

Configure user repository and enable security for WebSphere® Application Server and WebSphere Partner Gateway

What this exercise is about	2
What you should be able to do	2
Exercise Instructions	2
Part 1: Configure Tivoli Directory Server user repository with WebSphere Partner Gateway users	4
Part 2: Enable LDAP security for WebSphere Application Server V6.1	8
Part 3: Logging into WebSphere Partner Gateway community console.....	14
Part 4: Create participants & users	15
Part 5: Enable LDAP container based authentication for WebSphere Partner Gateway console.....	19
Part 6: Map WebSphere Partner Gateway user roles	20
Part 7: Logging into community console with LDAP authentication enabled.....	23
Part 8: Disable LDAP based authentication	25
What you did in this exercise	27

What this exercise is about

The objective of this lab is to provide step by step instructions for installing and configuring IBM Tivoli Directory Server (LDAP).

List of software required for the student to complete the lab:

- WebSphere Application Server V6.1 Network Deployment Installed
- WebSphere Partner Gateway Server V6.1 Installed
- IBM DB2[®] UDB ESE 8.2 or higher installed
- IBM Tivoli[®] Directory Server V6.0

What you should be able to do

At the end of this lab you should be able to:

- Configure users in the Tivoli Directory Server (LDAP) server and configure security for WebSphere Application Server and WebSphere Partner Gateway Components

Exercise instructions

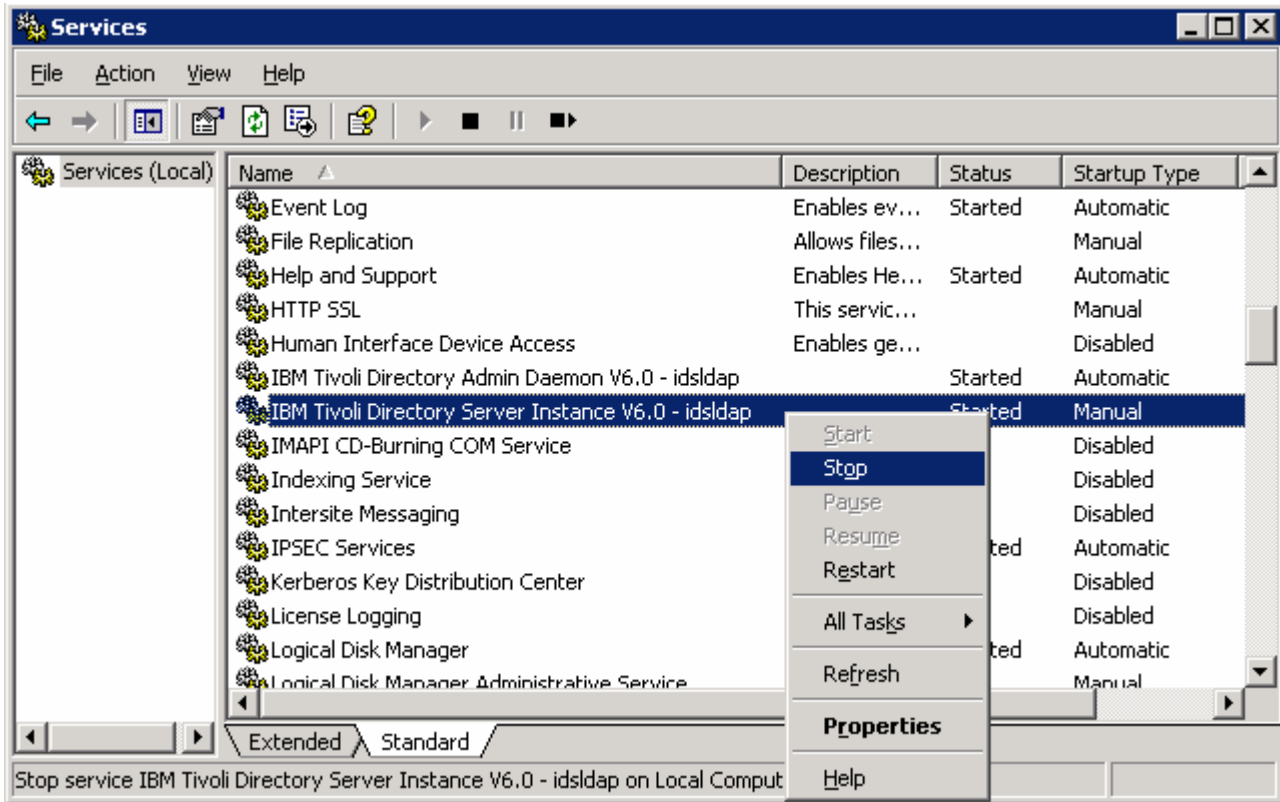
Some instructions in this lab may be Windows[®] operating-system specific. If you plan on running the lab on an operating-system other than Windows, you will need to run the appropriate commands, and use appropriate files (.sh vs. .bat) for your operating system. The directory locations are specified in the lab instructions using symbolic references, