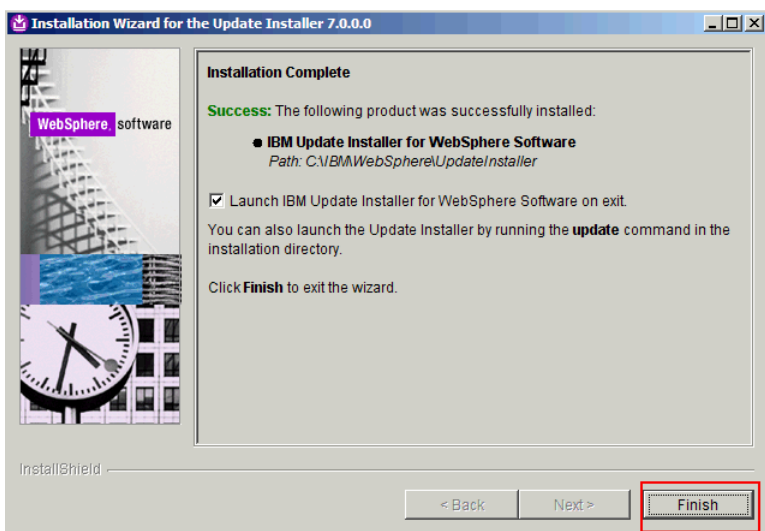
If the prerequisites check is successful, click **Next**. The following panel is displayed.



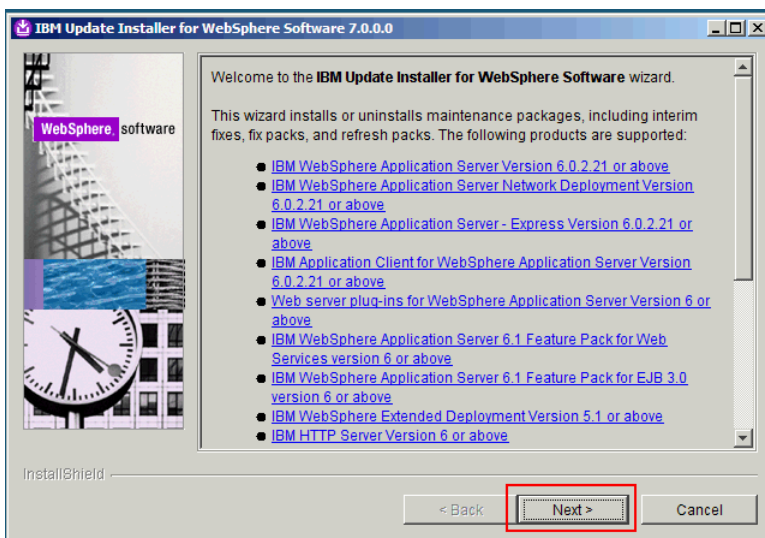
Select an installation directory, preferably not in C:\Program Files, and click **Next**. The following panel is displayed.



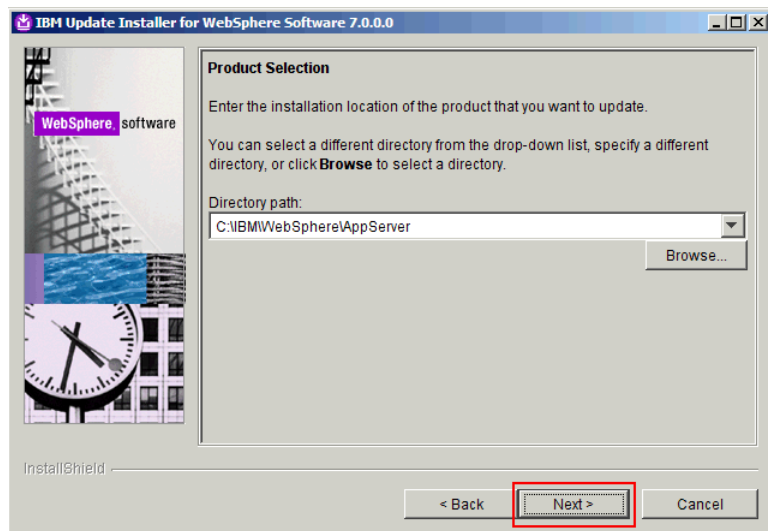
Review the installation summary and click **Next**. The following panel is displayed.



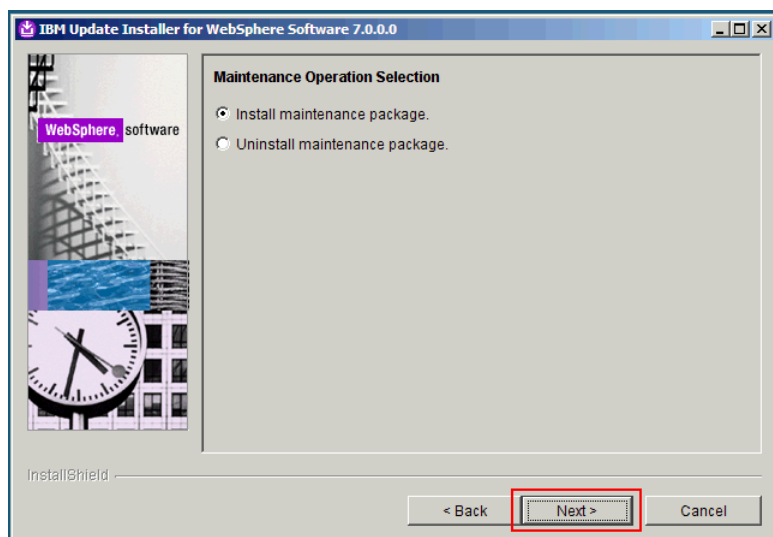
Select the check box "Launch IBM Update installer for WebSphere Software on exit." The following panel is displayed.



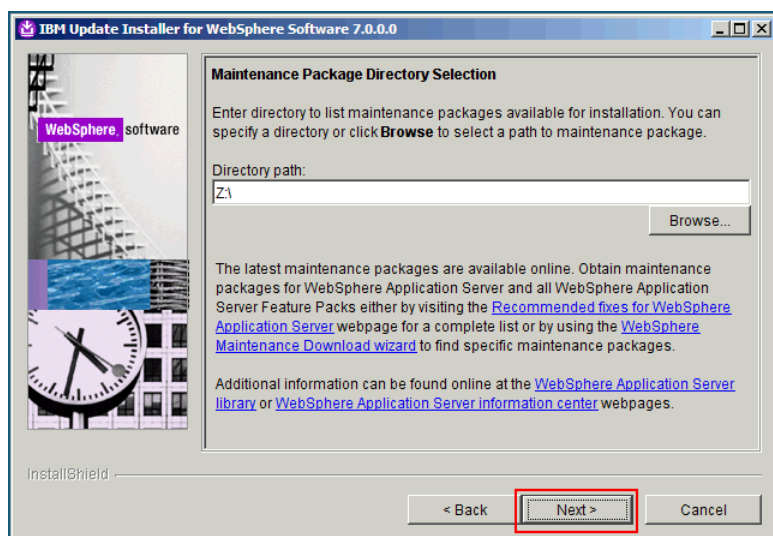
Click **Next**. The following panel is displayed.



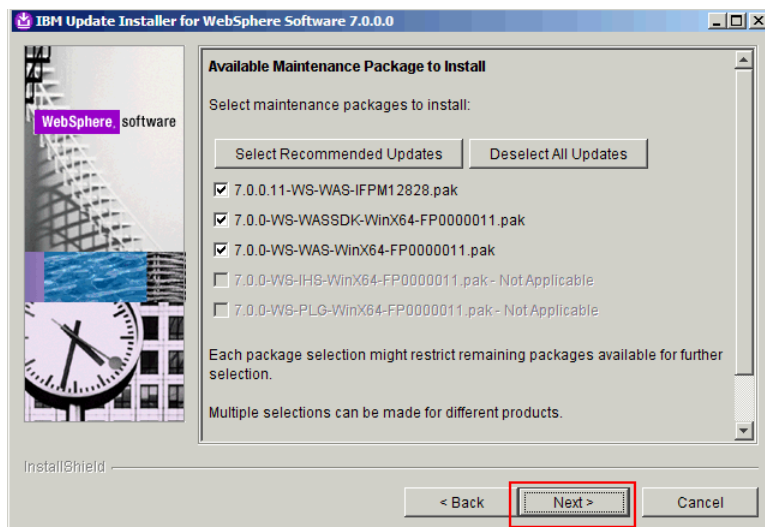
The location of the AppServer is already filled in. Click **Next**. The following panel is displayed.



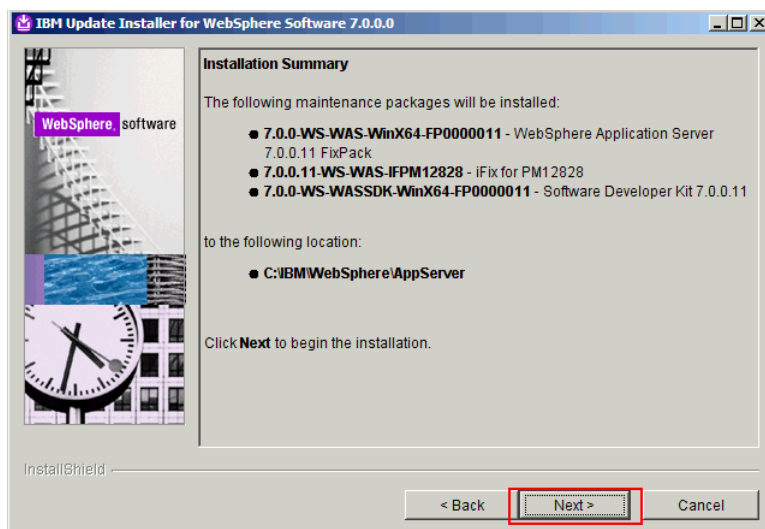
Select "Install maintenance package" and click **Next**. The following panel is displayed.



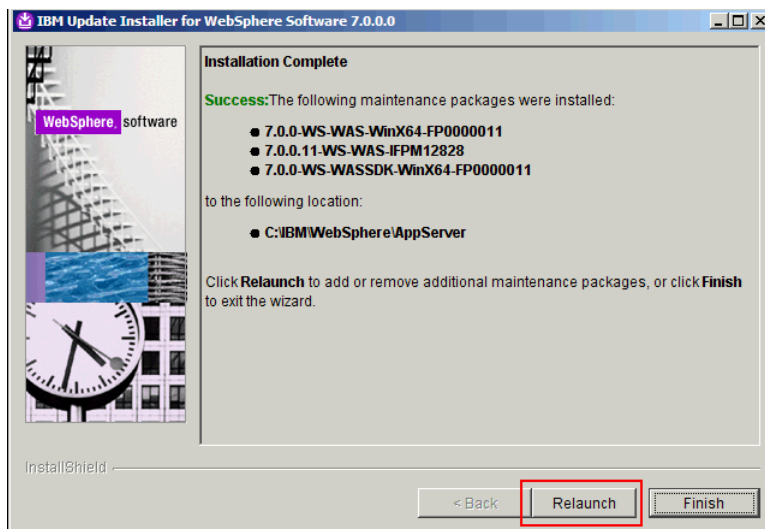
Select the directory where you copied the 7.0.0-WS-WAS-WinX64-FP0000011.pak, 7.0.0-WS-WASDK-WinX64-FP0000011.pak, 7.0.0.11-WS-WAS-IFPM12828.pak, 7.0.0.0-WS-WAS-IFPM23410 *, 7.0.0.0-WS-WASJavaSDK-WinX64-IFPM24384*, 7.0.0.11-WS-WAS-IFPM25931 *, and 7.0.0.11-WS-WAS-IFPK54565* and click **Next**. The following panel is displayed.



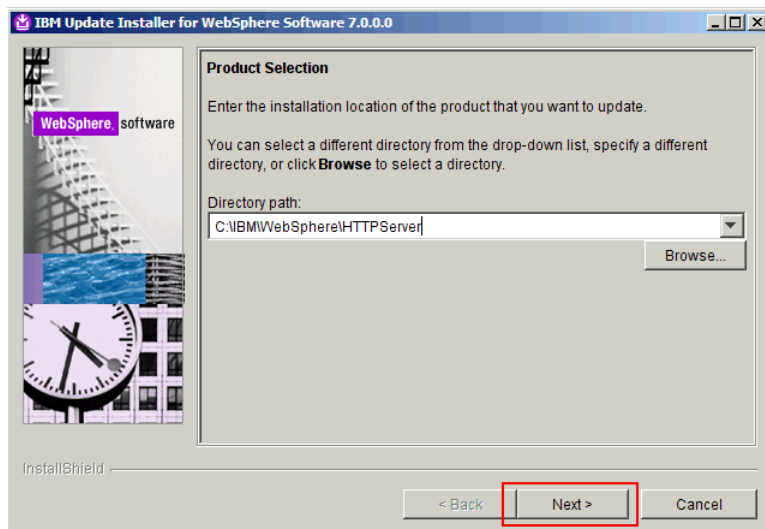
Select the check boxes and click **Next**. The following panel is displayed.



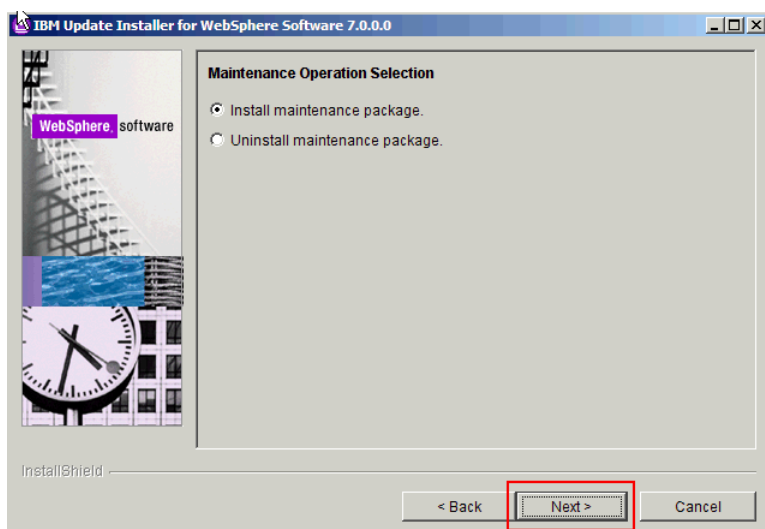
Review the installation summary and click **Next**. The following panel is displayed.



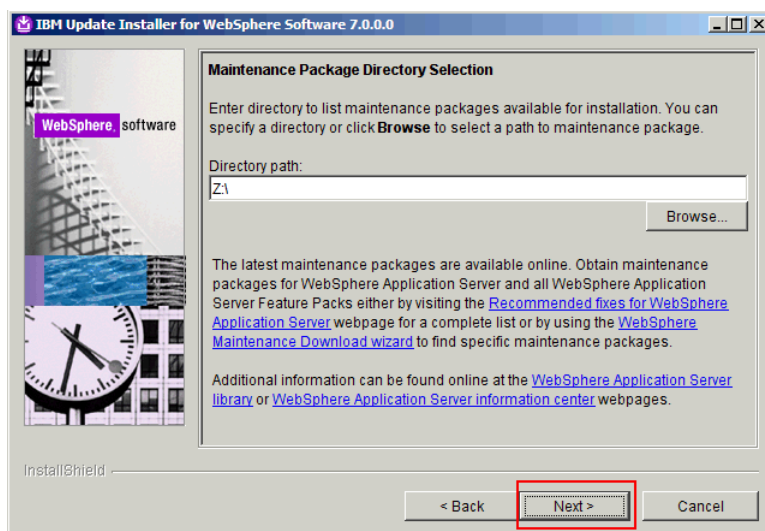
Click **Relaunch**. The following panel is displayed.



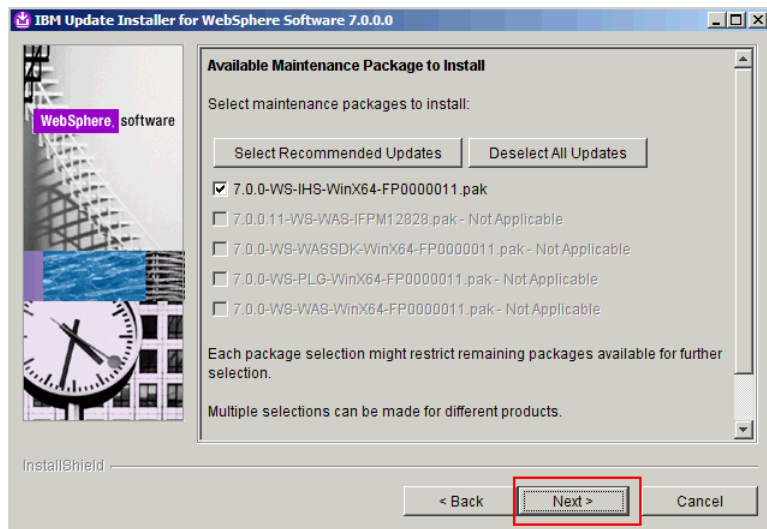
From the drop-down list, select the path for the HTTP server and click **Next**. The following panel is displayed.



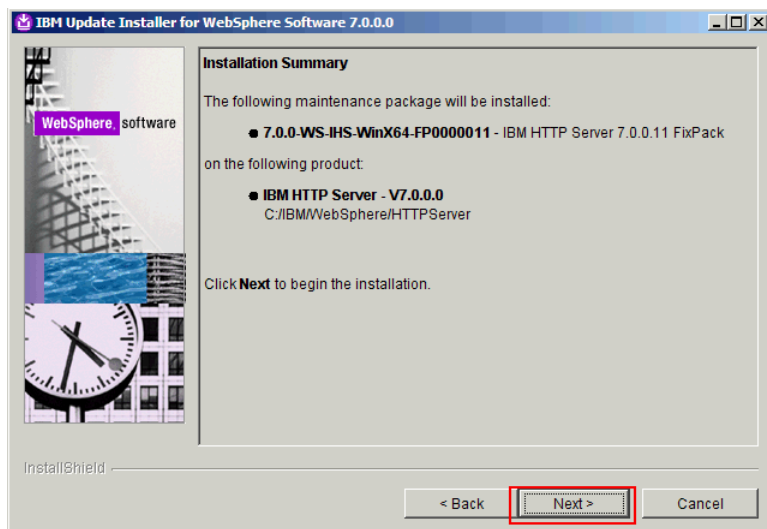
Click **Next**. The following panel is displayed.



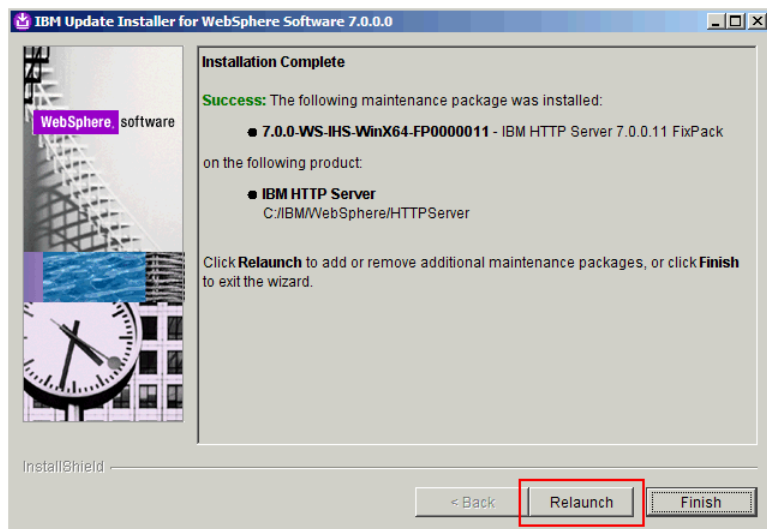
Select the path where you downloaded the fix packs, 7.0.0-WS-IHS-WinX64-FP000011.pak and 7.0.0.0-WS-WASJavaSDK-WinX64-IFPM24384* and click **Next**. The following panel is displayed.



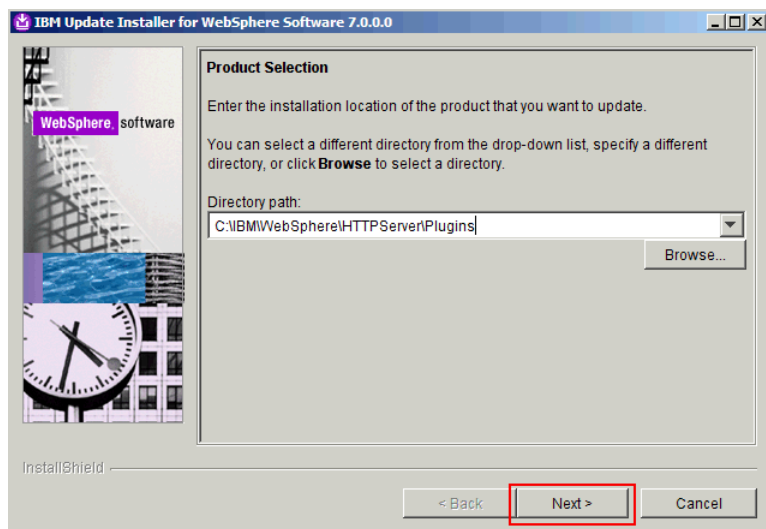
Leave the check box selected and click **Next**. The following panel is displayed.



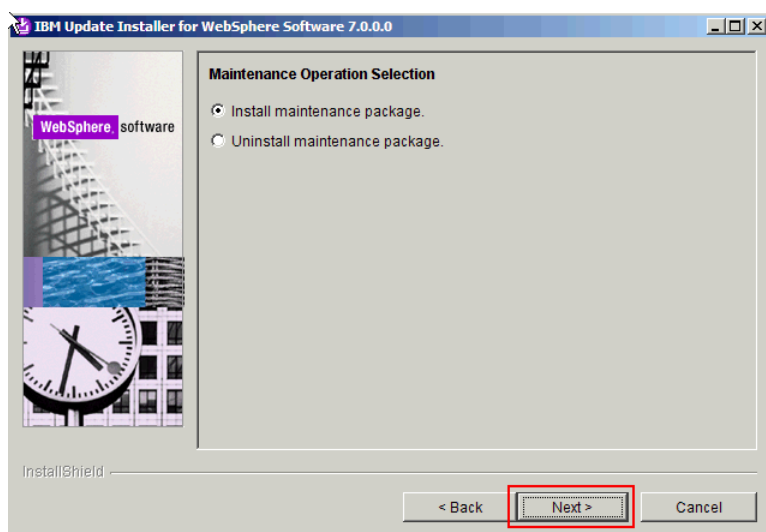
Review the summary and click **Next**. The following panel is displayed.



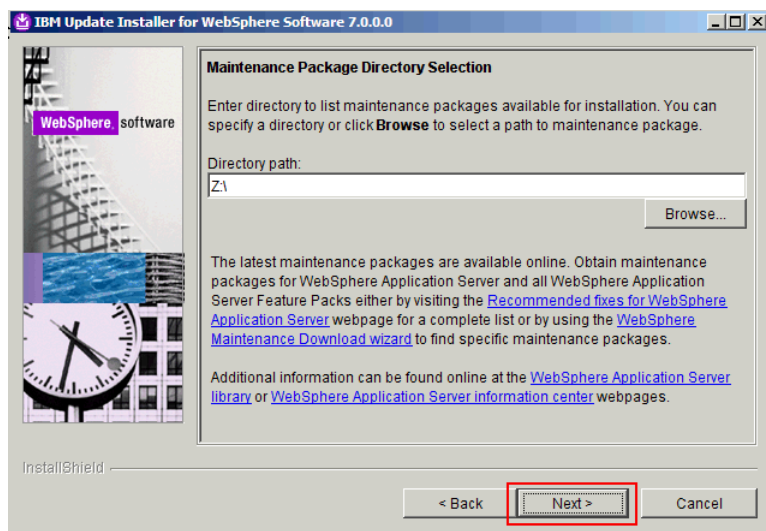
Click **Relaunch**. The following panel is displayed.



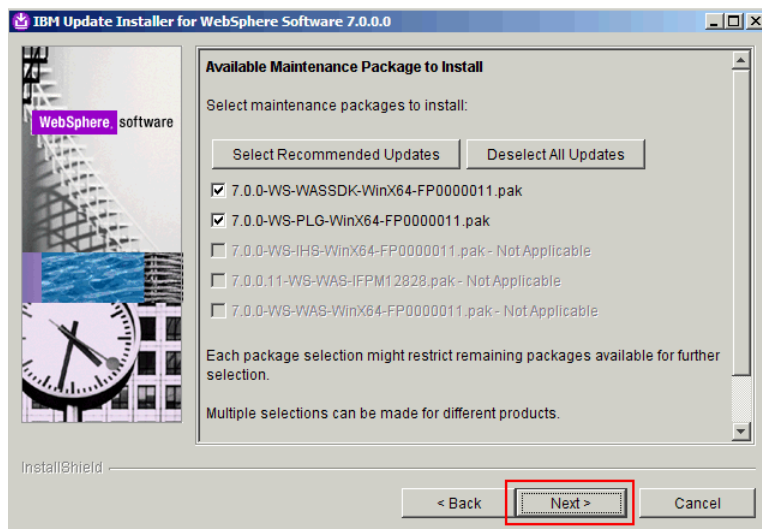
From the drop-down list, select the path for the HTTP server plug-ins and click **Next**. The following panel is displayed.



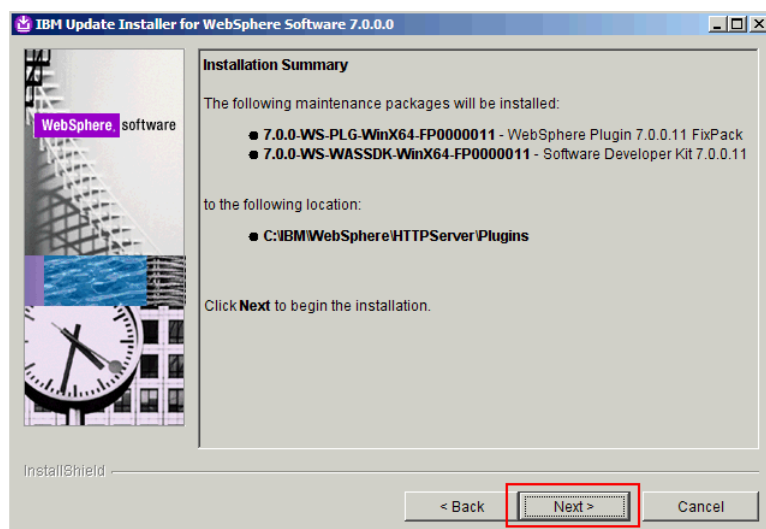
Select "Install maintenance package" and click **Next**. The following panel is displayed.



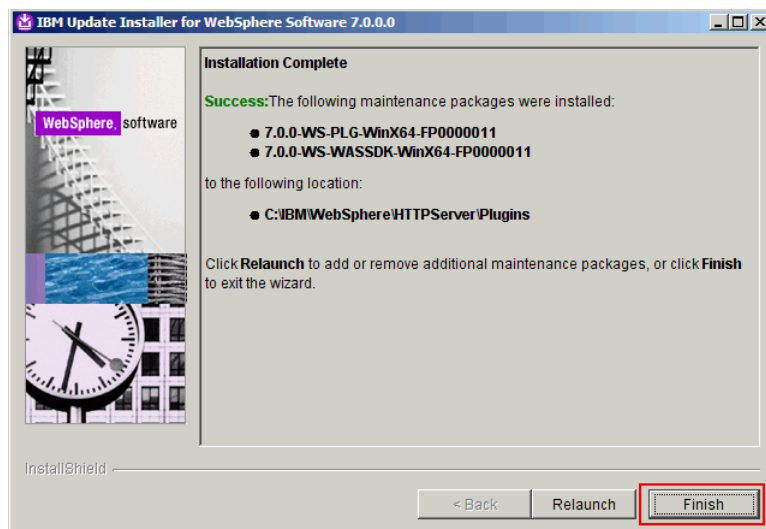
Select the path where you downloaded the fix packs, 7.0.0-WS-PLG-WinX64-FP0000011.pak, 7.0.0-WS-WASSDK-WinX64-FP0000011.pak and 7.0.0-WS-WASJavaSDK-WinX64-IFPM24384* and click **Next**. The following panel is displayed.



Click **Next**. The following panel is displayed.



Click **Next**. The following panel is displayed.



Click **Finish**.

This ends the installation and update of WebSphere Application Server Network Deployment V7.0 and IBM HTTP Server V7.0 to the required level for Lotus Connections 3.0.

Installing of DB2 Enterprise Edition V9.7 Fix pack 2

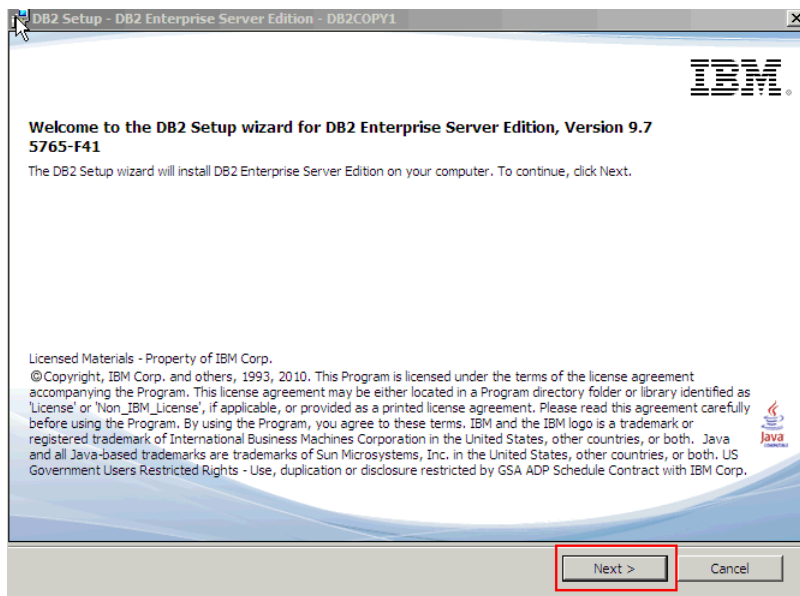
Run `v9.7fp2_ntx64_server.exe` to unzip the contents. Go to the "SERVER" directory and run `setup.exe`. The following panel is displayed.



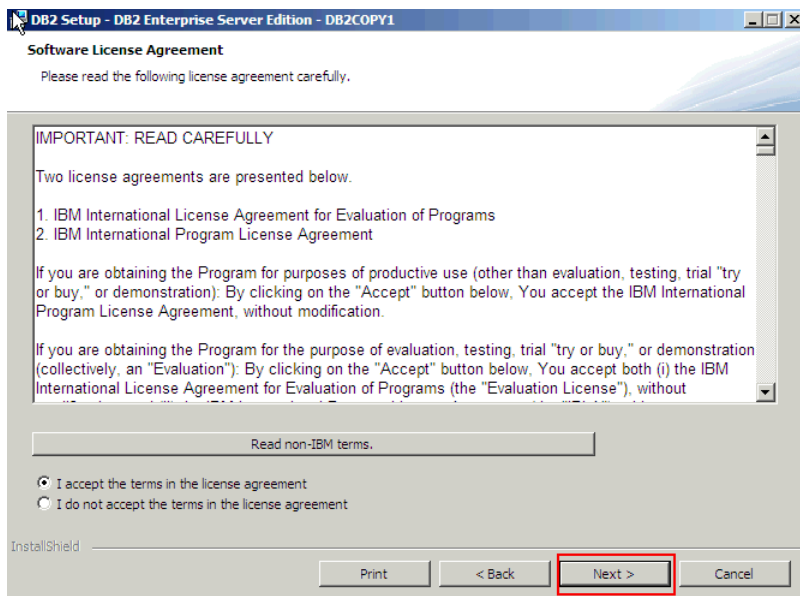
Click the **Install a Product** link. The following panel is displayed.



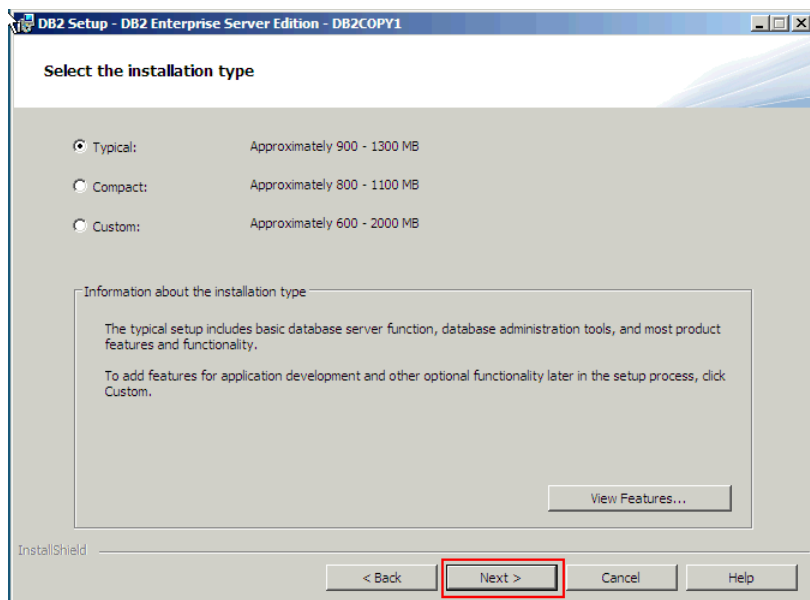
Click **Install New**. The following panel is displayed.



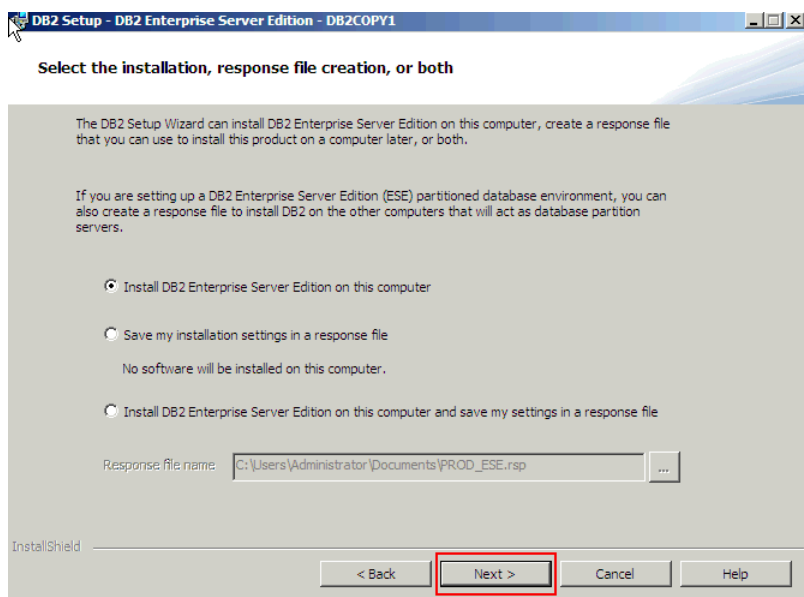
Click **Next**. The following panel is displayed.



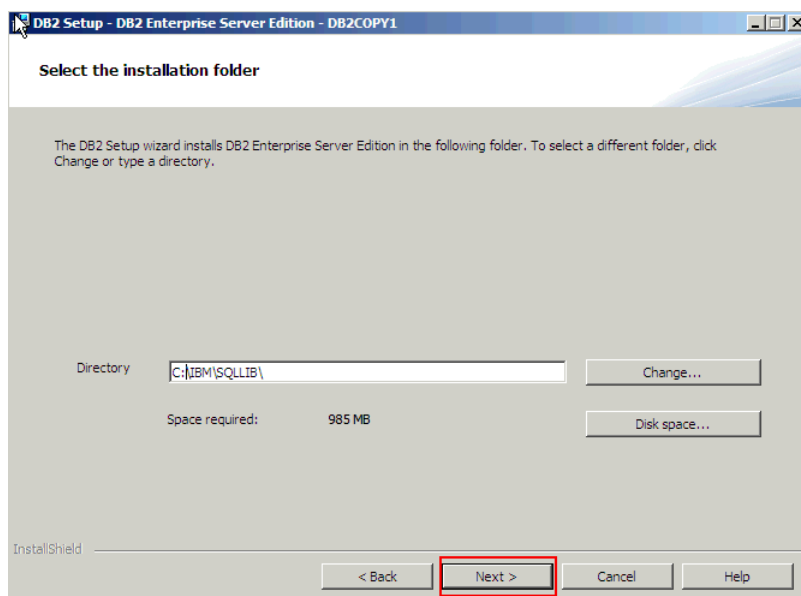
Accept the license and click **Next**. The following panel is displayed.



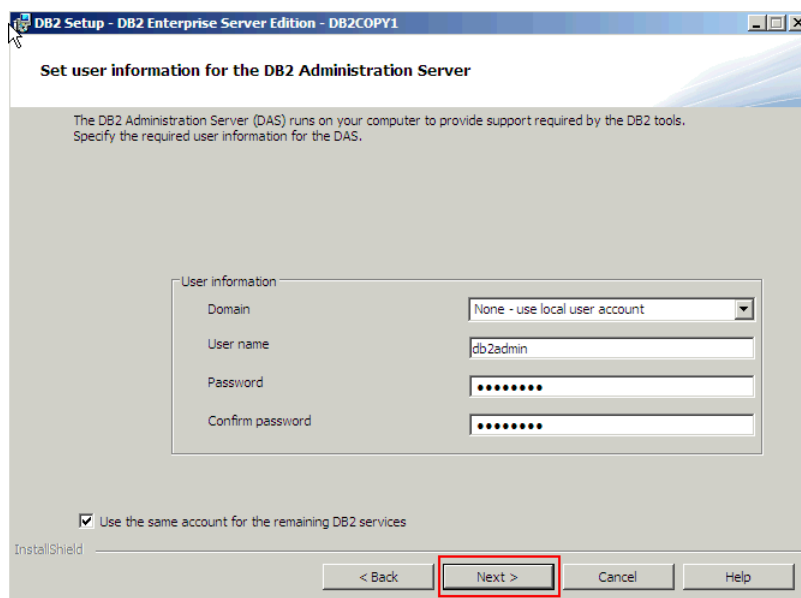
Select "Typical" and click **Next**. The following panel is displayed.



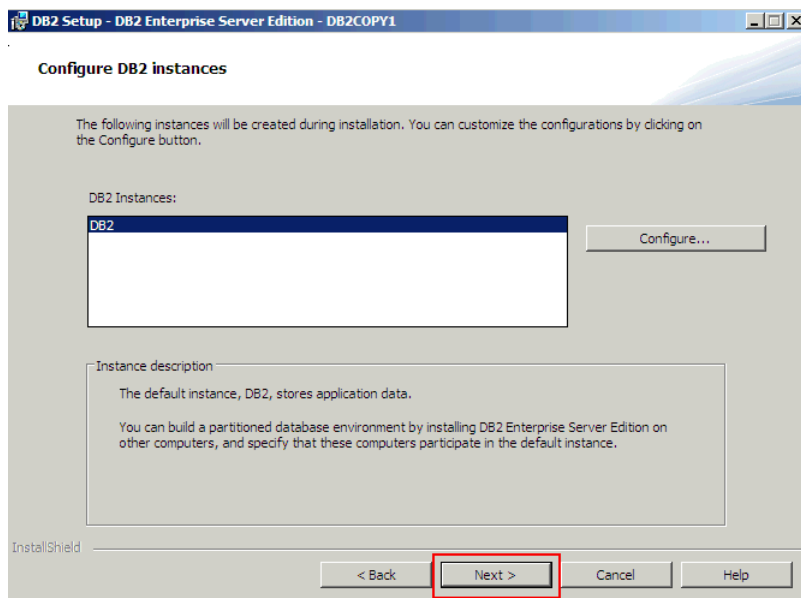
Select "Install DB2 Enterprise Server Edition on this computer" and click **Next**. The following panel is displayed.



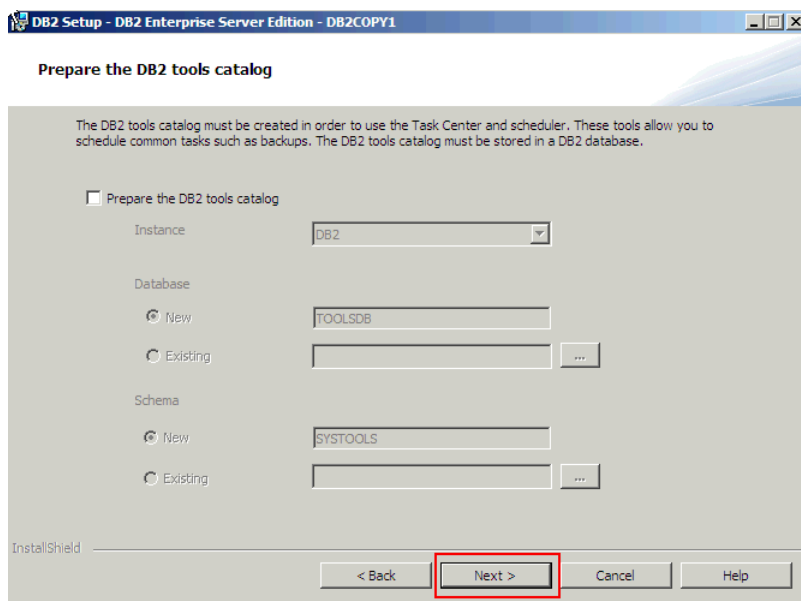
Choose the installation directory and click **Next**. The following panel is displayed.



Choose a user name and a password and click **Next**. The following panel is displayed.



Click **Next**. The following panel is displayed.



The catalog is not required. Leave the check box blank and click **Next**. The following panel is displayed.

Set up notifications

You can set up your DB2 server to automatically send e-mail or pager notifications to alert administrators when a database needs attention. The contact information is stored in the administration contact list. You need an unauthenticated SMTP server to send these notifications.

If you do not set up your DB2 server to send notifications at this time, the health alerts are still recorded in the administration notification log.

Set up your DB2 server to send notifications

Notification SMTP server:

Administration contact list location:

- Local - Create a contact list on this computer
- Remote - Use an existing contact list on another DB2 server

Remote DB2 server:

InstallShield

< Back **Next >** Cancel Help

Notifications are not required. Leave the check box blank and click **Next**. The following panel is displayed.

Enable operating system security for DB2 objects

Specify if you would like to enable operating system security for DB2 files, folders, registry keys, and other objects on your computer. If you enable this security, operating system access to DB2 objects will be limited to the groups specified below.

Enable operating system security

Information on the DB2 administrators group and DB2 users group is available by clicking Help.

DB2 administrators group

Domain:

Group name:

DB2 users group

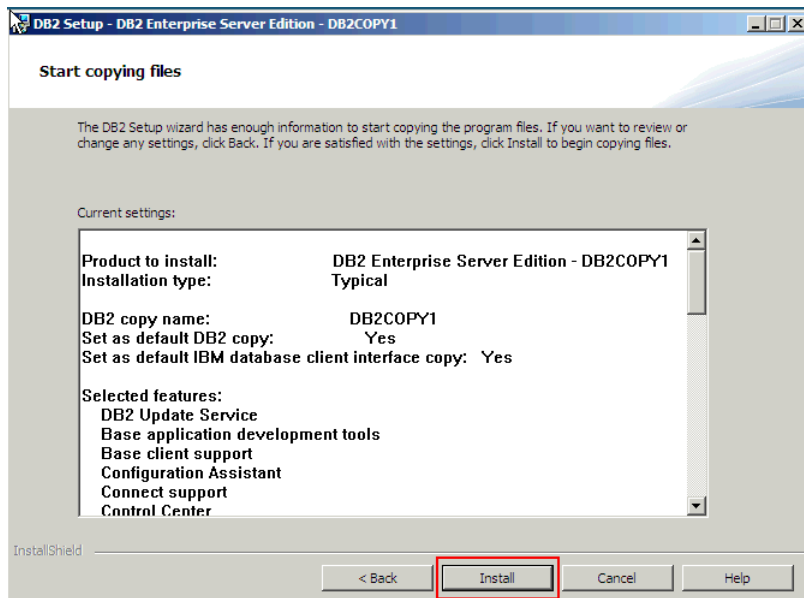
Domain:

Group name:

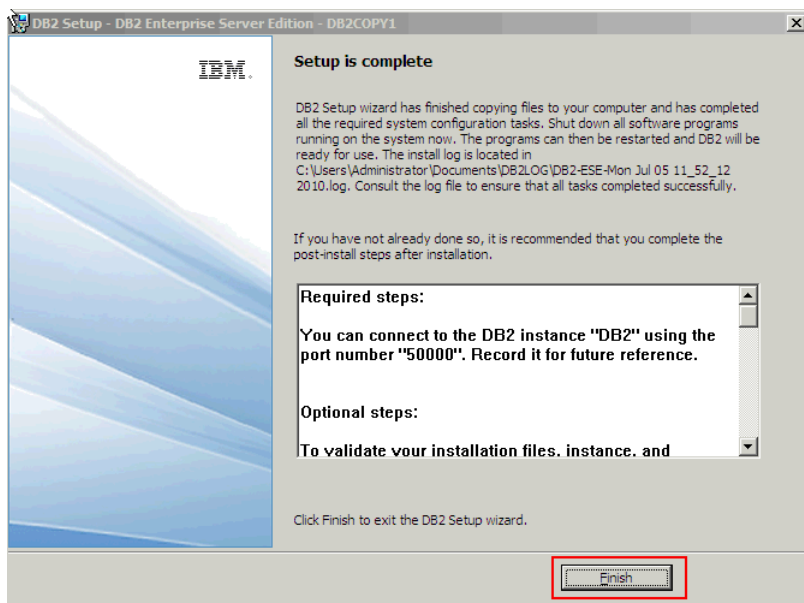
InstallShield

< Back **Next >** Cancel Help

Enabling OS security is not necessary. Leave the check box blank and click **Next**. The following panel is displayed.



Review the setup and click **Install**. After a few minutes, the following panel is displayed.



Click **Finish**.

Verify & Apply DB2 Licence

Verify that you have a DB2 license. Check the license status using the following command:

```

C:\Users\Administrator>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"

C:\Users\Administrator>db2level
DB210851 Instance "DB2" uses "64" bits and DB2 code release "SQL09072" with
level identifier "00030107".
Informational tokens are "DB2 09.7.200.350", "s100514", "IP23084", and Fix Pack
"2".
Product is installed at "C:\IBM\SQLLIB" with DB2 Copy Name "DB2COPY1".

C:\Users\Administrator>_

```

Locate the DB2 license file named **db2ese_o.lic**. Apply this file using the following command:

```

C:\Users\Administrator>db2licm -a c:\IBM\SQLLIB\BIN\db2ese_o.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: "C:\IBM\SQLLIB\license\en"

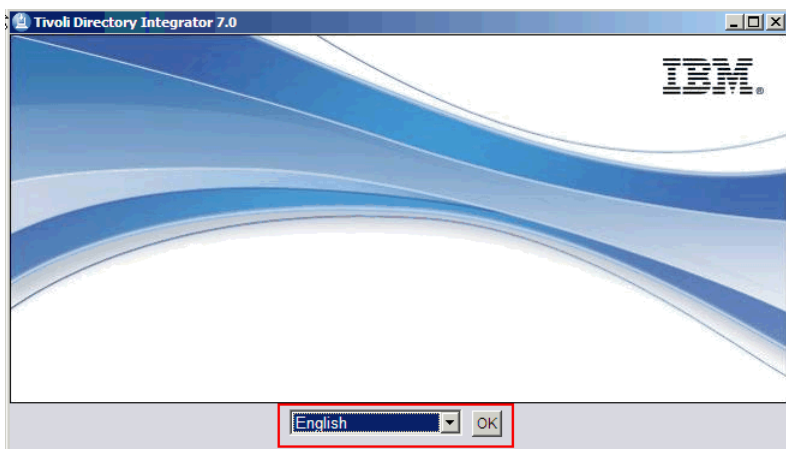
C:\Users\Administrator>db2level
DB21085I Instance "DB2" uses "64" bits and DB2 code release "SQL09072" with
level identifier "08030107".
Informational tokens are "DB2 09.7.200.358", "s100514", "IP23084", and Fix Pack
"2".
Product is installed at "C:\IBM\SQLLIB" with DB2 Copy Name "DB2COPY1".

C:\Users\Administrator>db2licm -l
Product name:          "DB2 Enterprise Server Edition"
License type:         "Restricted"
Expiry date:          "Permanent"
Product identifier:   "db2ese"
Version information:  "9.7"

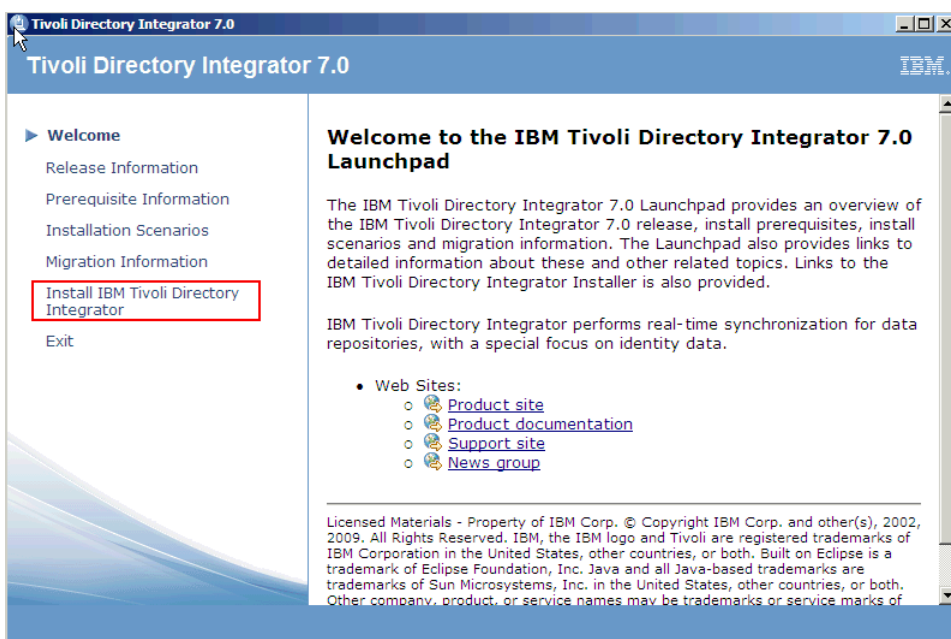
```

Installing Tivoli Directory Integrator V7.0 & fix pack 5

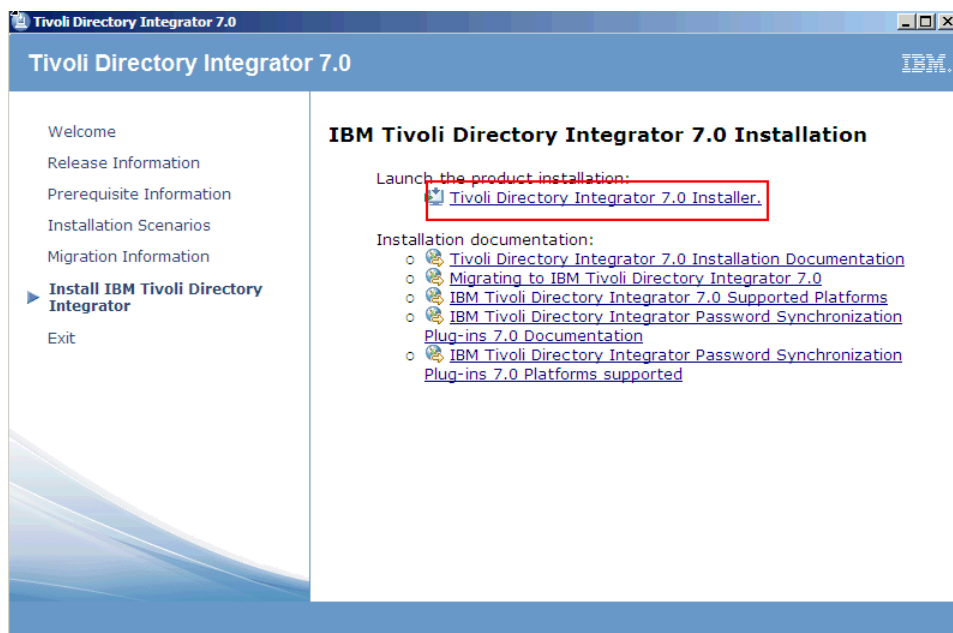
Unzip the file that you downloaded in a directory on your hard disk. Go to the directory and run **launchpad.exe**. The following panel is displayed.



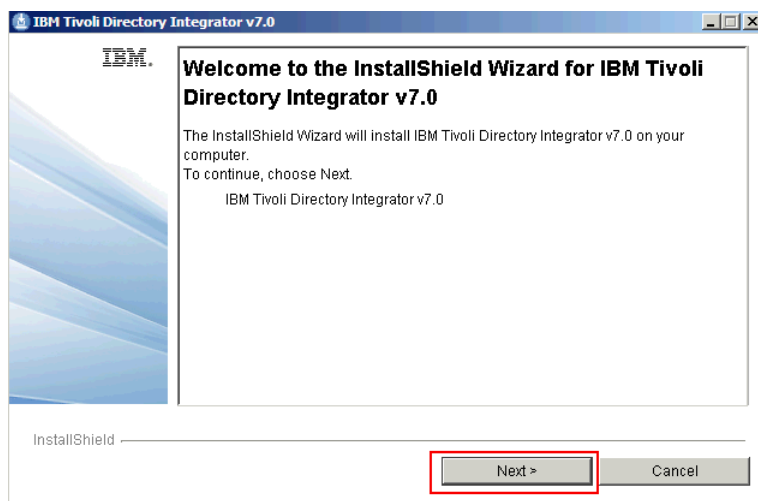
Select the language and click **OK**. The following panel is displayed.



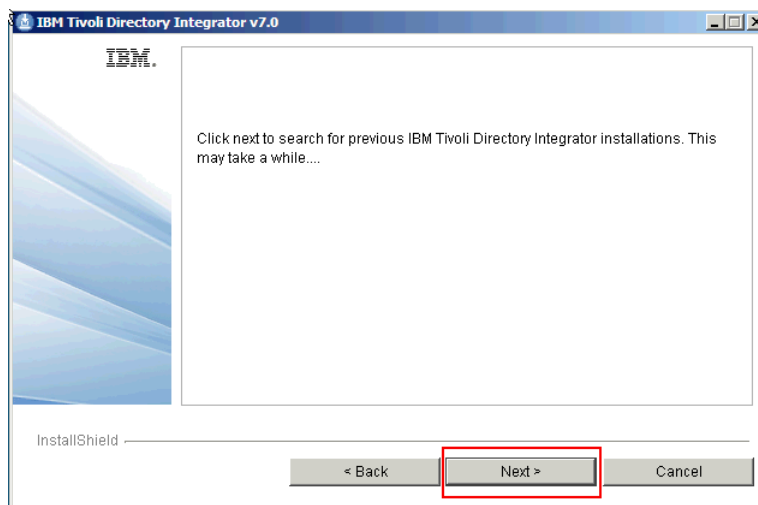
Click the "Install IBM Tivoli Directory Integrator" link. The following panel is displayed.

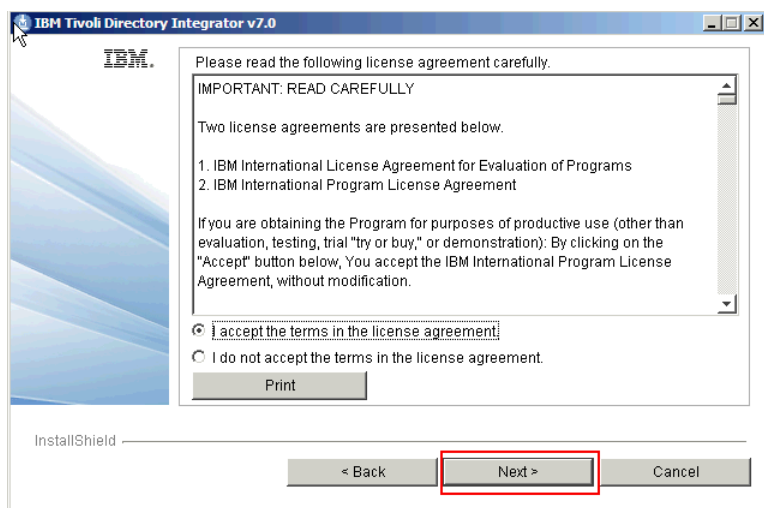


Click the "Tivoli Directory Integrator 7.0 Installer" link. The following panel is displayed.

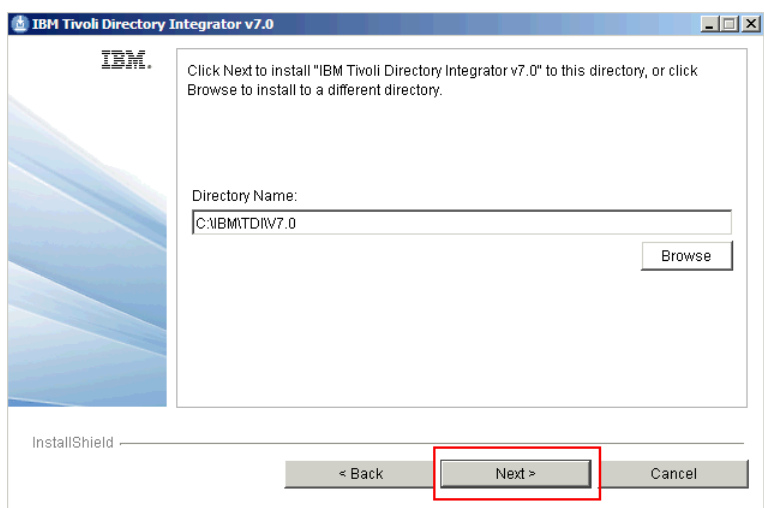


Click **Next**. The following panel is displayed.

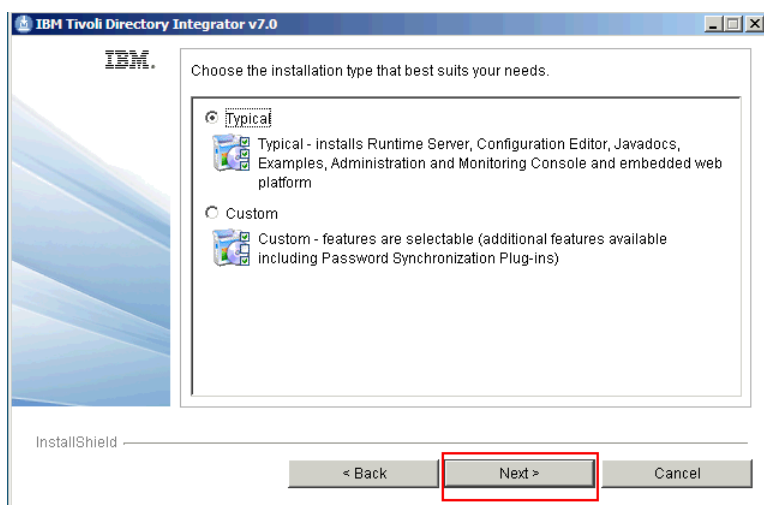




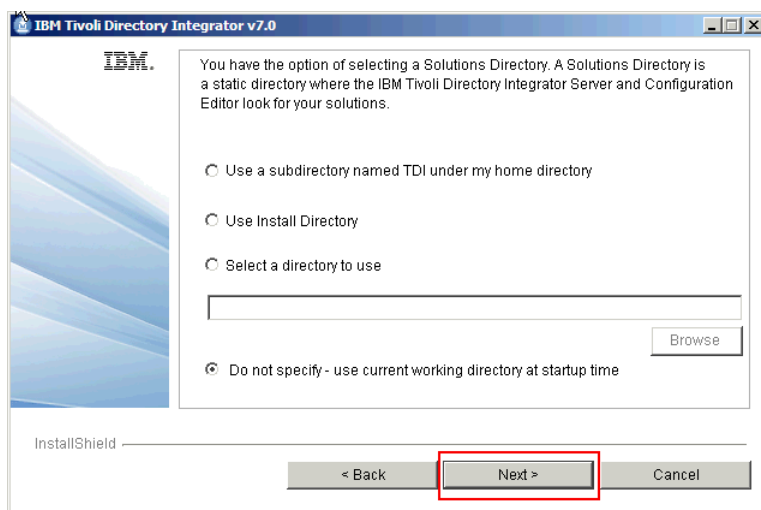
Accept the license and click **Next**. The following panel is displayed.



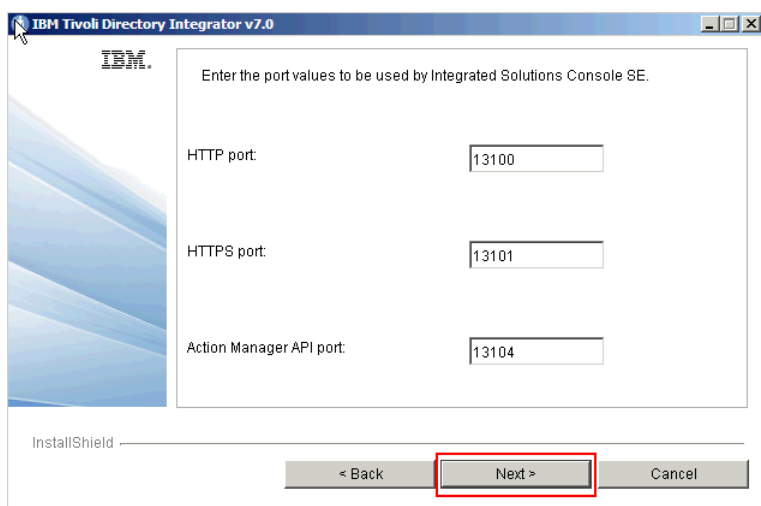
Choose the installation directory and click **Next**. The following panel is displayed.



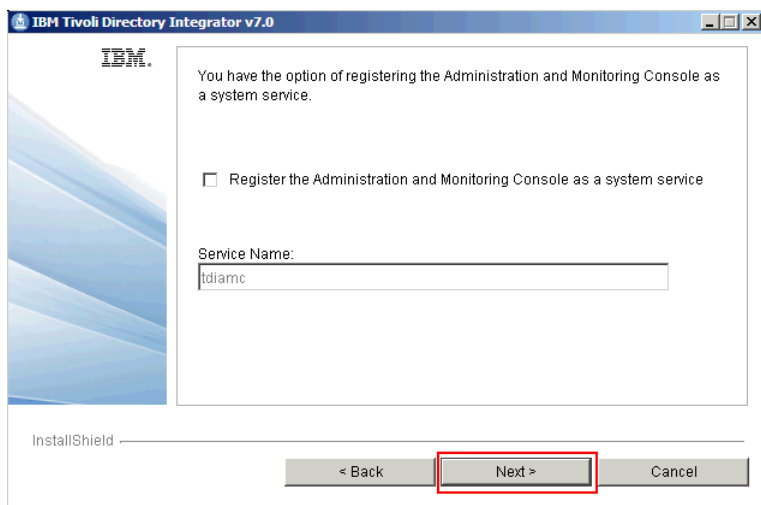
Select "Typical" and click **Next**. The following panel is displayed.



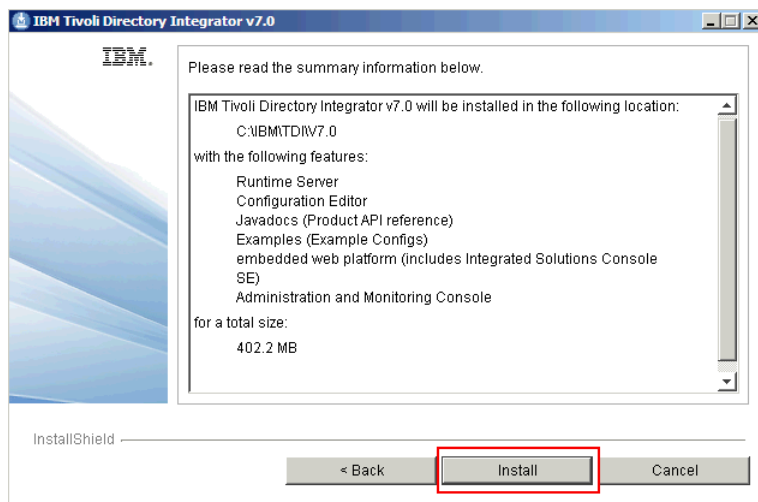
Select "Do not specify - use current working directory at startup time" and click **Next**. The following panel is displayed.



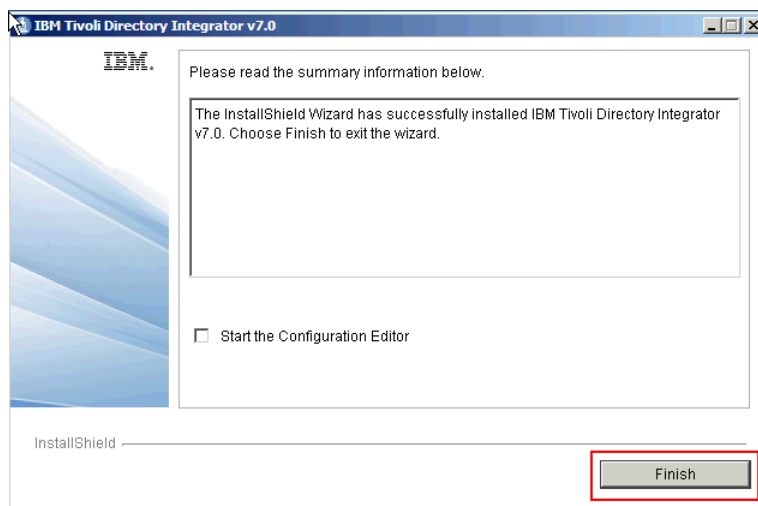
Leave the default values and click **Next**. The following panel is displayed.



Leave the check box blank and click **Next**. The following panel is displayed.



Review the setup and click **Install**. After a few minutes, the following panel is displayed.



Click **Finish**.

Apply fix pack 5 to TDI

Unzip the file 7.0.0-TIV-TDI-FP0005.zip to create a folder with the same name (in this example, the file is unzipped in C:\). Change to this directory and locate the UpdateInstaller.jar Jar file. Copy and paste this file in the C:\IBM\TDIV7.0\maintenance directory, replacing the existing file with the same name.

Change to the C:\IBM\TDIV7.0\bin directory and run the following command:

```
applyUpdates.bat -update C:\7.0.0-TIV-TDI-FP0005\TDI-7.0-FP0005.zip
```

```
Administrator: Command Prompt
Microsoft Windows [Version 6.0.6001]
Copyright (c) 2006 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\IBM\TDI\U7.0\bin
C:\IBM\TDI\U7.0\bin>applyUpdates.bat -update C:\7.0.0-TIV-TDI-FP0005\TDI-7.0-FP0005.zip
CTGDK0023I Applying fix 'TDI-7.0-FP0005' using backup directory 'C:\IBM\TDI\U7.0\maintenance\BACKUP\TDI-7.0-FP0005'.
CTGDK0027I Updating SERUER.
CTGDK0027I Updating CE.
CTGDK0027I Updating EXAMPLES.
C:\IBM\TDI\U7.0\bin>
```

Setting up Federated Repositories and Application Security

Make sure that the Deployment Manager is started.

Open the WebSphere Administration Console: <http://connections.example.com:9060/lbm/console>

Log in with the user you defined previously as administrator.

Integrated Solutions Console

Log in to the console.

User ID:

Password:

Expand the "Security" section and click **Global security**.

Integrated Solutions Console Welcome wsadmin Help | Logout

Cell=connectionsCell01, Profile=Dmgr01 Close pa

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security**
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

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

Administrative security

Enable administrative security

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

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources

Warn if applications are granted custom permissions

Restrict access to resource authentication data

User account repository

Current realm definition
 Federated repositories

Available realm definitions
 Federated repositories

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 Se...

Use realm-qualified user names

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

Click **Configure**.

Integrated Solutions Console Welcome wsadmin Help | Logout

Cell=connectionsCell01, Profile=Dmgr01 Close pa

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

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

Administrative security

Enable administrative security

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

Application security

Enable application security

Java 2 security

Use Java 2 security to restrict application access to local resources

Warn if applications are granted custom permissions

Restrict access to resource authentication data

User account repository

Current realm definition
 Federated repositories

Available realm definitions
 Federated repositories

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 Se...

Use realm-qualified user names

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

Click **Add Base entry to Realm**.

Integrated Solutions Console Welcome wsadmin Help | Logout

Cell=connectionsCell01, Profile=Dmgr01

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

Global security > Federated repositories

By federating repositories, identities stored in multiple repositories can be managed in a single, virtual realm. The realm can consist of identities in the file-based repository that is built into the system, in one or more external repositories, or in both the built-in repository and one or more external repositories.

General Properties

* Realm name
defaultWIMFileBasedRealm

* Primary administrative user name
wsadmin

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

Server user ID or administrative user on a Version 6.0.x node

Password

Ignore case for authorization

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

You can administer the following resources:

Click **Add Repository**.

Cell=connectionsCell01, Profile=Dmgr01

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

Global security > Federated repositories > Repository reference

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.

General Properties

* Repository
 none defined

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm

Distinguished name of a base entry in this repository

Type a name in the "Repository identifier" field, select a Directory type, type the "Primary host name," and then type the user name and password of the "Bind distinguished name." Use default values for the other fields.

Cell=connectionsCell01, Profile=Dmgr01 Close

View: All tasks

- Welcome
- Guided Activities
- Servers
- Applications
- Services
- Resources
- Security
 - Global security
 - Security domains
 - Administrative Authorization Groups
 - SSL certificate and key management
 - Security auditing
 - Bus security
 - JAX-WS and JAX-RPC security runtime
- Environment
- System administration
- Users and Groups
- Monitoring and Tuning
- Troubleshooting
- Service integration
- UDDI

Global security

Global security > Federated repositories > Repository reference > New

Specifies the configuration for secure access to a Lightweight Directory Access Protocol (LDAP) repository with optional failover servers.

General Properties

* Repository identifier
myLDAP

LDAP server

* Directory type
IBM Tivoli Directory Server

* Primary host name
ldap.example.com

Port
389

Failover server used when primary is not available:

Delete

Select	Failover Host Name	Port
None		

Add

Support referrals to other LDAP servers
ignore

Security

Bind distinguished name
cn=root

Bind password

Login properties
uid

LDAP attribute for Kerberos principal name

Certificate mapping
EXACT_DN

Certificate filter

Require SSL communications

Centrally managed
Manage endpoint security configurations

Use specific SSL alias
CellDefaultSSLSettings SSL configurations

At the bottom of the page, click **Apply**. Next, at the beginning of the page, click **Save** as shown in the following panel.

Messages

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

The server may need to be restarted for these changes to take effect.

Fill the first field with the value of the base DN of the user container of your LDAP server. This changes depending on the type of LDAP that you have. In this example, TDS is used so the value is

dc=connections,dc=example,dc=com.

The second field defines the location in the LDAP directory information tree from which the LDAP search begins. The entries beneath it in the tree can also be accessed by the LDAP search. In this example, the value is dc=connections,dc=example,dc=com.

For other LDAP servers:

Domino - Type ou=, o=, ... (for example, all that follows CN=username in the User Name in Domino in both fields)

Active Directory - Use the same value as TDS.

When you are done, click **Apply** and then click **Save**.

Global security

Global security > Federated repositories > dc=connections,dc=example,dc=com

Specifies a set of identity entries in a repository that are referenced by a base entry into the directory information tree. If multiple repositories are included in the same realm, it might be necessary to define an additional distinguished name that uniquely identifies this set of entries within the realm.

General Properties

* Repository
myLDAP Add Repository...

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm
dc=connections,dc=example,dc=com

Distinguished name of a base entry in this repository
dc=connections,dc=example,dc=com

Apply OK Reset Cancel

Click **OK** and then click **Save**.

Verify that the new base entry has been saved.

Repositories in the realm:

Select	Base Entry	Repository Identifier	Repository Type
<input type="checkbox"/>	dc=connections,dc=example,dc=com	myLDAP	LDAP:IDS
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

Click **OK** and then click **Save**.

Enable Administrative security and Application security. Do not enable Java 2 security. Click **Apply** and then click **Save**.

Integrated Solutions Console Welcome wsadmin Help | Logout Close page

View: All tasks

Cell=connectionsCell01, Profile=Dmgr01

Global security

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

Security Configuration Wizard | Security Configuration Report

Administrative security

- Enable administrative security
 - [Administrative user roles](#)
 - [Administrative group roles](#)
 - [Administrative authentication](#)

Application security

- Enable application security

Java 2 security

- Use Java 2 security to restrict application access to local resources
 - Warn if applications are granted custom permissions
 - Restrict access to resource authentication data

User account repository

Current realm definition:

Federated repositories:

Available realm definitions: Federated repositories

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](#)

Optional: If you want to set up SSO later, you must do the following:

Expand the "Security" section and click **Global security**. On the right, click the + sign next to "Web and SIP security" and then click **Single sign-on (SSO)**.

Authentication

Authentication mechanisms and expiration

- LTPA
- Kerberos and LTPA
 - [Kerberos configuration](#)
 - [Authentication cache settings](#)
- Web and SIP security
 - General settings
 - Single sign-on (SSO)**
 - SPNEGO Web authentication
 - Trust association
 - SIP digest authentication
- RMI/IIOP security
- Java Authentication and Authorization Service
 - Use realm-qualified user names

Insert the Domain name (for example, **example.com**) and then select the "Interoperability Mode" check box.

Global security

Global security > Single sign-on (SSO)

Specifies the configuration values for single sign-on.

General Properties

- Enabled
- Requires SSL
- Domain name:
- Interoperability Mode
- Web inbound security attribute propagation

Click **Apply** and then click **Save**.

Log out from the administrative console. Then, stop and restart the Deployment Manager.

Installation and Configuration Instructions

After all of the prerequisite steps are complete, take the following actions to configure, create, and populate the database as well as install Lotus Connections 3.0.

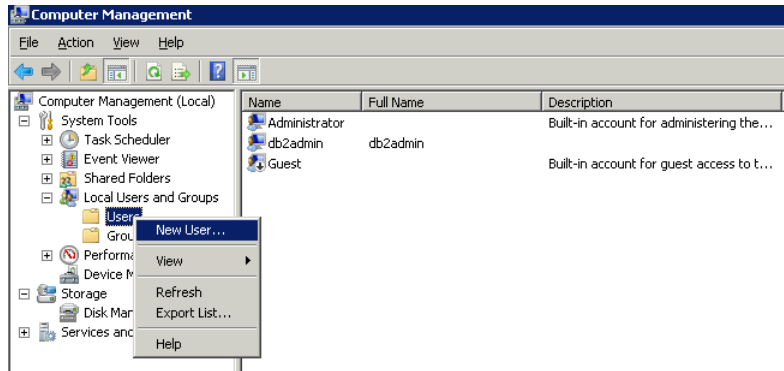
Configure the Database Instance

Following the DB2 install process proposed above, the instance named **DB2** is created. This instance is used to host our databases for this scenario.

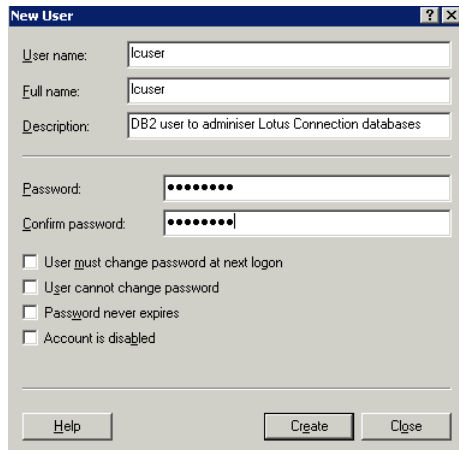
On the **db.example.com** machine, extract the Lotus Connections Wizards to a directory. From here, find the folder named **Wizards**. This folder contains two batch files of interest - dbWizard.bat and populationWizard.bat, the first of which is a wizard that creates the nine databases required to run Lotus Connections, the second that populates the profiles database with user data.

- Note that in a Linux environment, these files have the extension '.sh' and are used in exactly the same way.

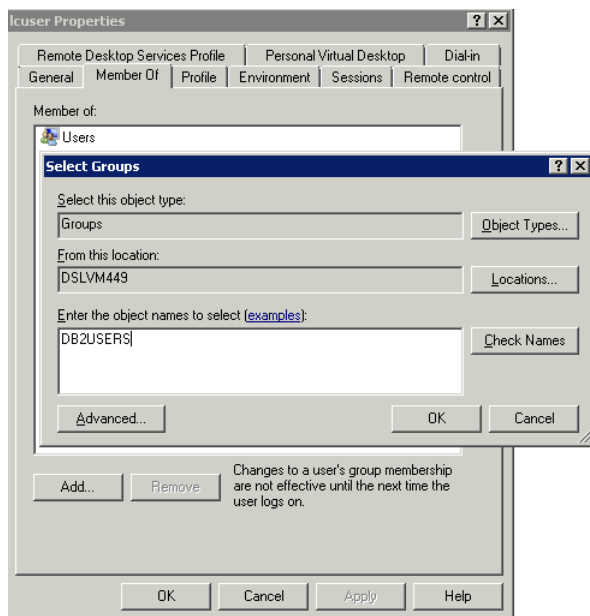
Before creating the databases, you must create a user on the operating system for DB2 named **lcuser**. This user will be the owner of the databases when they are created. On the database machine, expand **Computer Management > System Tools > Local Users and Groups > Users**. Right click on **Users** and select **New User...** as shown.



Enter user and password details of **lcuser**. Ensure to deselect the "User must change password at next logon" option. Click **Create** when ready.



After the user is created, right-click the user and click **Properties**. Select the **Member of** tab. The **lcuser** user must be added to the **DB2USERS** group. Click **Add** and type **DB2USERS** in the "Enter the object names to select" field as shown below. Click **OK** until you are back to the Computer Management panel. Your computer is now prepared for the Lotus Connections databases to be created.



Note: If the DB2USERS group is not found, extended security for DB2 on Windows might not be enabled. To enable extended security on Windows, stop the database, run the **db2extsec.exe** command, and then restart the database again as shown. For more information about Extended Windows security using DB2ADMNS and DB2USERS groups, refer to the DB2 product documentation.

```
PS C:\IBM\SQLLIB\BIN> db2stop
12/08/2010 14:36:59      0      0      SQL1064N  DB2STOP processing was successful.
SQL1064N  DB2STOP processing was successful.
PS C:\IBM\SQLLIB\BIN> .\db2extsec.exe
The DB2EXTSEC command completed successfully.
PS C:\IBM\SQLLIB\BIN> db2start
12/08/2010 14:37:58      0      0      SQL1063N  DB2START processing was successful.
SQL1063N  DB2START processing was successful.
PS C:\IBM\SQLLIB\BIN>
```

Linux Only Step

For Linux users, the following steps cover the process mentioned above:

- Log into the DB2 server as root user and then type the following commands to create the user:


```
useradd lcuser
passwd lcuser
```
- When prompted for a new password, enter it, and then confirm the password.

Important:

-

When using other databases, such as Oracle Database Server or Microsoft SQL Server, you do not need to create the "lcuser" user, as instructed above. Instead, when using the wizard to create the databases, new database users are created. You are prompted to provide a password for each of the database users.

* When using Microsoft SQL Server, you are prompted to provide a location on the file system for the databases being created.

Linux Only Step

Before running the database wizard (dbWizard) on Linux systems, ensure the following is set:

- Ensure that users (other than root) have permission to access the Lotus Connections Wizards directory. To do so, run the following command against the directory containing these wizards:


```
chmod -R 777 <wizards_directory>
```
- To grant display authority to other users, run the following command as root:


```
xhost +
```
- Take note of the DISPLAY variable with following command:


```
echo $DISPLAY
```
- On Linux, **dbWizard** must be run by the database instance user (for example, **db2inst1** user). Switch to this database user from the terminal as follows:


```
su - db2inst1
```
- Set the DISPLAY variable with the following command:


```
export DISPLAY=<hostname:displaynumber.screennumber>
```

Where *<hostname:displaynumber.screennumber>* specifies the client system, monitor number and window number (for example, **localhost:0.0**).

- To verify that this user can use the display with the following simple test, enter the following command:

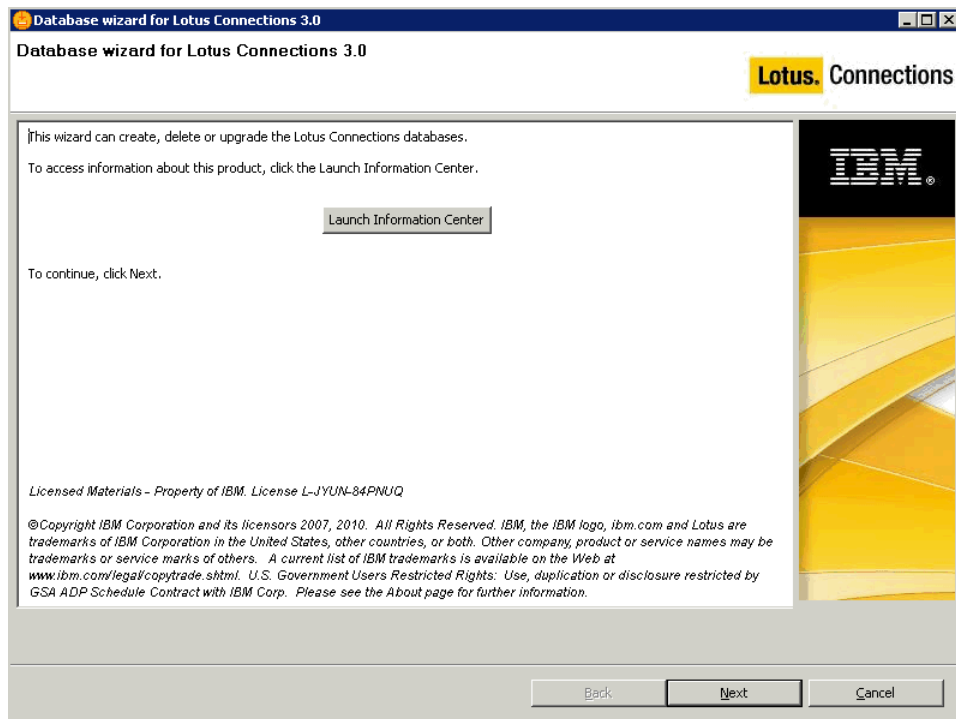

```
xclock
```

If the clock launches, the system is ready to begin the dbWizard. Press **Ctrl+C** to exit the clock.

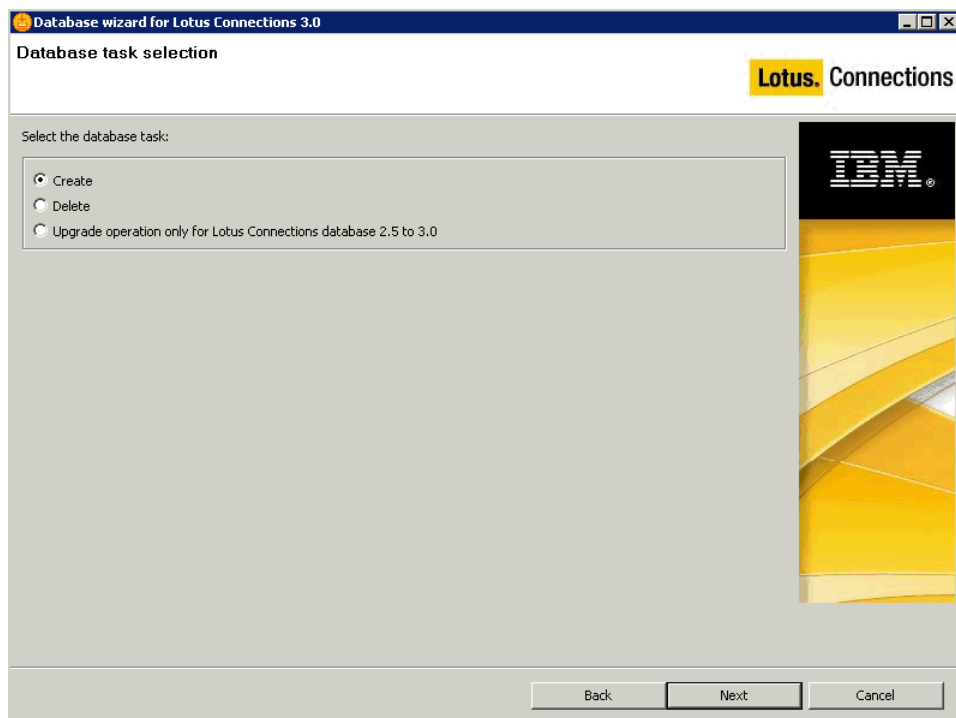
- Ensure the database is started and run the **dbWizard.sh** command to begin to create the databases. The screen shots below are the same for all operating systems.

To run the database wizard, follow these steps:

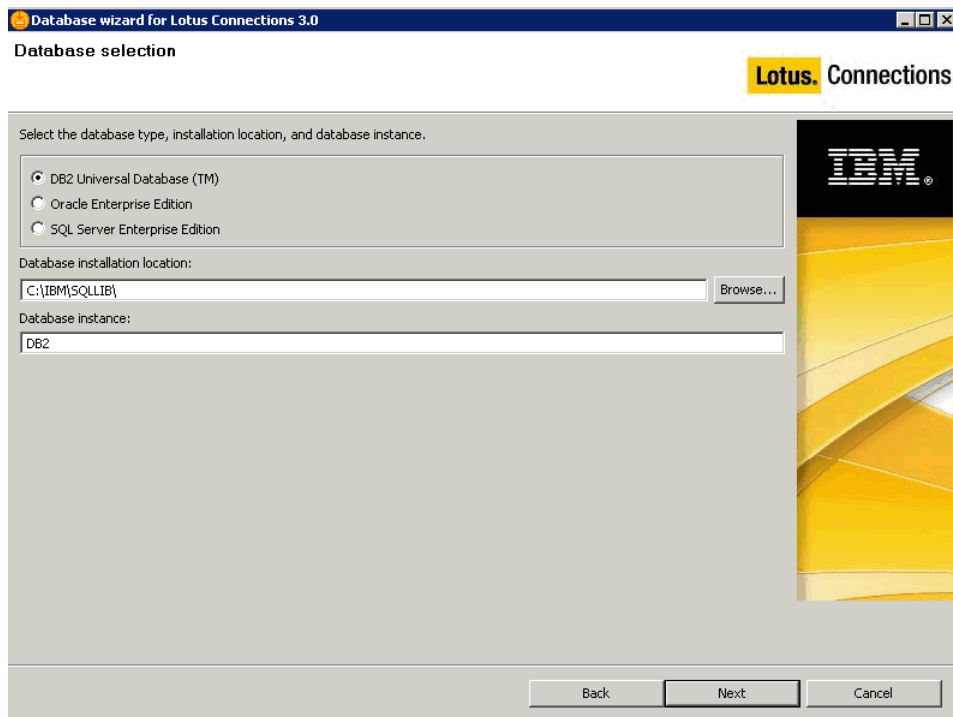
- 1.Run dbWizard.bat. The following panel is displayed.



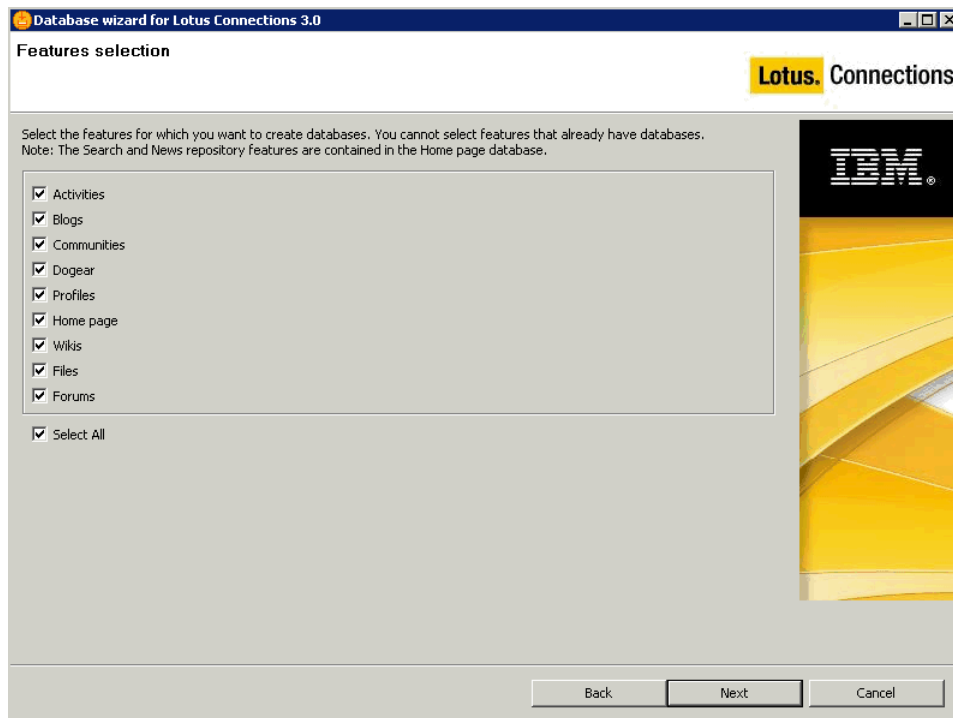
2. Select **Next** on the welcome panel. The following panel is displayed.



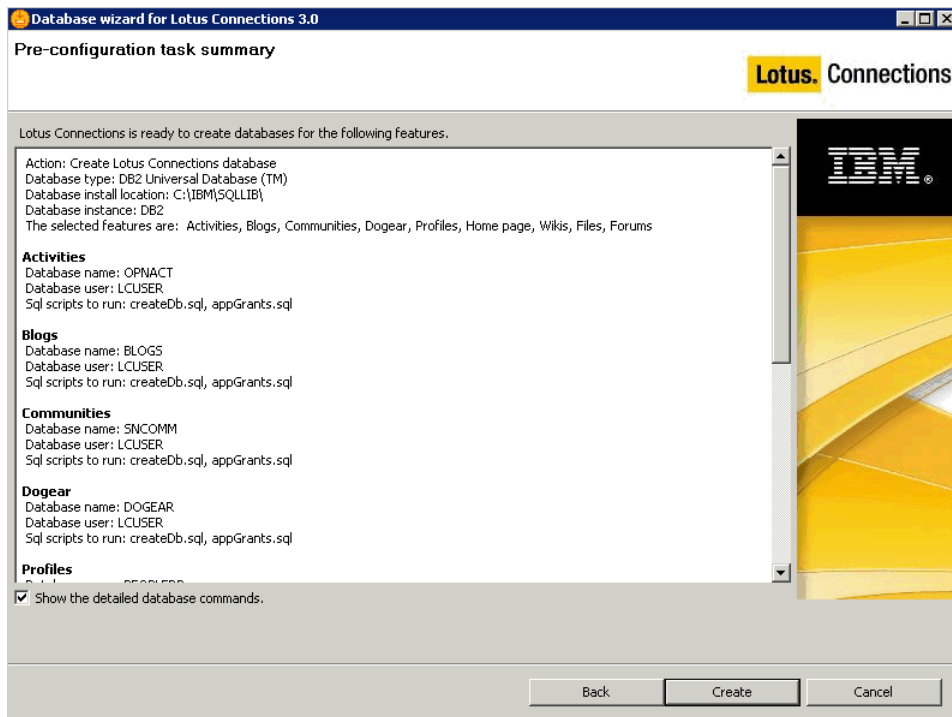
3. Select which task to use on the panel above. For example, select **Create** and then click **Next**. The following panel is displayed.



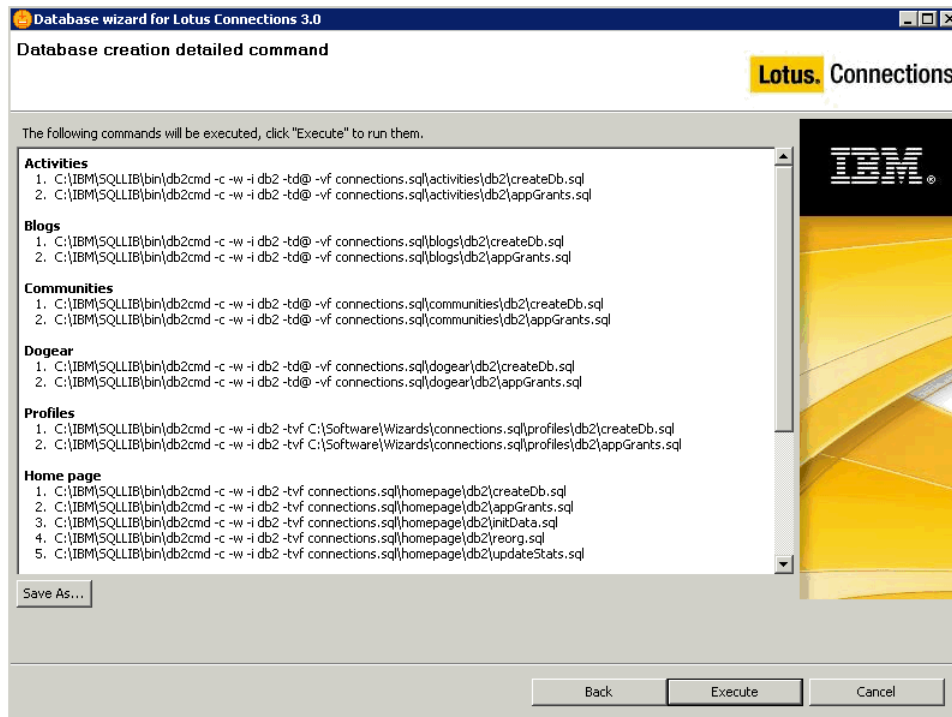
4. On the panel above, check the database type you are using, in this case DB2. Then select the installation location and the DB2 instance name. Click **Next** to display the following panel.



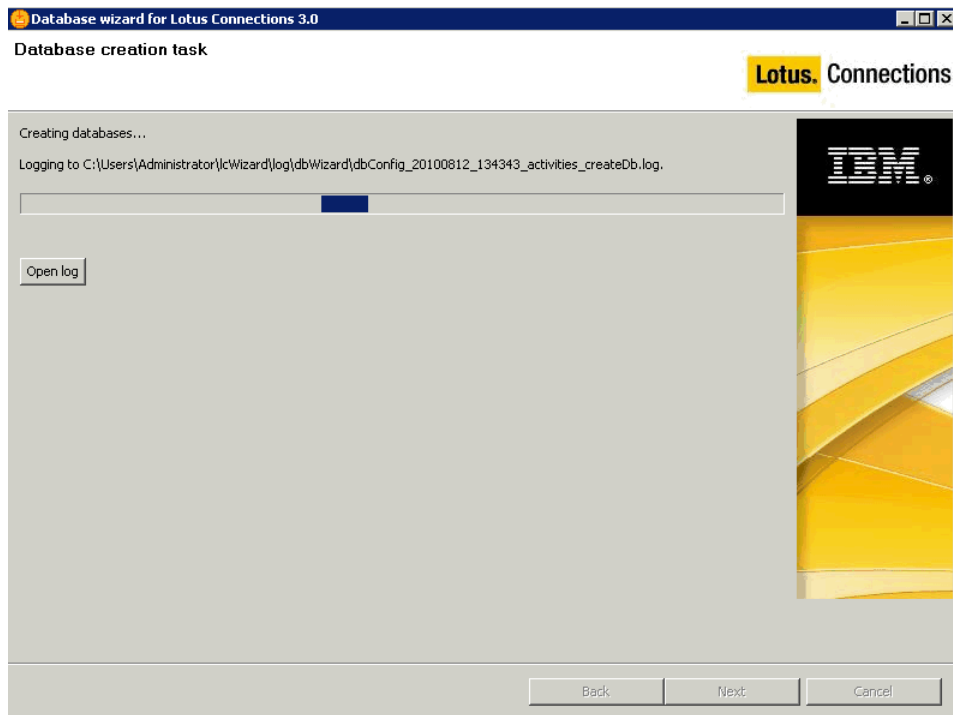
5. Select which database tables to create. In this case, all database tables are required since all Lotus Connections services are being installed. Ensure all check boxes are selected and then click **Next**. The following panel is displayed.



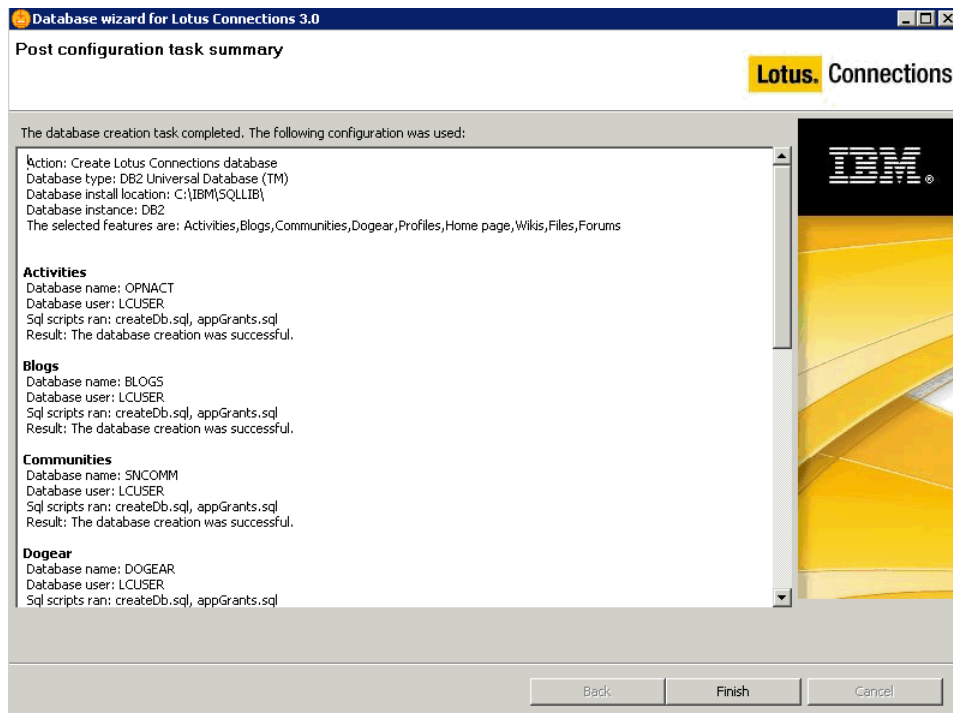
6. The panel above provides a summary of which databases will be created and which scripts are run to achieve this. For more information on the database commands, select the "Show the detailed database commands" check box. If you select this check box and click **Create**, the following panel is displayed. If you do not select this check box, a progress indicator is displayed as the databases are created.



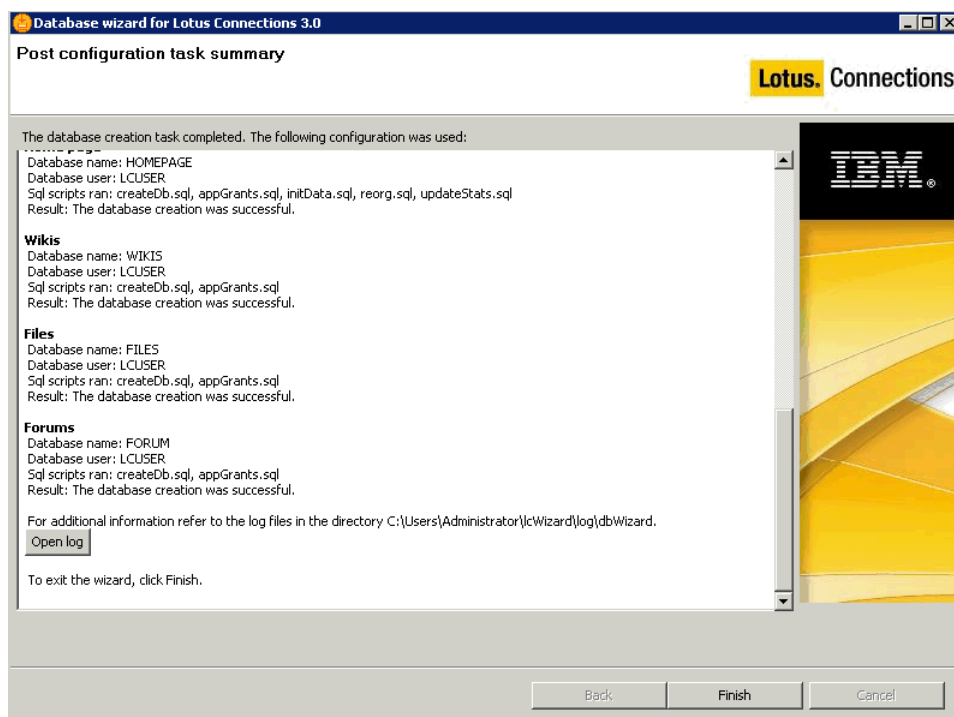
If you choose to view the detailed database command panel above, you can save these commands via the **Save As...** button or click **Execute** to launch the creation of these databases.



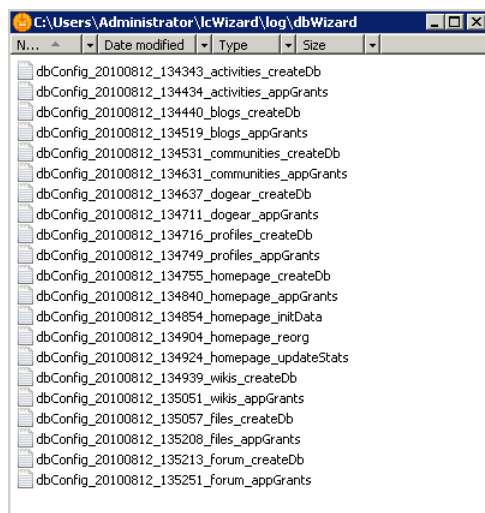
7. During the creation process, you can open the log files to view progress. The **Open log** button opens the directory containing the logs. The database creation process should only take a few minutes, depending on the speed of your system. After the process is complete, the following summary panel is displayed:



8. Results are displayed. The result field for each database should state, "The database creation was successful". Scroll down the list to verify that the databases were created successfully. In the event that there were issues with the database creation, click **Open log** to view the logs for the script that failed. The log file should indicate what the problem is. For additional help, see the Troubleshooting section of this document.



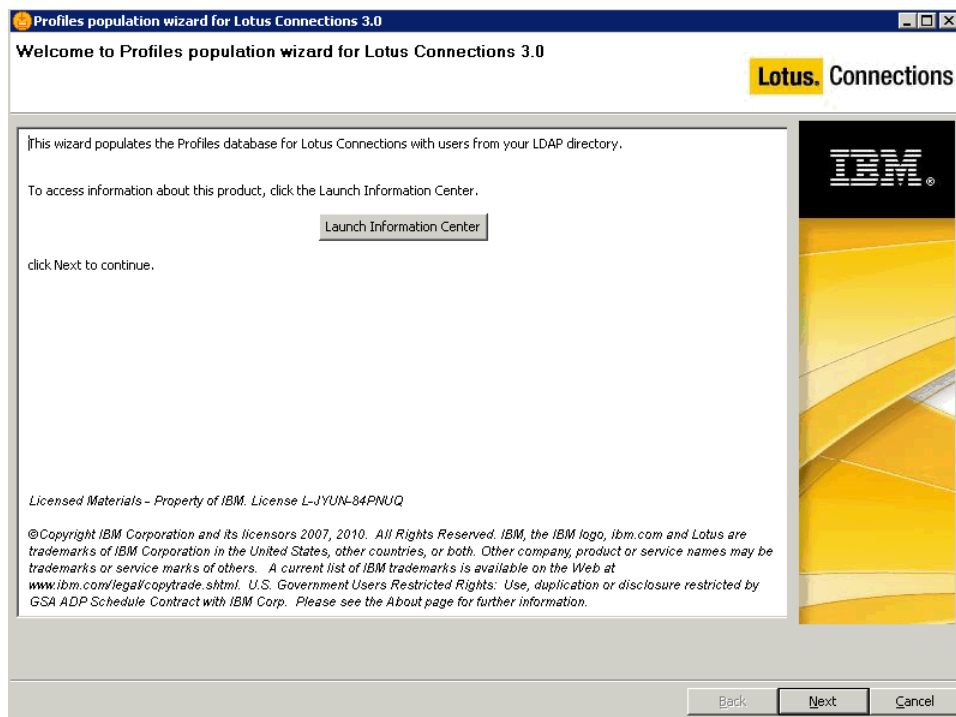
9. If you click the **Open log** button, the following folder displays the individual logs for each of the database creation scripts. To close this window, click the **X** icon on the top right. This action returns you to the summary panel in step 8. Click **Finish** to close the database wizard.



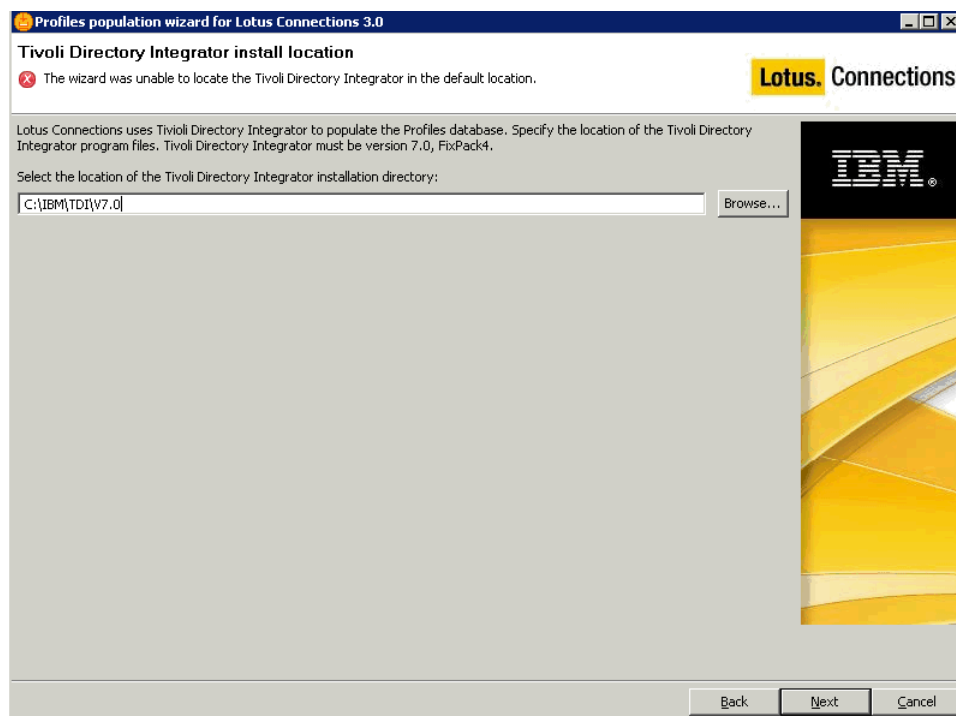
Populating the Profiles Database

The profiles database must be populated with users from the LDAP before you can log in to Lotus Connections 3.0. To begin populating user data in the profiles database, run the **populationWizard.bat** file.

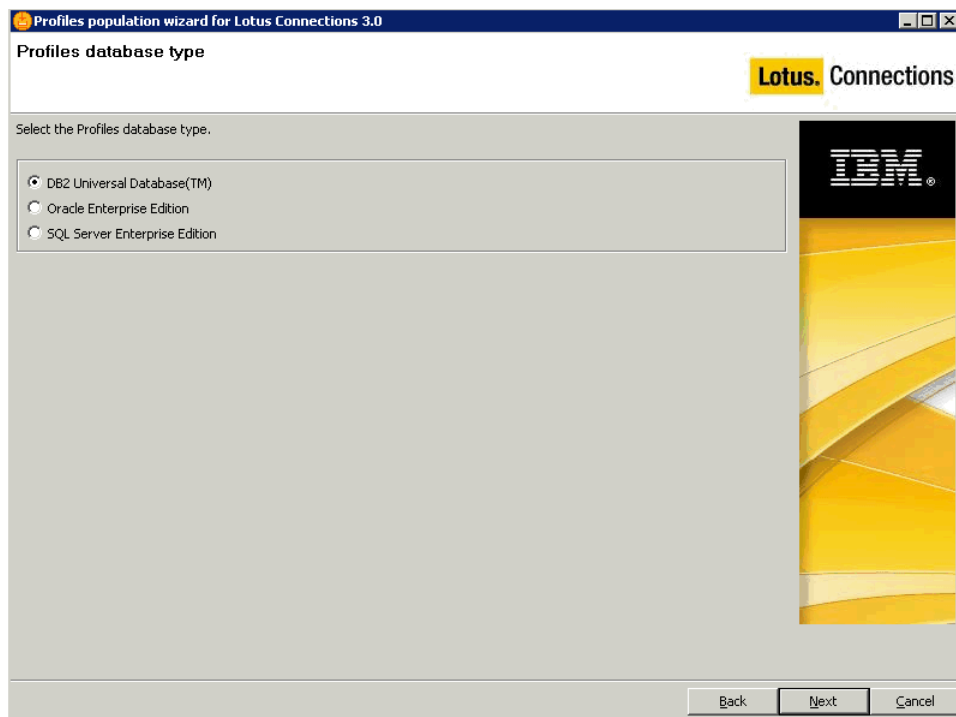
On the welcome panel, click **Next**. The following panel is displayed.



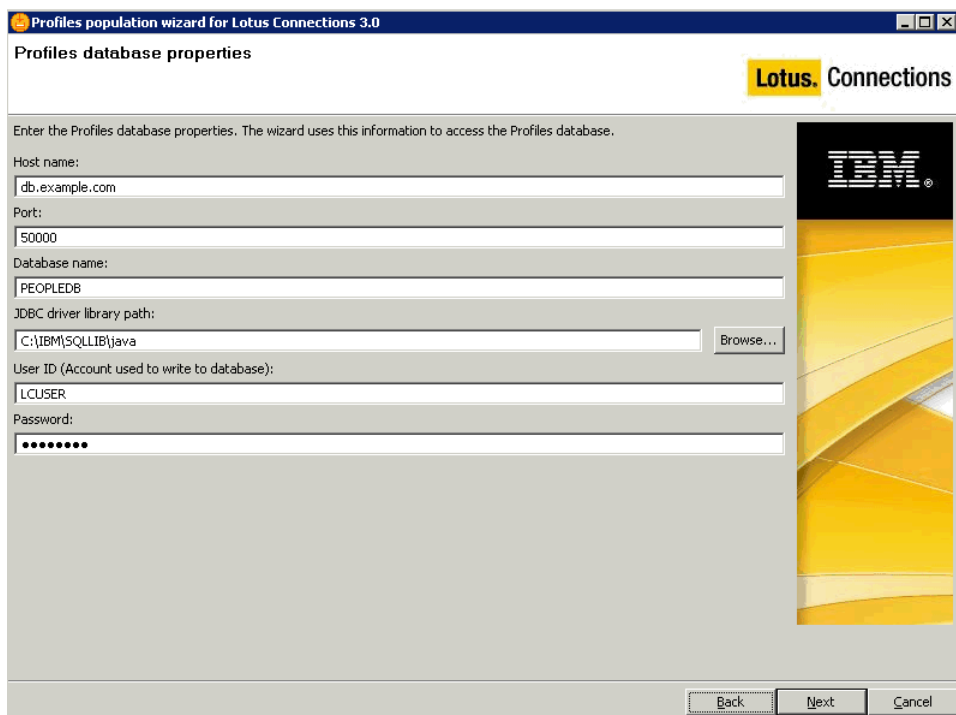
The wizard warns that Tivoli Directory Integrator is not installed in its default location. Select the location where it was installed, C:\IBMTDIV7.0, and then click **Next**.



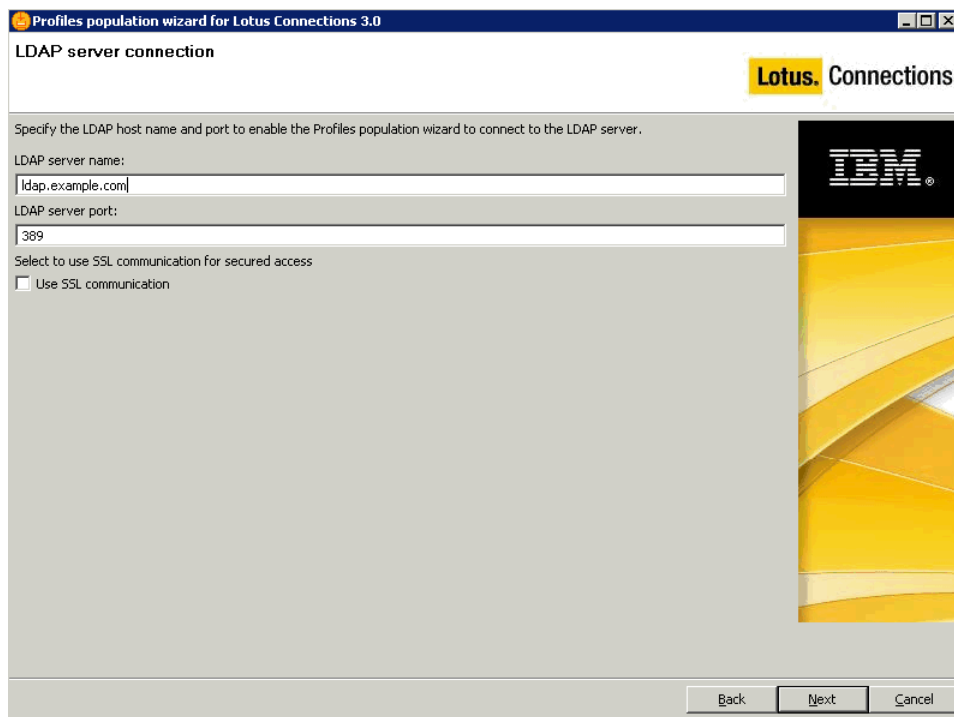
Select the database type, in this case DB2. Click **Next** to continue.



Now input the database information into the wizard. Update the fields as follows. The port number is **50000** by default, unless this was updated in the db2 config. Note that on Linux systems, the default port number is **50001**. Click **Next** to continue.



Type the LDAP server name and port number and then click **Next**.



The screenshot shows a window titled "Profiles population wizard for Lotus Connections 3.0" with the subtitle "LDAP server connection". The window includes the Lotus Connections logo and an IBM logo. The main content area contains the following text and fields:

Specify the LDAP host name and port to enable the Profiles population wizard to connect to the LDAP server.

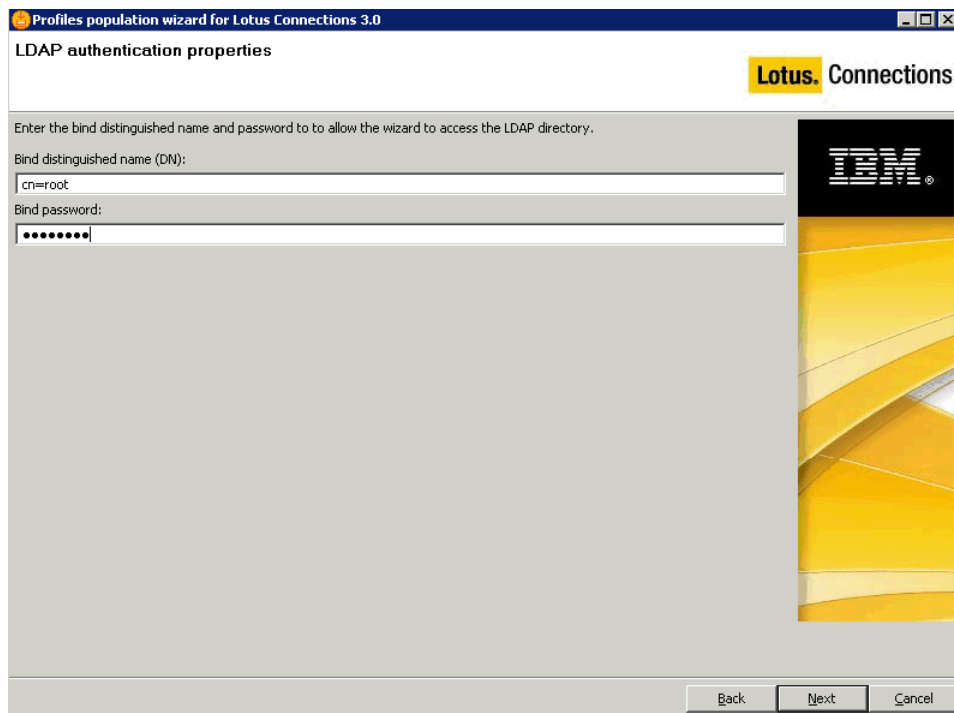
LDAP server name:

LDAP server port:

Select to use SSL communication for secured access
 Use SSL communication

At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

Enter the bind user and password and then click **Next**.



The screenshot shows a window titled "Profiles population wizard for Lotus Connections 3.0" with the subtitle "LDAP authentication properties". The window includes the Lotus Connections logo and an IBM logo. The main content area contains the following text and fields:

Enter the bind distinguished name and password to allow the wizard to access the LDAP directory.

Bind distinguished name (DN):

Bind password:

At the bottom right, there are three buttons: "Back", "Next", and "Cancel".

Select the search base and ensure that the LDAP user search filter is correctly identified. This filter can differ based on different LDAPs. Click **Next** to continue.

Profiles population wizard for Lotus Connections 3.0

Base distinguished name and filter for searches

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

LDAP user search base:

LDAP user search filter:

Back Next Cancel

You can customize the mappings between the LDAP and profiles database. For this example, default settings are used. Click **Next** to continue.

Profiles population wizard for Lotus Connections 3.0

Profiles database mapping

Select an LDAP attribute or a JavaScript function for each field in the Profiles database. You can sort the columns by selecting the column header, or select each row to add, remove, or edit the LDAP attribute or JavaScript function.

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

Back Next Cancel

Optional tasks can be run to add additional information to the profiles database, such as county, department and organizational details, which are not in LDAP. For this example, the default values are selected. For more information about running this task, see the following wiki article: http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Mapping_fields_manually_lc3

Profiles population wizard for Lotus Connections 3.0

Optional database tasks

Select the check box for each type of optional information that you want to add. You must supply a CSV file with data for each information type.

Countries
C:\Software\Wizards\TDIPopulation\TDISOL\win\socc.csv

Departments
C:\Software\Wizards\TDIPopulation\TDISOL\win\deptinfo.csv

Organizations
C:\Software\Wizards\TDIPopulation\TDISOL\win\orginfo.csv

Employee types
C:\Software\Wizards\TDIPopulation\TDISOL\win\emptytype.csv

Work locations
C:\Software\Wizards\TDIPopulation\TDISOL\win\workloc.csv

Do you want to run the task that marks the profiles of each manager?
 Yes
 No

When you are ready to begin population, click **Configure** as shown.

Profiles population wizard for Lotus Connections 3.0

Profiles population configuration summary

Profile population wizard is ready to run the population with the following configuration.

Configuration details:

```

Database host name: db.example.com
Database name: PEOPLEDB
Database port: 50000
JDBC driver library path: C:\IBM\SQLLIB\java
Database user ID: LCUSER
Database type: DB2 Universal Database(TM)
LDAP host name: ldap.example.com
LDAP server port: 389
Bind distinguished name: cn=root
LDAP user search base: DC=CONNECTIONS,DC=EXAMPLE,DC=COM
LDAP user search filter: (&(uid=*)(objectclass=inetOrgPerson))
Tivoli Directory Integrator installation location: C:\IBM\TDI\V7.0
Use SSL communication: No
Optional task list: Mark managers

```

To change any settings, click Back. To begin the configuration, click Configure

Profiles population wizard for Lotus Connections 3.0

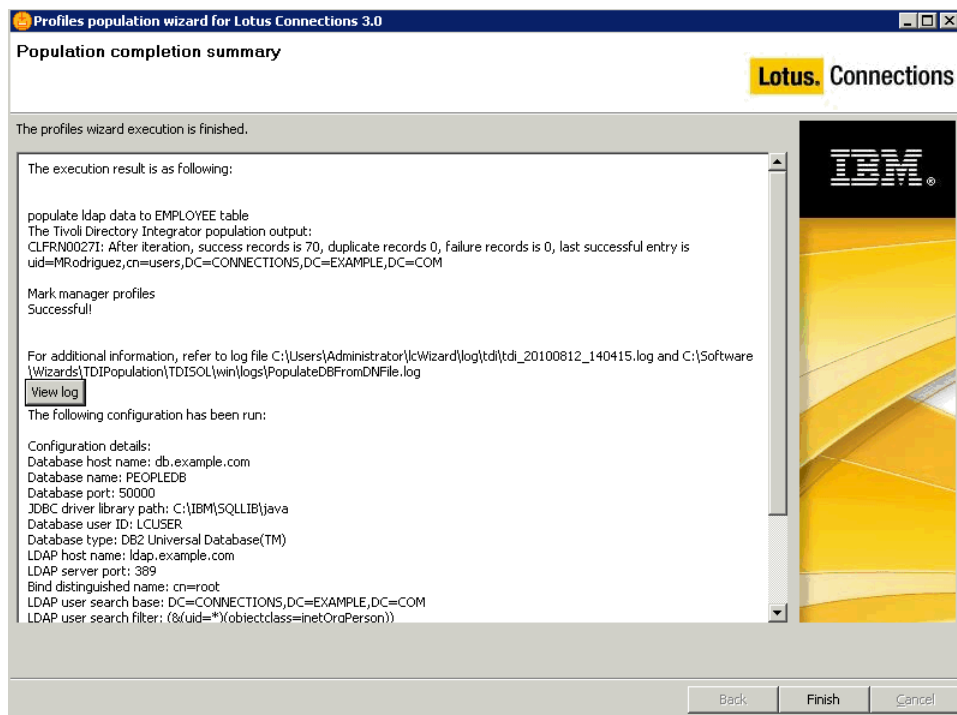
Executing population task

This task may take several minutes or hours, depending on the size of your LDAP directory.

Populating...

Logging into C:\Users\Administrator\cWizard\log\tdi_20100812_140415.log

When the profiles population is complete, the following completion summary is displayed. Verify the results before proceeding. Click **Finish** to close the Profiles population wizard.



Installing Lotus Connections 3.0

To install Lotus Connections ,complete the prerequisite tasks and then launch the installer.

Before You Install

Before beginning the installation, review the following considerations:

Rational Installation Manager

Lotus Connections 3.0 uses the Rational Installation Manager to provide an enhanced installation experience. Before beginning the installation, make sure to uninstall any older version of Rational Installation Manager. You are prompted to install this software when you launch the Lotus Connections 3.0 installation wizard.

Deployment Manager and Node Agent

Start the Deployment Manager before launching the installation wizard. The node agent should also be started so that resynchronization is possible between the Deployment Manager and node when required.

Linux / AIX Issues

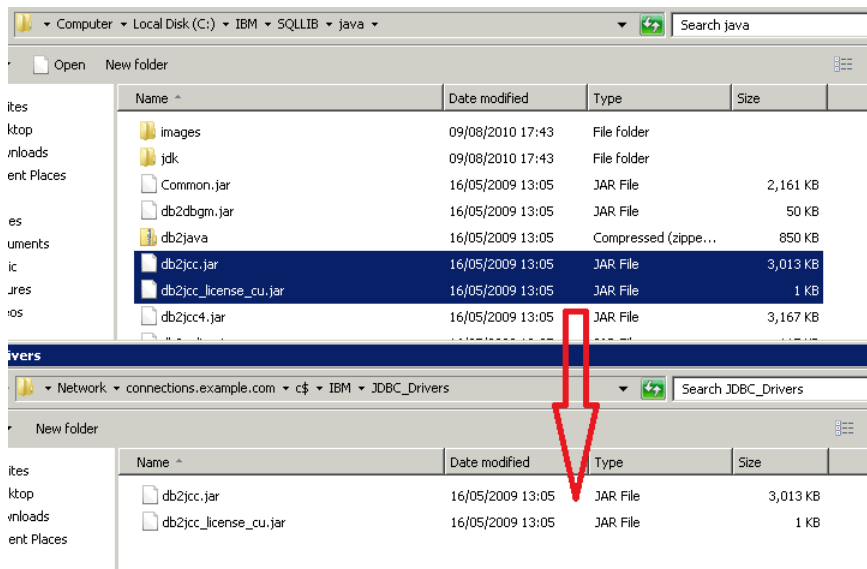
If installing Lotus Connections 3.0 on a Linux system as a non-root user, refer to the topic about installing as a non-root user at http://www-10.lotus.com/ldd/lcwiki.nsf/dx/Installing_as_a_nonroot_user_lc3. In AIX environments, GNU Tar is required to untar the installation packages. You can download GNU Tar from the following location: <http://www.ibm.com/systems/power/software/aix/linux/toolbox/alpha.html>.

Shared Data Folder

Because this is a one-node deployment, there is no need to mount a shared space for Lotus Connections data content to be stored. During installation, you are prompted to provide the location of the shared data directory. In this case, the local disk drive is used. The shared data directory, however, must be mounted on each node when there is more than one node.

DB2

Before you begin to install Lotus Connections 3.0, you must copy the JDBC driver from the DB2 server (db.example.com) to a local directory on connections.example.com - the directory used is C:\IBM\JDBC_Drivers). These drivers are used by Lotus Connections to connect to the database. On the DB2 machine, these drivers are located in the C:\IBM\SQLLIB\java directory. The names of the drivers required are db2jcc.jar and db2jcc_licence_cu.jar.

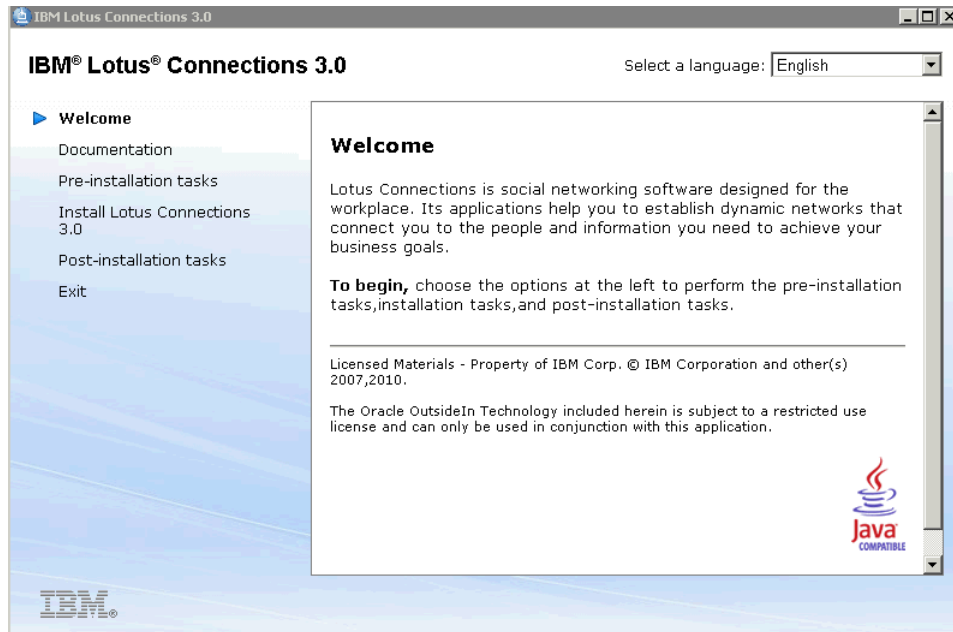


In cases where DB2 is not the database used, consult the following table to see which JDBC Driver to use. The drivers should be copied to this same location, regardless of which DB is used.

Database Type	JDBC Driver Name
DB2 v9.7 FP2	db2jcc.jar
	db2jcc_licence_cu.jar
Oracle	ojdbc6.jar
MS SQL Server	sqljdbc4.jar

Begin the Installation

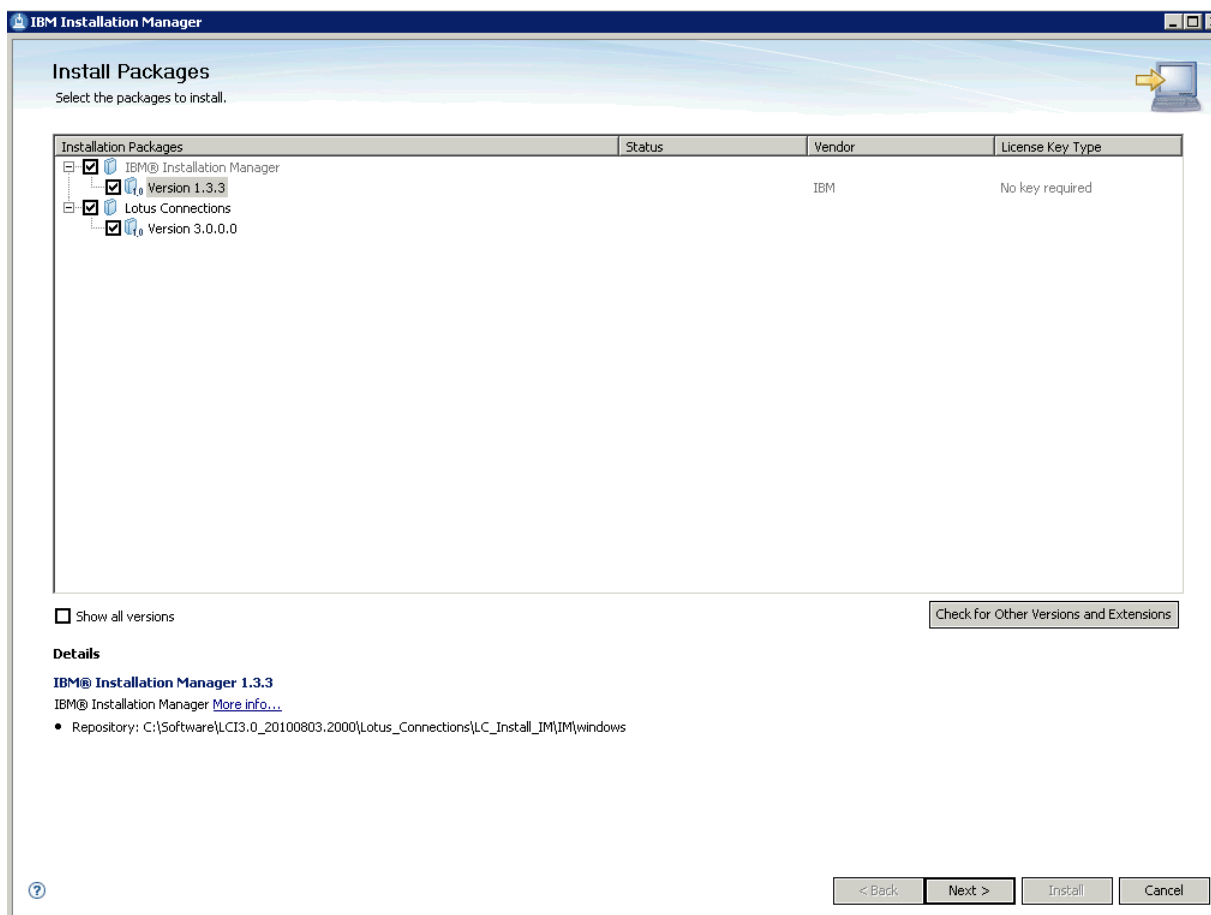
Extract the Lotus Connections installation files to a location on connections.example.com, such as C:\Software. From the extracted folder (LC_Install_IM), double-click **launchpad.exe** to begin the installation.



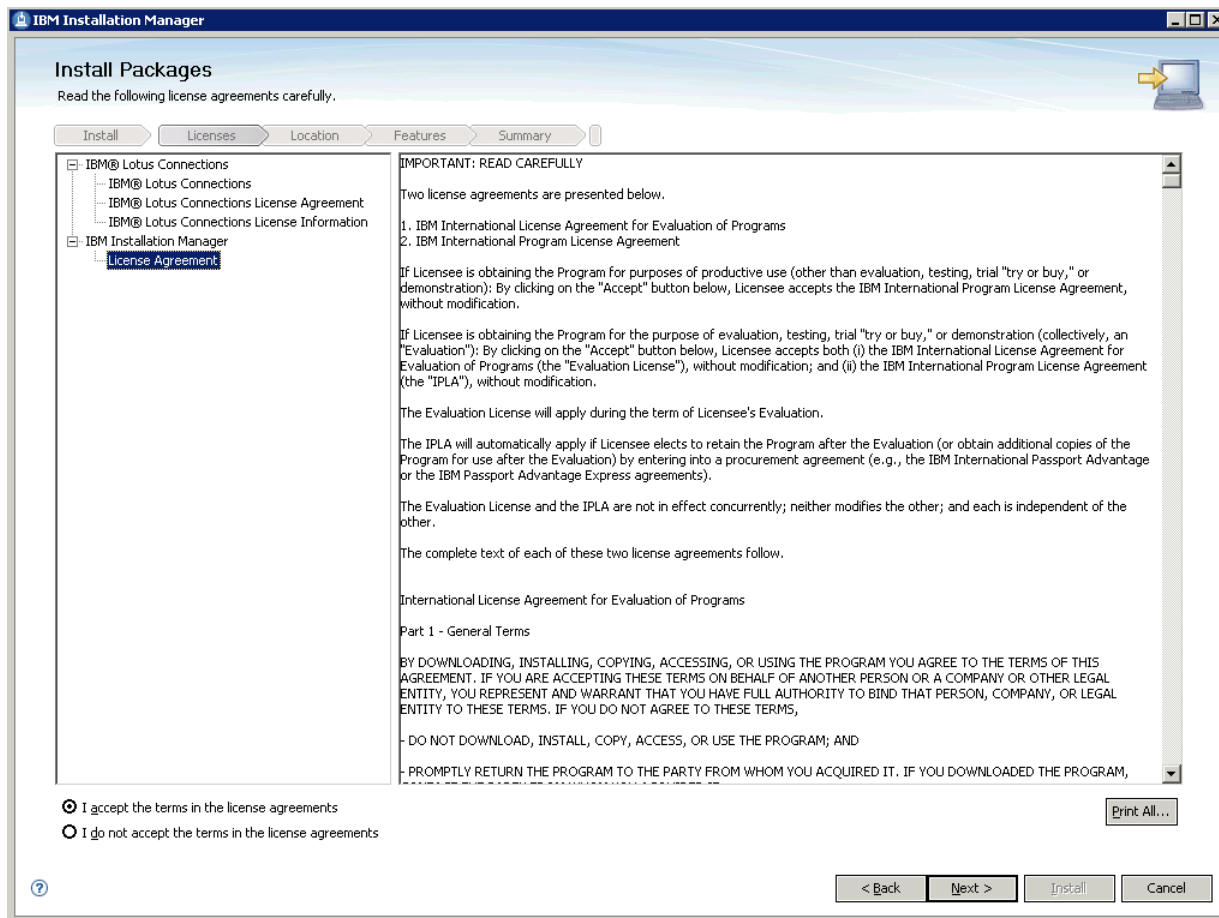
The welcome panel contains links to general documentation as well as information about pre- and post-installation tasks. Select the **Install Lotus Connections 3.0** option as shown.



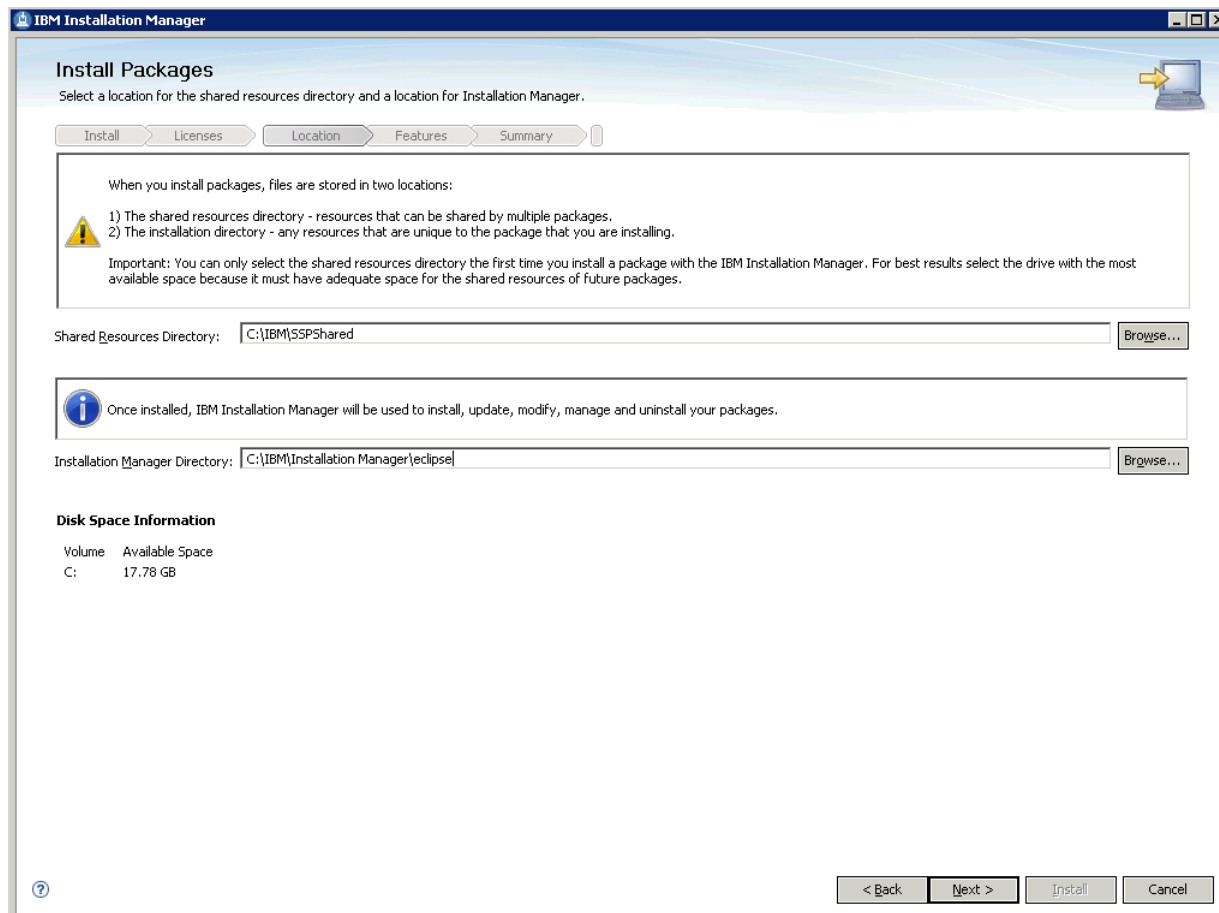
The above panel contains information about Rational Installation Manager and includes an important note about starting the Deployment Manager before beginning the installation. See the section in this article about starting and stopping Lotus Connections 3.0 to find out how to start the Deployment Manager. After the Deployment Manager is started, select the "Launch the Lotus Connections 3.0 install wizard" option shown above. The following installer panel is displayed.



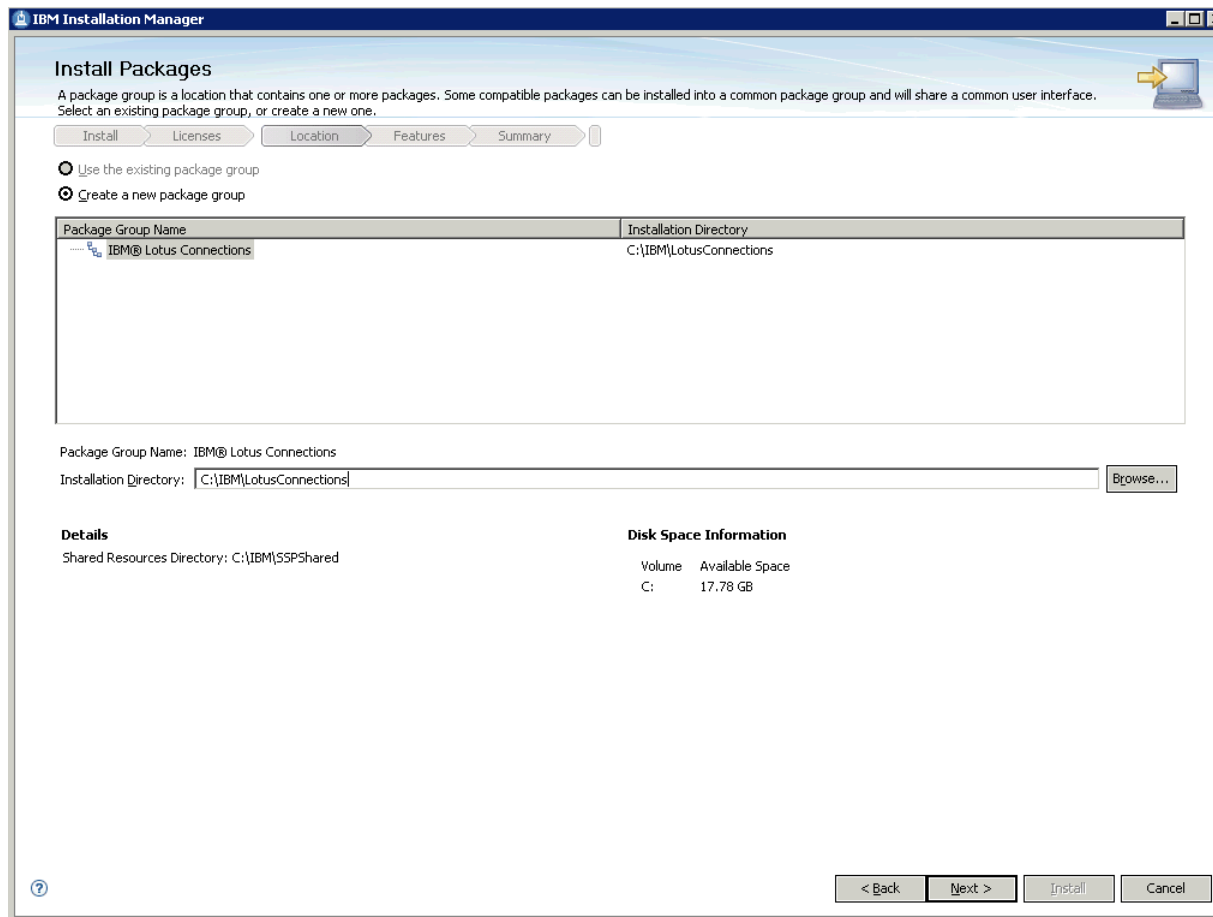
Ensure all check boxes are selected as shown in the screen shot above. To install Lotus Connections 3.0 and the correct version of Rational Install Manager, click **Next**.



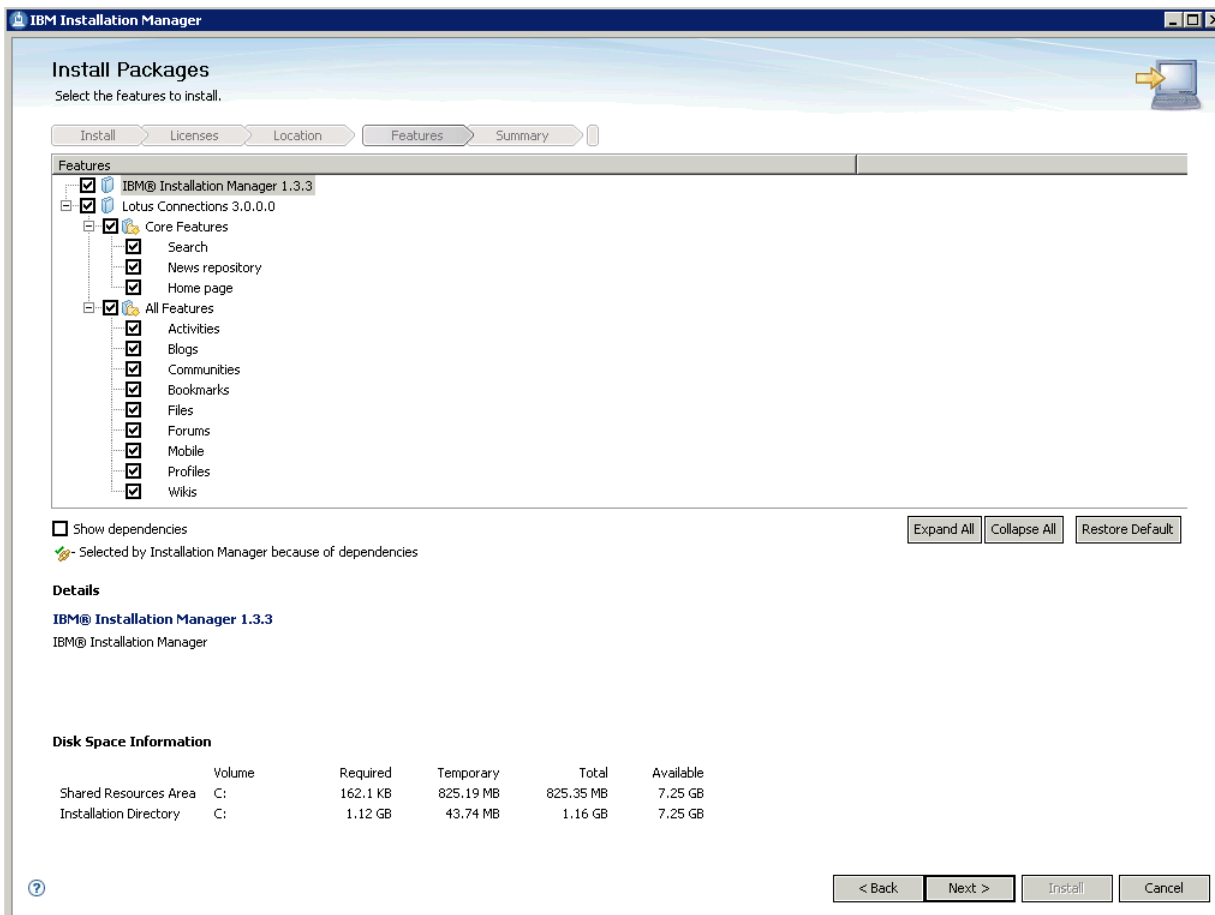
Accept the license agreement and click **Next** to continue.



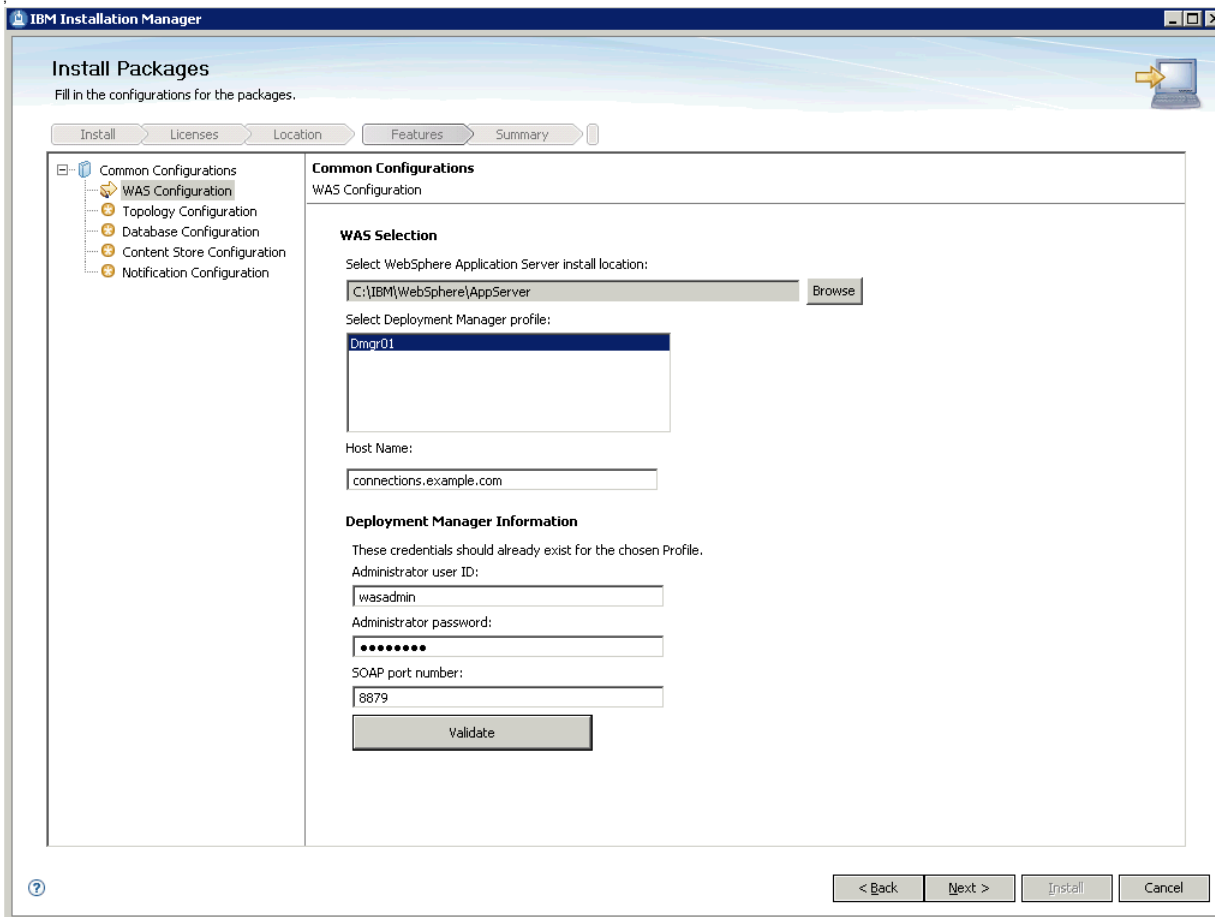
Select the location to install Rational Installation Manager and the shared resources directory. Use the above locations for ease of use. Click **Next** to continue.



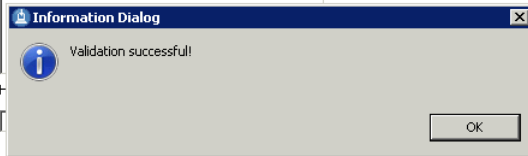
A new package group is created for Lotus Connections. Select the install directory as shown above and then click **Next** to continue.



To install all Lotus Connections components, ensure that all check boxes are selected and then click **Next** to continue.

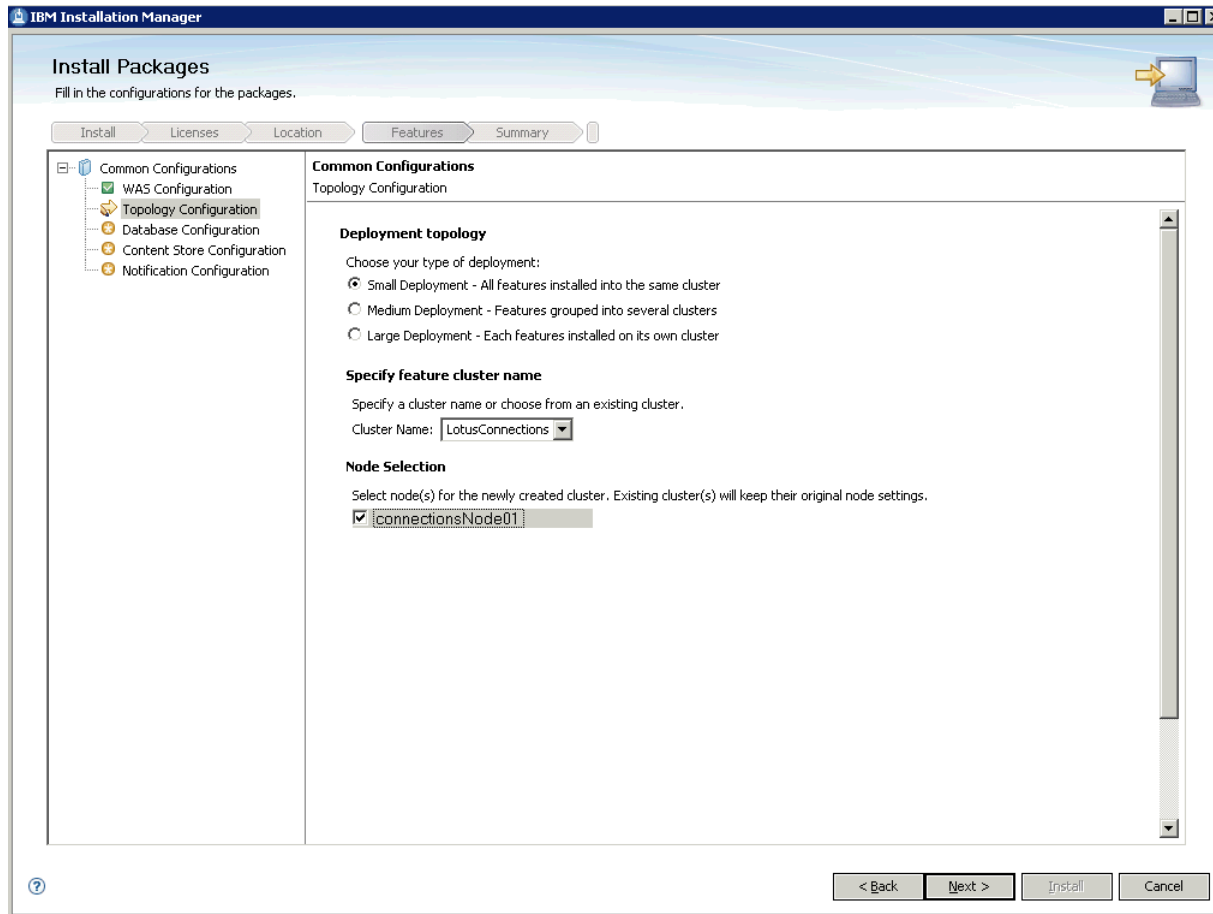


Now we need to provide the installer details of the Deployment Manager. To do so, provide the location to the Application Server as shown above. The Deployment Manager will be detected. Input the hostname, connections.example.com, and the Deployment Manager administrator and password. If your configuration is planned to be deployed with a third-party security suite, such as Tivoli Access Manager, SiteMinder or SPNEGO, it is very important that the administrative user specified be both an LDAP and a Deployment Manager administrator. Click **Validate** to verify these settings before proceeding.

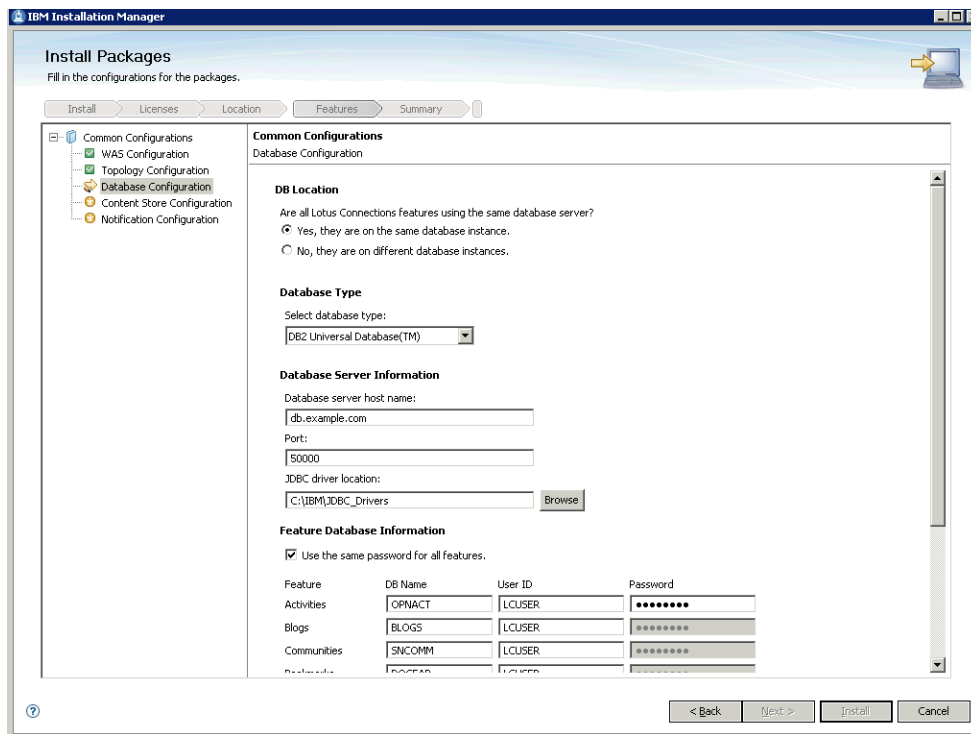


Deployment Manager Information

If all details are correct, the above validation message is displayed. Click **OK** and **Next** to continue.



Select the Small Deployment check box from the above options. This indicates that all applications will be installed into the same cluster. You must name the cluster. In the above example, the name is simply **LotusConnections**. Ensure that the node connectionsNode01 is also selected from the Node Selection section. Click **Next** to continue.



In this deployment, all features are using the same database server; therefore, select the **Yes** check box above. Set DB2 as the database type and provide the database server information as shown. Next, select the check box to use the same password for all features and supply the passwords for the databases in the appropriate fields.

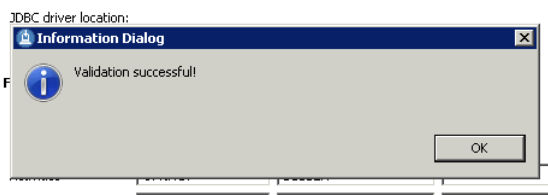
Feature Database Information

Use the same password for all features.

Feature	DB Name	User ID	Password
Activities	OPNACT	LCUSER	*****
Blogs	BLOGS	LCUSER	*****
Communities	SNCOMM	LCUSER	*****
Bookmarks	DOGEAR	LCUSER	*****
Files	FILES	LCUSER	*****
Forums	FORUM	LCUSER	*****
Homepage	HOMEPAGE	LCUSER	*****
Profiles	PEOPLEDB	LCUSER	*****
Wikis	WIKIS	LCUSER	*****

Validate

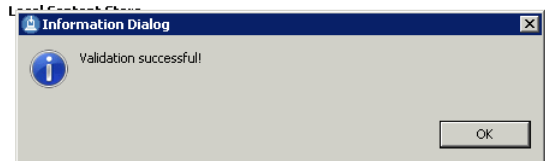
Click **Validate** to verify that the details provided are correct. The following dialog is displayed:



Click **OK** and **Next** to continue to the next panel.

The screenshot shows the 'Install Packages' window in IBM Installation Manager. The 'Location' step is active, and the 'Content Store Configuration' section is expanded. The 'Shared Content Store' field is set to 'C:\IBM\LotusConnections\data\shared', and the 'Local Content Store' field is set to 'C:\IBM\LotusConnections\data\local'. A 'Validate' button is visible below the local content store field. At the bottom of the window, there are buttons for '< Back', 'Next >', 'Install', and 'Cancel'.

Here we are providing the locations for the local and shared data stores. As this is a small deployment, both of these locations are local as shown above. Click **Validate** again to validate these locations.



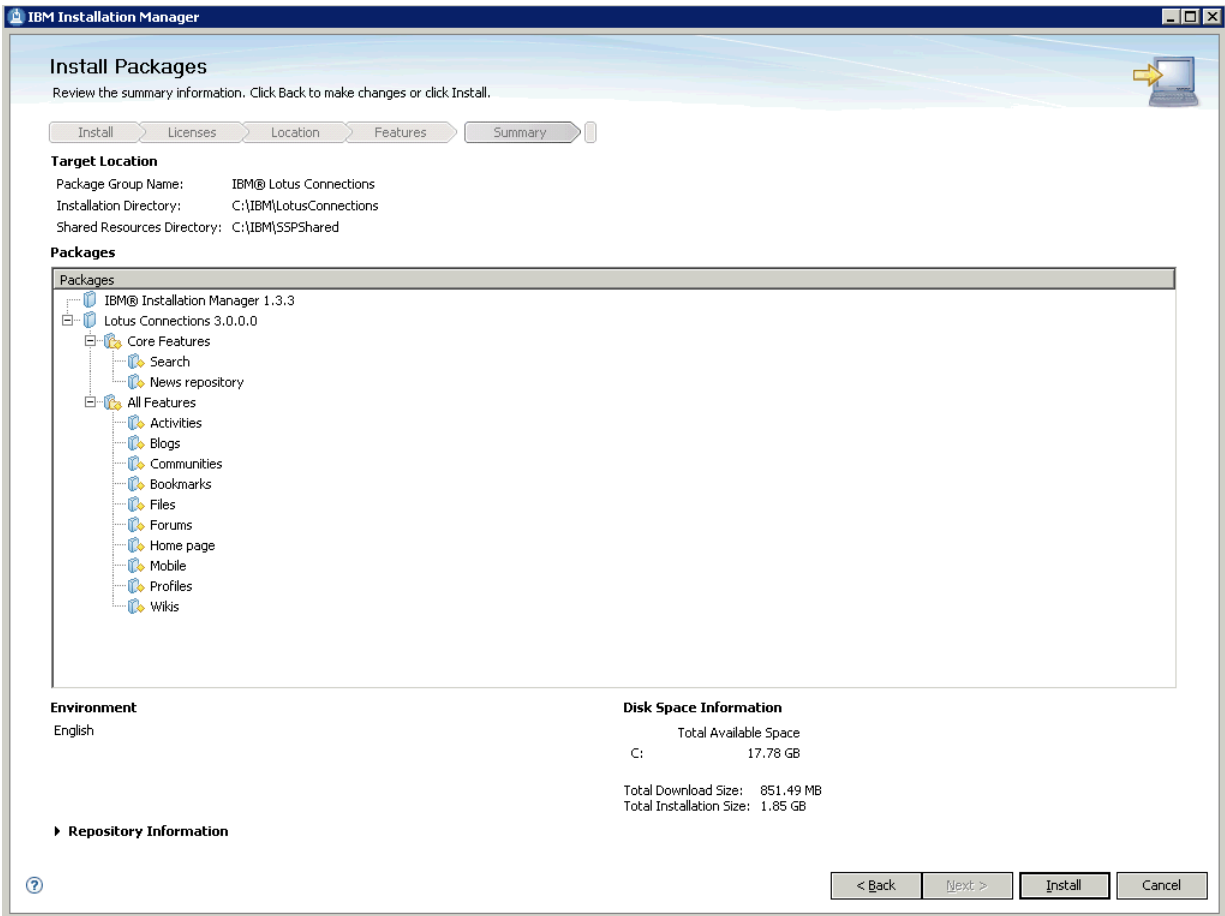
Click **OK** and **Next** to continue.

The screenshot shows the 'Install Packages' window in IBM Installation Manager. The window title is 'IBM Installation Manager'. The main heading is 'Install Packages' with a sub-heading 'Fill in the configurations for the packages.' Below this are navigation tabs: 'Install', 'Licenses', 'Location', 'Features', and 'Summary'. The 'Features' tab is active, showing a tree view on the left with 'Common Configurations' expanded to 'Notification Configuration'. The main area is titled 'Common Configurations' and 'Notification Configuration'. It contains the following sections:

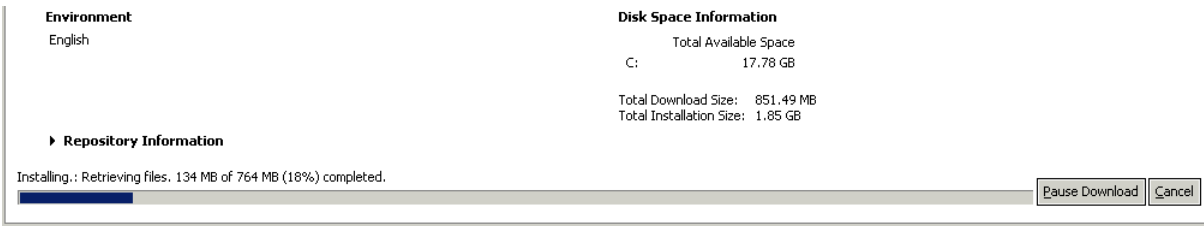
- Notification Solution**: Notification enables Lotus Connections features to send mail notifications based on key events, and allow users to send their own notification. Choose the notification solution :
 - WebSphere Java Mail Session - Use a single mail server for all notifications
 - DNS MX Records - Use information from DNS to determine which mail servers to use
 - Do not enable notification
- SMTP Server Information**: Specify the properties of the SMTP messaging server. This server is used to send outgoing mail notifications.
 - Host name of SMTP messaging server:
 - This SMTP server requires authentication:
 - User ID :
 - Password :
 - Encrypt outgoing mail traffic to the SMTP messaging server using SSL
 - Port (default for non-SSL is 25, SSL is 465) :

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

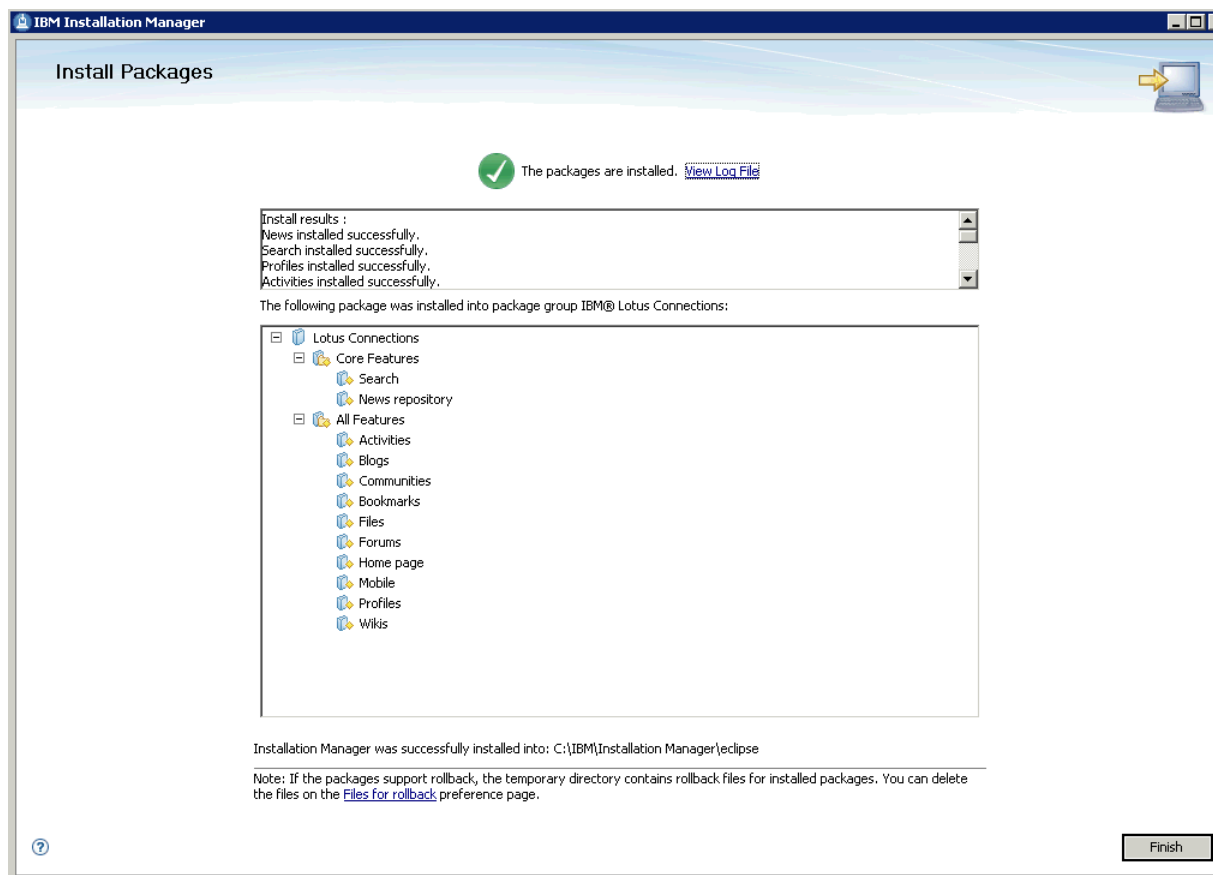
The above panel is the final panel before a summary of items to install is displayed. Provide details of your mail server. In this instance, the Java mail session is selected. Provide the location to the SMTP messaging server and the user ID required to use this server. You might also need to select the Encrypt check box if sending mail over SSL. Click **Next** to continue to the summary panel.



The above panel summarizes what is about to be installed on this system. Verify that this information is correct and click **Install** to start the installation.



The progress bar keeps you informed as to the installation's progress. After installation is completed, the following summary panel is displayed. All packages should be installed successfully as shown.



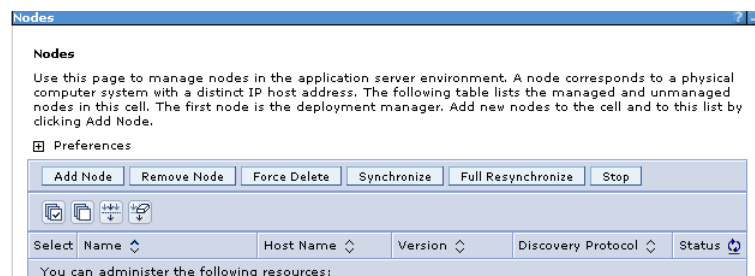
Click **Finish** to complete the installation of Lotus Connections. Note that there are a number of post installation tasks which must be performed to complete the configuration. Before beginning these tasks, you must restart the Deployment Manager for changes to take effect. After the Deployment Manager is restarted, follow these steps.

Configuring the HTTP Server

Before beginning this task, ensure that the IBM HTTP Administration server is started. The administration server must be started to synchronize configuration files between the HTTP Server and the Deployment Manager. To start the admin server on Windows, go to **Start > Programs > IBM HTTP Server V7.0 > Start Admin Server**. To start the admin server on Linux and AIX systems, use the terminal. Navigate to the HTTPServer/bin directory and issue the following command: **Jadminctl start**

Add Web Server as Unmanaged Node

After the administration server is started, open the WebSphere Administration Console and add the Web server to the cell as an unmanaged node. Open the WebSphere Administration Console at <http://connections.example.com:9060/admin>.



Go to System Administration - Nodes and click the Add Node button:

Add Node

Use this page to add either a managed or an unmanaged node.

Managed node
Specifies the creation of a managed node. A managed node contains an application server process that runs within the deployment manager cell. The managed node is associated with a node agent process that maintains the configuration for the node and controls its operation. Choosing this option results in running the add node utility to federate an existing standalone application server.

Unmanaged node
Specifies the creation of an unmanaged node. An unmanaged node represents a node in the topology that does not have an application server process or a node agent process. Unmanaged nodes are for other server processes, such as Web servers that exist on their own node in the topology.

Select the unmanaged node option and click **Next**.

Nodes

[Nodes](#) > [New](#)

Use this page to view or change the configuration for an unmanaged node. An unmanaged node is a node defined in the call topology that does not have a node agent running to manage the process. Unmanaged nodes are typically used to manage Web servers.

Configuration

General Properties

* Name
webservice

* Host Name
connections.example.com

* Platform Type
Windows

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

Additional Properties

■ Custom Properties

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

Messages

⚠ Changes have been made to your local configuration. You can:

- [Save](#) directly to the master configuration.
- [Review](#) changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

⚠ The server may need to be restarted for these changes to take effect.

Now click **Save**.

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.

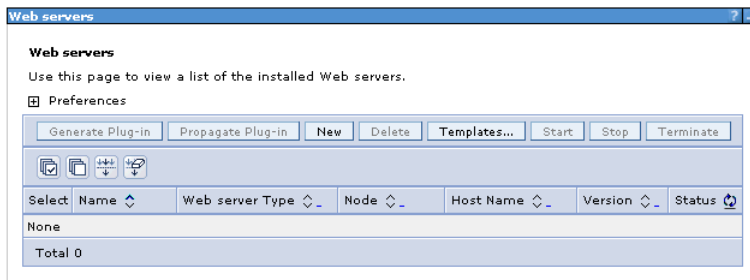
Preferences

Select	Name	Host Name	Version	Discovery Protocol	Status
	connectionsCellManager01	connections.example.com	ND 7.0.0.11	TCP	↕
<input type="checkbox"/>	connectionsNode01	connections.example.com	ND 7.0.0.11	TCP	↕
<input type="checkbox"/>	webservice	connections.example.com	Not applicable	TCP	
Total 3					

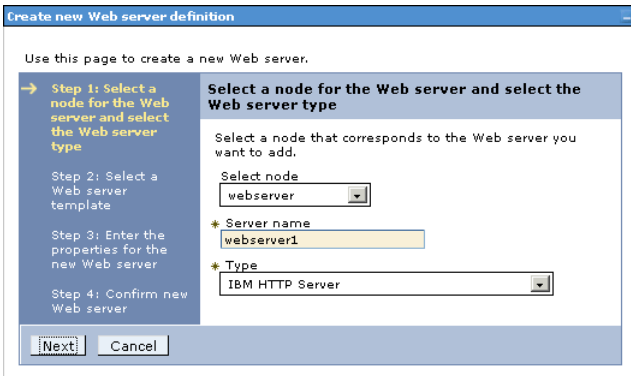
On the nodes panel, the Web server is displayed in the list above.

Add Web Server as a Server

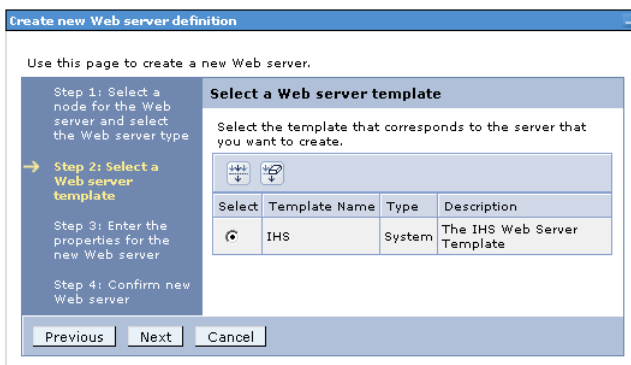
Next, add the Web server as a server in the configuration. To do so, follow these steps:



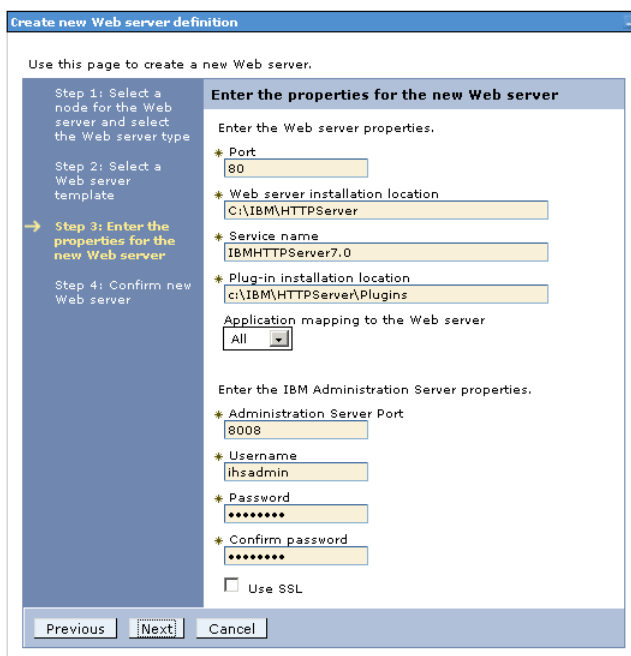
From **Servers - Server Types - Web Servers**, click the **New** button.



Select the Web server node and provide the name of this server "webservers1" - this is the same name that is provided during the plug-ins installation on the Web server. Click **Next** to continue.



The IHS option is selected. Click **Next**.



Provide all of the Web server details as indicated above and then click **Next**.

Create new Web server definition

Use this page to create a new Web server.

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

Step 2: Select a Web server template

Step 3: Enter the properties for the new Web server

→ Step 4: Confirm new Web server

Confirm new Web server

The following is a summary of your selections. Click the Finish button to complete the Web server creation. If there are settings you wish to change, click on Previous button to review the server settings.

Summary of actions:

New Web server entry "webservice1" will be created on node "webservice1"
 Platform Type "Windows"
 Web server installation root "C:\IBM\HTTPServer"
 Plug-in installation root "c:\IBM\HTTPServer\Plugins".

Previous Finish Cancel

Confirm the new Web server and click **Finish**.

Messages

New server is created successfully.

Modify variables, resources, and other server configuration settings, such as message broker queue names before running the newly created server.

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

The server may need to be restarted for these changes to take effect.

Now save this change. Before proceeding, do a full synchronize between nodes in the deployment.

Nodes

Messages

Successfully initiated synchronization of the repository on node connectionsNode01 with the deployment manager's repository.

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
	connectionsCellManager01	connections.example.com	ND 7.0.0.11	TCP	↔
<input checked="" type="checkbox"/>	connectionsNode01	connections.example.com	ND 7.0.0.11	TCP	↔
<input type="checkbox"/>	webservice	connections.example.com	Not applicable	TCP	

Total 3

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

Web servers

Messages

PLGC0005I: Plug-in configuration file = C:\IBM\WebSphere\AppServer\profiles\Dmgr02\config\cells\connectionsCell01\nodes\webservice\webservice1\plugin-cfg.xml

PLGC00052I: Plug-in configuration file generation is complete for the Web server. connectionsCell01.webservice.webservice1.

Web servers

Use this page to view a list of the installed Web servers.

Preferences

Generate Plug-in Propagate Plug-in New Delete Templates... Start Stop Terminate

Select	Name	Web server Type	Node	Host Name	Version	Status
<input type="checkbox"/>	webservice1	IBM HTTP Server	webservice	connections.example.com	Not applicable	➔

Total 1

Do this by selecting the check box besides **webserv1** and then click the **Generate Plug-in** button.

Web servers

Messages

- PLGC0062I: The plug-in configuration file is propagated from C:\IBM\WebSphere\AppServer\profiles\Dmgr02\config\cells\connectionsCell01\nodes\webservice\webserv1\plugin-cfg.xml to c:\IBM\HTTPServer\Plugins\config\webserv1\plugin-cfg.xml on the Web server computer.
- PLGC0048I: The propagation of the plug-in configuration file is complete for the Web server. connectionsCell01.webservice.webserv1.

Web servers

Use this page to view a list of the installed Web servers.

Preferences

Generate Plug-in Propagate Plug-in New Delete Templates... Start Stop Terminate

Select Name Web server Type Node Host Name Version Status

You can administer the following resources:

Select	Name	Web server Type	Node	Host Name	Version	Status
<input type="checkbox"/>	webserv1	IBM HTTP Server	webservice	connections.example.com	Not applicable	

Total 1

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

Web servers

[Web servers](#) > [webserv1](#)

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

Runtime Configuration

General Properties

Web server name: webserv1

Type: IBM HTTP Server

* Port: 80

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

* Configuration file name: \${WEB_INSTALL_ROOT}/conf/httpd.conf Edit

* Service name: IBMHTTPServer7.0

Apply OK Reset Cancel

Configuration settings

- Web Server Virtual Hosts
- Global Directives

Additional Properties

- Log file
- Configuration File
- Plug-in properties**
- Remote Web server management
- Custom properties
- Ports

Click **webserv1** and then select the Plug-in properties link as shown above.

Repository copy of Web server plug-in files:

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

Automatically generate the plug-in configuration file

Automatically propagate plug-in configuration file

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

Manage keys and certificates

Copy to Web server key store directory

From the "Repository copy of Web server plug-in files" section, click **Copy to Web server key store directory** as shown above.

Messages

- PLGC0064I: The plug-in keying file is propagated from C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\cells\connectionsCell01\nodes\webservice\webserv1\plugin-key.kdb to c:\IBM\HTTPServer\Plugins\config\webserv1\plugin-key.kdb on the Web server computer.
- PLGC0069I: The propagation of the plug-in keying is complete for the Web server. connectionsCell01.webservice.webserv1.

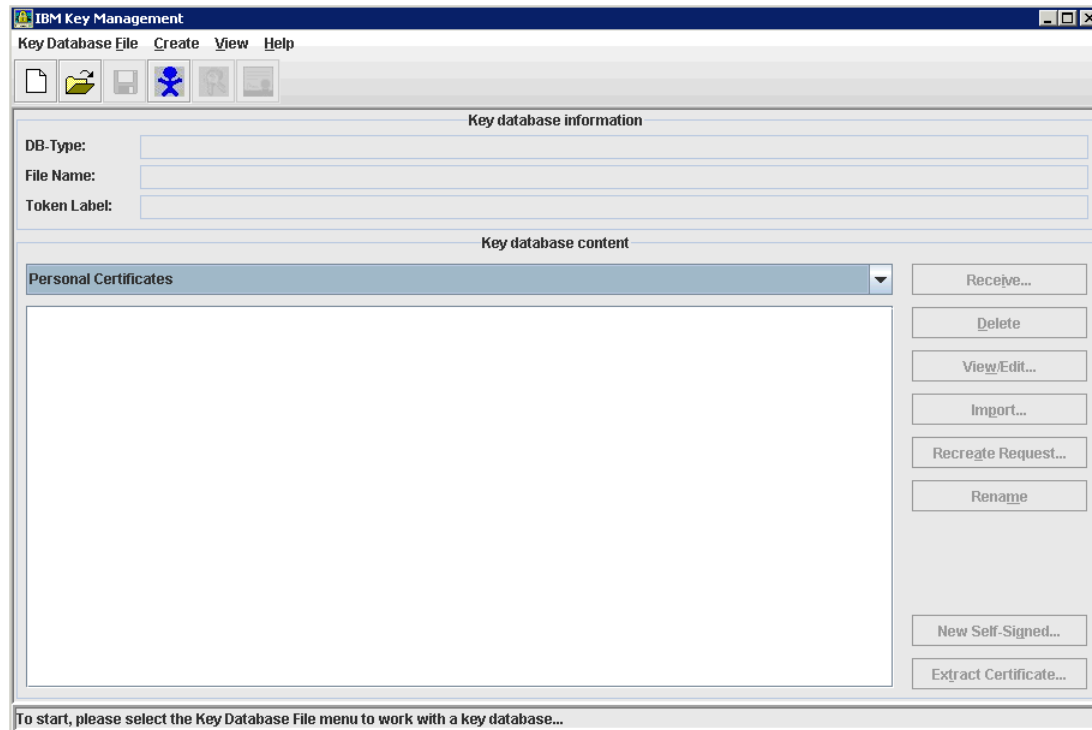
The following message is displayed, indicating the successful copying of these keys. Restart the Web server for the plug-in changes to take effect.

Configuring IBM HTTP Server for SSL

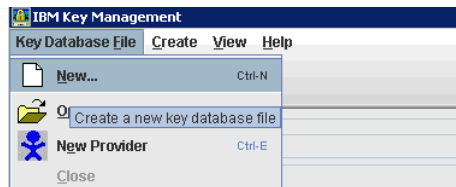
To support SSL, create a self-signed certificate and then configure IBM HTTP Server for SSL traffic. If you use this certificate in production, users might receive warning messages from their browsers. In a typical production deployment, you would use a certificate from a trusted certificate authority.

The first step is to create a key file. Start the IKEYMAN utility. To do so, double-click the ikeyman.bat file, located in C:\IBM\HTTPServer\bin (or ikeyman.sh from /opt/IBM/HTTPServer/bin on a Linux/AIX system).

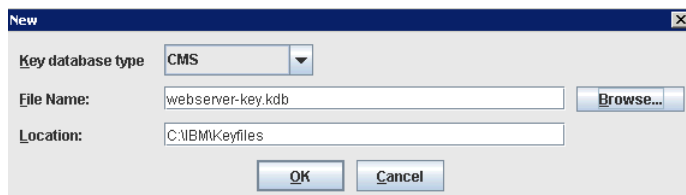
The following panel is displayed when you launch this utility.



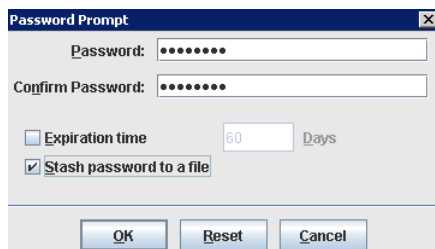
Select **Key Database File > New...**



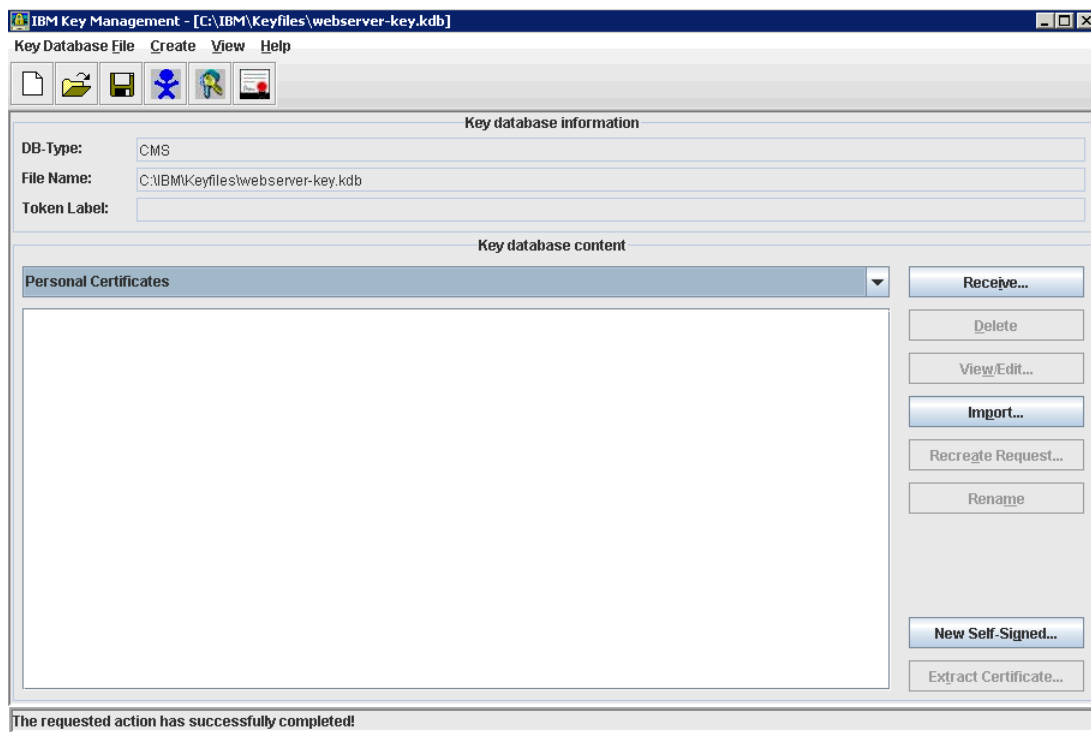
Ensure the key database type is selected as CMS. Input a name for the key file and location to store it.



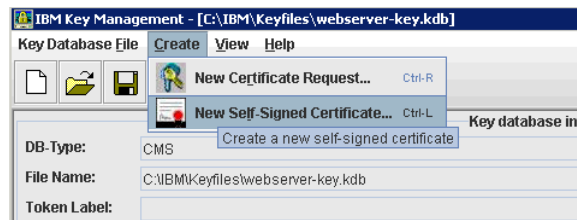
Enter a password and select the stash password to a file check box.



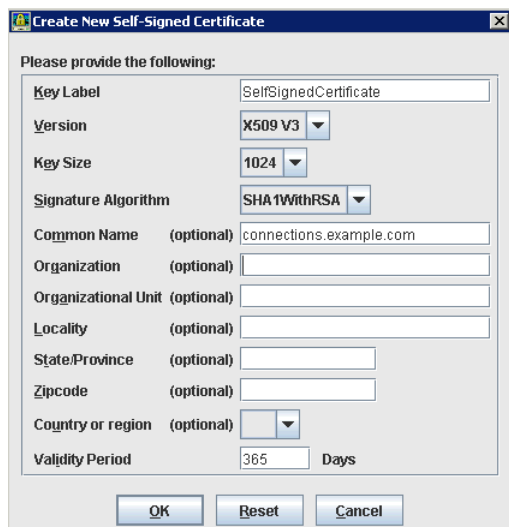
You are returned to the IKEYMAN panel with the webserver-key.kdb opened.



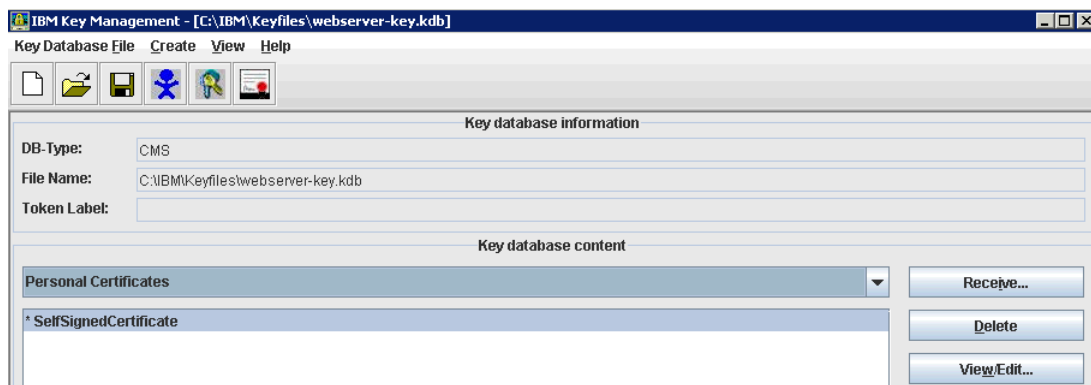
Create a self-signed certificate. To do so, select **Create > New Self-Signed Certificate...**



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

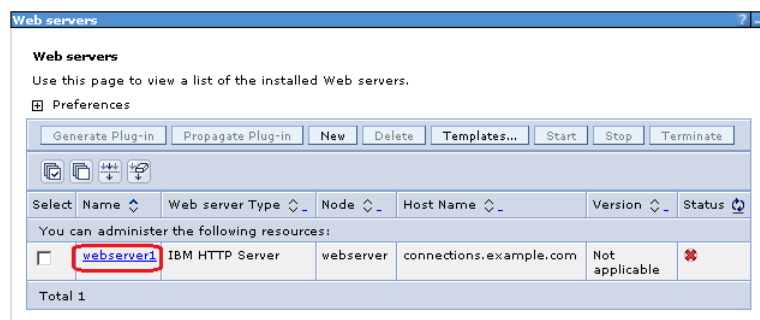


The certificate now appears in the key file as shown.



Next, stop the IBM HTTP Server, if started. After you have verified that the server is stopped, log in to the WebSphere Administration Console and configure the Web server for SSL.

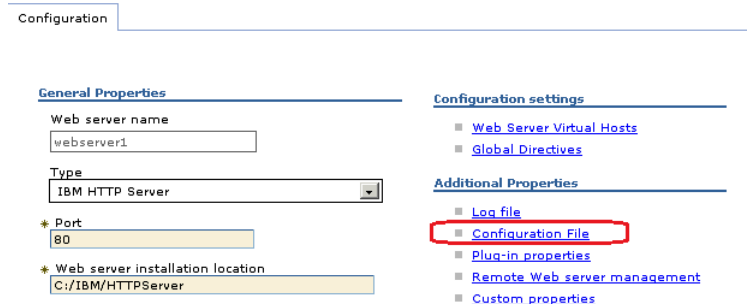
From the Web servers panel, select the **webserver1** link.



Click the Configuration File link to open the httpd.conf from the WebSphere Administration Console.

[Web servers](#) > **webserver1**

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



The httpd.conf opens in the browser as shown.

[Web servers](#) > [webserver1](#) > `${WEB_INSTALL_ROOT}/conf/httpd.conf`

Use this page to view or modify the contents of the Web server configuration file.



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

```
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
```

```
</VirtualHost>
```

```
</IfModule>
```

```
SSLDisable
```

```
Keyfile "C:\IBM\Keyfiles\webserver-key.kdb"
```

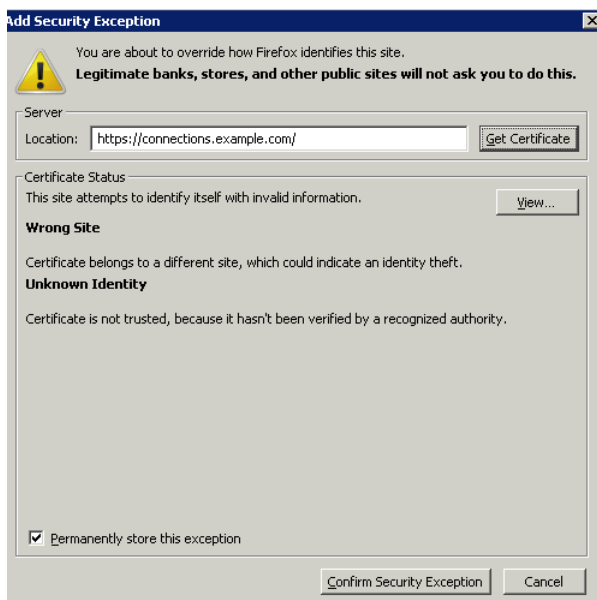
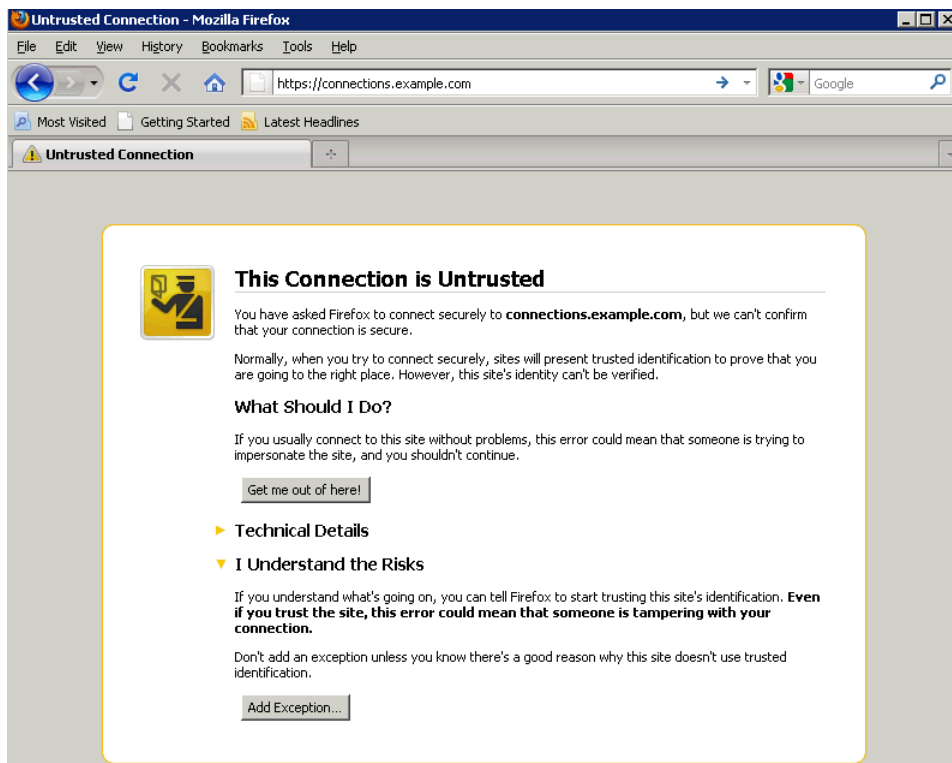
```
SSLStashFile "C:\IBM\Keyfiles\webserver-key.sth"
```

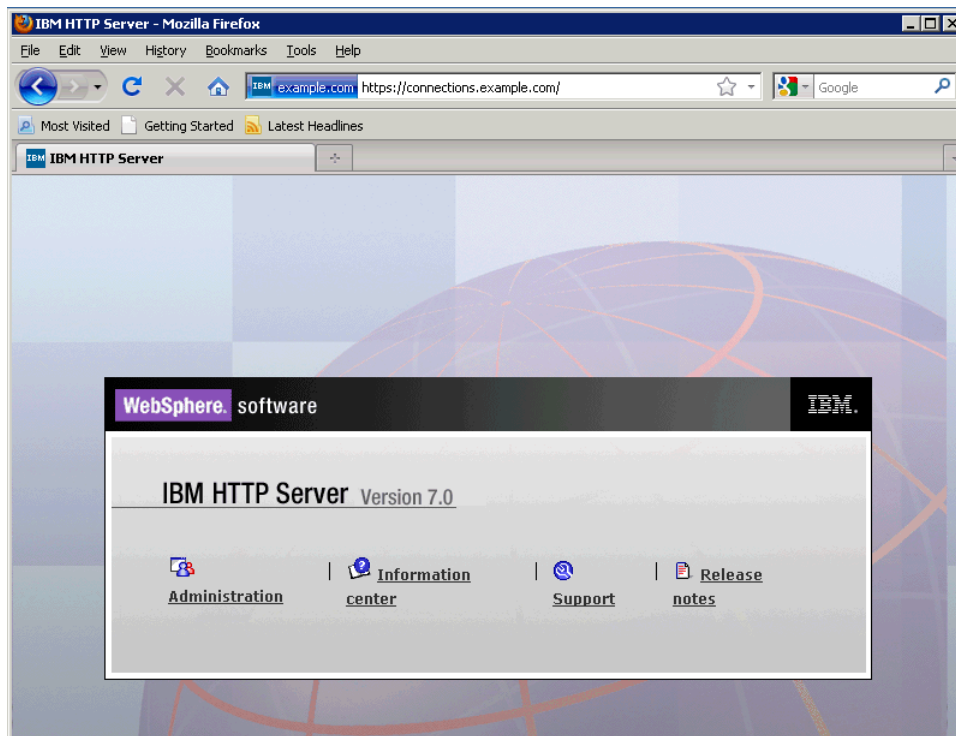
Scroll to the bottom of the configuration file. At the end of the httpd.conf, add the above lines to load the SSL module using the key file we just created.

Click **OK** to save this change.

```
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
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "C:\IBM\Keyfiles\webserver-key.kdb"
SSLStashFile "C:\IBM\Keyfiles\webserver-key.sth"
```

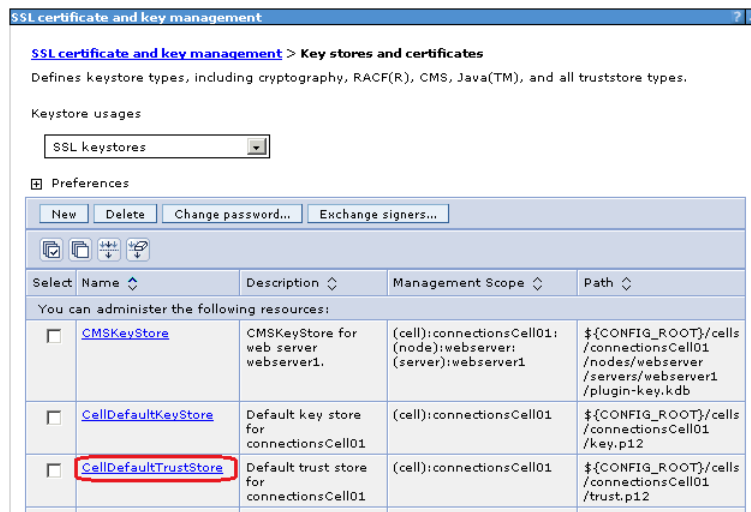
Start the IBM HTTP Server. To verify that the SSL settings took effect correctly, enter <https://connections.example.com> in a browser. If the IBM HTTP Server page appears over https, this step was successful. Note that you might need to accept the certificate to your browser as it is not signed.



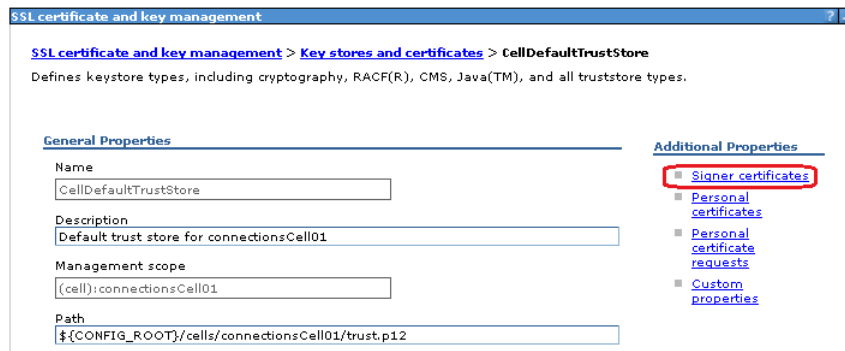


Adding Certificates to the WebSphere Trust Store

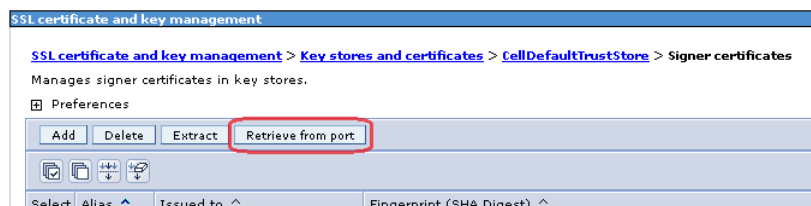
From the WebSphere Administration Console, go to **Security > SSL Certificate and Key Management**. Next, click the **CellDefaultTrustStore** link as shown.



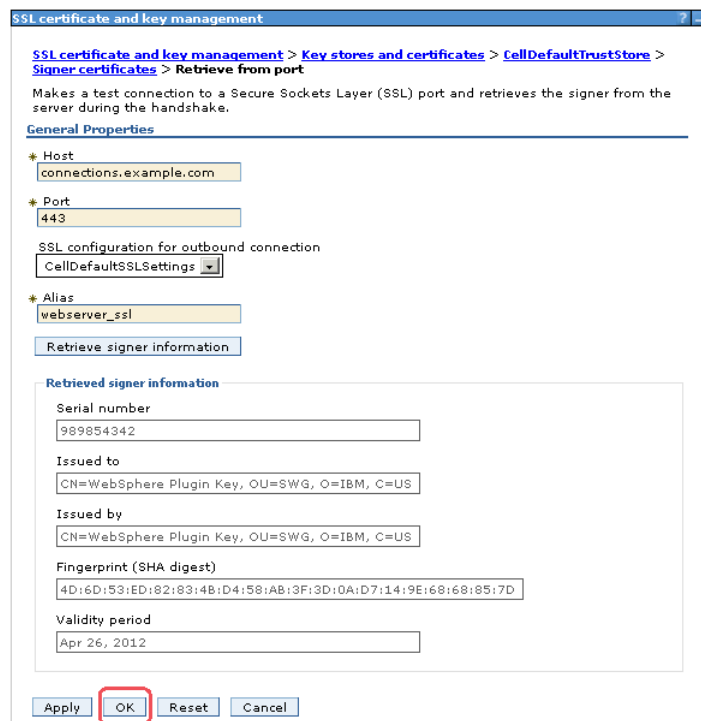
From within **CellDefaultTrustStore**, click the **Signer certificates** link in the right hand pane.



Add the webservers signer to the trust store by clicking the **Retrieve from port** button.



Specify the host name of the Web server and its SSL port (typically 443). Then click the **Retrieve Signer Information** button, which retrieves the information shown on the bottom of this screen shot. Provide an alias for this signer certificate and click **OK** to add this certificate to the list of signers.



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

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, update all href and ssl_href values to reflect the host name of the HTTP Server. Do not include any port numbers.

An example of this follows :

```
<slc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections"
  <slc:href>
    <slc:hrefPathPrefix>/activities</slc:hrefPathPrefix>
    <slc:static href="http://connections.example.com:9081" ssl_href="https://connections.example.com:9444"/>
    <slc:interService href="https://connections.example.com:9444"/>
  </slc:href>
</slc:serviceReference>
```

Convert the original values below of the hrefs ssl_hrefs from their default values above to their new values, in this case all that is done is to drop the port numbers 9081 and 9044 from these urls.

```
<slc:serviceReference bootstrapHost="connections.example.com" bootstrapPort="2811" clusterName="LotusConnections"
  <slc:href>
    <slc:hrefPathPrefix>/activities</slc:hrefPathPrefix>
    <slc:static href="http://connections.example.com" ssl_href="https://connections.example.com"/>
    <slc:interService href="https://connections.example.com"/>
  </slc:href>
</slc:serviceReference>
```

Repeat this process for all href and ssl_hrefs that are currently set to connections.example.com. After this process is complete, save the file and check it back in using the wsadmin client. After the file is checked in, resynchronize the node so that this change is pushed out.

This completes the Web server, SSL, and certificate configuration for this scenario. Now when the application is started, it can be accessed at <http://connections.example.com><component where <component represents any of the Connection's applications.

The commands to perform the above tasks are shown below (the above updates take place after the check out command).

```

Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\bin
The system cannot find the path specified.

C:\Users\Administrator>cd C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>wsadmin -lang jython -username
e wasadmin -password wasadmin -port 8879
WASX7209I: Connected to process "dmgr" on node connectionsCellManager01 using SOAP
connector; The type of process is: DeploymentManager
WASX7031I: For help, enter: "print Help.help()"
wsadmin>execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin
\connectionsConfig.py")
Connections Administration initialized

wsadmin>LCConfigService.checkOutConfig("C:/temp","connectionsCell01")
Connections configuration file successfully checked out
wsadmin>
wsadmin>LCConfigService.checkInConfig()
Using configuration arguments :
  workingDirectory: C:/temp
  cellName: connectionsCell01
  nodeName: None
  serverName: None
Loading schema file for validation: /C:/temp/LotusConnections-config.xsd
Loading schema file for validation: /C:/temp/service-location.xsd
C:/temp/LotusConnections-config.xml is valid
Connections configuration file successfully checked in
wsadmin>
wsadmin>synchAllNodes()
Nodes synchronized
wsadmin>exit

C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin>_

```

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 wasadmin -password wasadmin -port 8879

2: execfile("C:\IBM\WebSphere\AppServer\profiles\Dmgr01\config\bin_lc_admin\connectionsConfig.py")

3: LCConfigService.checkOutConfig("C:/temp","connectionsCell01")

<Make changes to the checked out file>

4: LCConfigService.checkInConfig()

5: synchAllNodes()

Configuring Application Administrators and Configuring Blogs

After Lotus Connections 3.0 is installed, it is necessary to configure the blogs landing page. There are two steps involved::

1. Assigning administrative access to a blogs user.
2. Creating the blogs home page.

You may also want to give administrative access to particular users for other applications, such as home page, so that widgets can be enabled/disabled and determine who can read server metrics & statistics. The below example shows how to add an administrator to the blogs application. The same process is followed to add administrators to the other applications.

Before beginning this task, ensure to start Lotus Connections. For instructions, refer to the section in this article about starting and stopping Lotus Connections 3.0. After the deployment is started, verify that you can log in successfully to all components. It is a good idea to check the logs to ensure there are no errors occurring during the startup and verification.

Adding an Administrator to Blogs

1. Log in to the WebSphere Administration Console on connections.example.com at the url <http://connections.example.com:9060/admin>.
2. Go to **Applications - Application Types Web - WebSphere Enterprise Applications** and click the Blogs link.

Enterprise Applications

Enterprise Applications
Use this page to manage installed applications. A single application can be deployed onto multiple servers.

Preferences

Start Stop Install Uninstall Update Rollout Update Remove File Export Export DDL Export File

Select Name Application Status

You can administer the following resources:

Select	Name	Application Status
<input type="checkbox"/>	Activities	+
<input type="checkbox"/>	Blogs	+
<input type="checkbox"/>	Communities	+

From the list of options for this application select "Security role to user/group mapping" as shown.

Enterprise Applications > Blogs

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

Configuration Runtime

General Properties

Name: Blogs

Application reference validation: Issue warnings

Detail Properties

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

Modules

- Manage Modules

Web Module Properties

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

Enterprise Java Bean Properties

- Default messaging provider references
- Stateful session bean failover settings
- Application profiles
- Message Driven Bean listener bindings
- EJB JNDI names

From the following panel, it is possible to map users and groups to different roles. In the below example there is no user assigned as admin. Click the check box beside admin and then click **Map Users...**

Enterprise Applications

Enterprise Applications > Blogs > Security role to user/group mapping

Security role to user/group mapping

Each role that is defined in the application or module must map to a user or group from the domain user registry. accessIds: The accessIds are required only when using cross realm communication in a multi domain scenario. For all other scenarios the accessId will be determined during the application start based on the user or group name. The accessIds represent the user and group information that is used for Java Platform, Enterprise Edition authorization when using the WebSphere default authorization engine. The format for the accessIds is user:realm/uniqueUserID, group:realm/uniqueGroupID. Entering wrong information in these fields will cause authorization to fail. AllAuthenticatedInTrustedRealms: This indicates that any valid user in the trusted realms be given the access. AllAuthenticated: This indicates that any valid user in the current realm be given the access.

Map Users... Map Groups... Map Special Subjects

Select	Role	Special subjects	Mapped users	Mapped groups
<input type="checkbox"/>	person	All Authenticated in Application's Realm		
<input type="checkbox"/>	everyone	Everyone		
<input type="checkbox"/>	metrics-reader	Everyone		
<input checked="" type="checkbox"/>	admin	None		
<input type="checkbox"/>	global-moderator	None		
<input type="checkbox"/>	search-admin	None	wasadmin	
<input type="checkbox"/>	widget-admin	None	wasadmin	
<input type="checkbox"/>	reader	Everyone		

OK Cancel

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

Enterprise Applications

Enterprise Applications > Blogs > Security role to user/group mapping > Map users/groups

Use this page to search for users or groups and add them to the selected roles.

- admin

Search and Select Users

Select a user realm, specify the number of results to display, enter a search string (use * for wildcard) and click Search. Select users from the Available list and add them to the Mapped to role list.

User realm
ldap.example.com

Display a maximum of
20 results

Search string
jcollins

Search

Available: jcollins Selected:

Click the **OK** button below to return to the user - role mapping panel.

Available: Selected: jcollins

OK Cancel

The user 'jcollins' is assigned as an administrator in Blogs. Click **OK** to save this change.

Enterprise Applications

Enterprise Applications > Blogs > Security role to user/group mapping

Security role to user/group mapping

Each role that is defined in the application or module must map to a user or group from the domain user registry. accessIds: The accessIds are required only when using cross realm communication in a multi domain scenario. For all other scenarios the accessId will be determined during the application start based on the user or group name. The accessIds represent the user and group information that is used for Java Platform, Enterprise Edition authorization when using the WebSphere default authorization engine. The format for the accessIds is user:realm/uniqueUserID, group:realm/uniqueGroupID. Entering wrong information in these fields will cause authorization to fail. AllAuthenticatedInTrustedRealms: This indicates that any valid user in the trusted realms be given the access. AllAuthenticated: This indicates that any valid user in the current realm be given the access.

Map Users... Map Groups... Map Special Subjects

Select	Role	Special subjects	Mapped users	Mapped groups
<input type="checkbox"/>	person	All Authenticated in Application's Realm		
<input type="checkbox"/>	everyone	Everyone		
<input type="checkbox"/>	metrics-reader	Everyone		
<input type="checkbox"/>	admin	None	jcollins	
<input type="checkbox"/>	global-moderator	None		
<input type="checkbox"/>	search-admin	None	wasadmin	
<input type="checkbox"/>	widget-admin	None	wasadmin	
<input type="checkbox"/>	reader	Everyone		

OK Cancel

To save the change, click **Save** as follows:

Messages

Changes have been made to your local configuration. You can:

- Save directly to the master configuration.
- Review changes before saving or discarding.

An option to synchronize the configuration across multiple nodes after saving can be enabled in [Preferences](#).

The server may need to be restarted for these changes to take effect.

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

Creating the Blogs Homepage

Log in to Blogs as the newly-assigned administrator.

Lotus Connections Home Profiles Communities Apps Jodie Collins Settings

My Blogs Public Blogs My Updates Administration

Welcome to Blogs!

Follow these steps to finalize your Blogs installation:

- Create a blog**

Before you can start blogging, you need to create at least one blog. Just so you know, you can create as many as you want. Each user can have multiple blogs and each blog can have multiple authors.

Create your first blog via the [New Blog Creation Page](#)
- Designate a frontpage blog**

You must specify a blog to serve as the frontpage of your site. You can do this by going to the **Administration->Configuration** page. In the field labeled "Handle of the blog to serve as the frontpage" enter a one word name for your blog to be used in the URL for the blog.

Designate a frontpage blog on the [Administration Page](#)

Home Demo Help IBM Lotus Support Forums How to Bookmark Server Metrics About IBM Lotus Connections on ibm.com Submit Feedback

On the top of the page, there is now an Administration tab. Click the "New Blog Creation Page" link to create the new blog homepage.

My Blogs Public Blogs My Updates Administration

Start a Blog

*Name: BlogHomepage ?


*Blog address: https://connections.example.com/blogs/home ?

Tags: bloghomepage ?

Description: This is the blogs frontpage ?

Timezone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

Theme: Blogs Homepage ?



Save Cancel

On the page above, take note of the blog address (in this case 'home'). Also ensure that Theme is set to Blogs Homepage. Click **Save** to create the blog.

✔ New blog [BlogHomepage] has been successfully created.

My Blog

Start a Blog

BlogHomepage

Jodie Collins

[New Entry](#) | [Entries](#) | [Settings](#) | [\[Set as Primary Blog\]](#)

The above message is displayed. Click the Administration tab as shown.

My Blogs Public Blogs My Updates Administration

Configuration

Change configuration settings for the entire site. Changes are made as soon as you save; no server restart is required.

Site Settings

Site name (for Blogs Homepage and feed): Blogs

Blog title (shown in site banner): Blogs

Site description (for Blogs Homepage and feed):

Short name from blog address to serve as Blogs Homepage blog: home

Enable active content filtering:

Automatic save when editing (minutes): 15

Enter the blog URL (home), in the above field. Click **Save** to make this change.

✔ Change saved.

After the change is successful, log out of Blogs.

Now, if you navigate to `connections.example.com/blogs`, the above page is displayed.

Linux & AIX only : Setting Path Variables for Search

Starting and Stopping Lotus Connections 3.0

To completely start or stop the system, follow this process. It is assumed that LDAP is active throughout.

WebSphere Application Server

To start/stop these services, use the command prompt or shell in Linux. From the command prompt, issue the following commands:

Start:
 C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\startManager.bat
 C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\startNode.bat

Stop:
 C:\IBM\WebSphere\AppServer\profiles\Dmgr01\bin\stopManager.bat -username wasadmin -password wasadmin
 C:\IBM\WebSphere\AppServer\profiles\AppSrv01\bin\stopNode.bat -username wasadmin -password wasadmin

WebServer

Ensure the IHS administrator server is started. To do so, click **Start - All Programs - IBM HTTP Server V7.0 - Start Admin Server**.

From the WebSphere Administration Console, select **Servers - Server Types - Web Servers**. Select the check box beside `webserver1` and click **Start** or **Stop** as required.

Select	Name	Web server Type	Node	Host Name	Version	Status
<input checked="" type="checkbox"/>	webserver1	IBM HTTP Server	webserver	connections.example.com	Not applicable	➔

Database

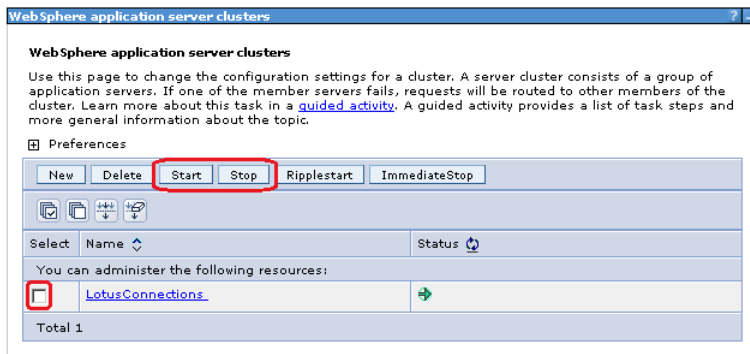
To start/stop these services use the command prompt or shell in Linux. From the command prompt, issue the following commands:

Set the instance to the correct name using this command:
 SET DB2INSTANCE=DB2

Use either of the below commands to start or stop DB2
 DB2START
 DB2STOP

Lotus Connections

From the WebSphere Administration Console, select **Servers - Clusters - WebSphere Application Server Clusters**. Select the check box beside `LotusConnections` and click **Start** or **Stop** as required.



After the cluster is started, verify that there are no problems by viewing the logs at C:\IBM\WebSphere\profiles\AppSrv01\logs\LotusConnections_server1\SystemOut.log.

Tuning and Optimizing Lotus Connections 3.0

This section contains information on how to tune the server heap size. As this guide is intended for a small deployment which may be used for a test deployment no other tuning is included in this section. If you need more information on basic tuning please see the tuning section of the scenario 2 article. There are many more possible tweaks and modifications that can be made on WebSphere Application Server to tune the configuration for optimal performance depending on your requirements. For further information, consult the Lotus Connections 3.0 tuning articles available on the Lotus Connections Wiki.

Tuning the JVM Heap Sizes

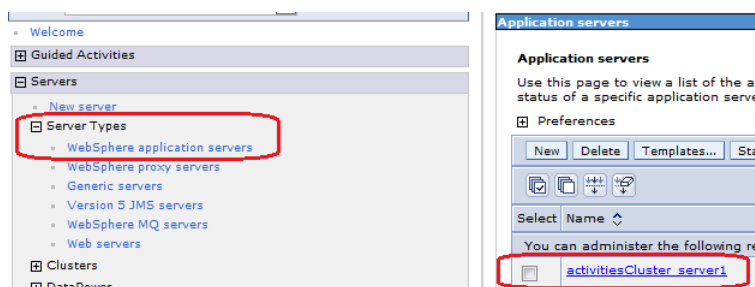
The JVM heap size on a small deployment is set by default to the below values:

Applications	Servers	Initial Heap Size (Mb)	Maximum Heap Size (Mb)
All	LotusConnectionsCluster_server1	512	2560

Follow this guide to tune the heap size as required. When increasing the heap size, it is a good idea to monitor overall memory consumption to ensure that your system can provide the necessary memory allocations without excessive paging.

In this scenario, the machine hosting the Deployment Manager, Application Server, and Web server has 8 GB RAM. When increasing the max heap size, ensure that you do not allocate more memory than the physical capacity of the system.

The following screen shots show how to set the maximum heap size for a server named 'activitiesCluster_server1'. Apply this process for the LotusConnectionsCluster_server1 server, which was created in this scenario. Open the Deployment Manager and navigate to **Server Types > WebSphere application servers**. Click the link for the server you want to modify (LotusConnectionsCluster_server1).



Locate the Server Infrastructure section and click **Process definition**.



Click the Java Virtual Machine link as shown.

[Application servers](#) > [activitiesCluster_server1](#) > **Process definition**

Use this page to configure a process definition. A process definition defines the command line information necessary to start or initialize a process.

Configuration

General Properties	Additional Properties
Executable name <input type="text"/>	<ul style="list-style-type: none"> • Java Virtual Machine • Environment Entries • Process execution • Process Logs • Logging and tracing
Executable arguments <input type="text"/>	

Enter the initial heap and maximum heap size for this server as per your requirements.

[Application servers](#) > [activitiesCluster_server1](#) > [Process definition](#) > **Java Virtual Machine**

Use this page to configure advanced Java(TM) virtual machine settings.

Configuration **Runtime**

General Properties

Classpath

Boot Classpath

Verbose class loading

Verbose garbage collection

Verbose JNI

Initial heap size
 MB

Maximum heap size
 MB

Click **OK** and **Save** this change.

About the Authors

Colm O'Brien is a member of the Lotus Connections System Verification Test (SVT) specialising in the area of product deployment and reliability/workload testing.

Roberto Boccadoro is a Collaborative solutions Architect in the Lotus Client Technical Professionals team.

Elena Sangalli is an IT Specialist in the Lotus Client Technical Professionals team.

▼ Article information

Category: [Deployment Scenarios](#)

Tags: [3](#), [deploying](#), [3_deployment](#), [scenarios](#), [test_infrastructure](#)

This Version: Version 18 July 26, 2011 2:27:31 PM by Michelle Mahoney 

► Attachments (1)**► Versions (18)**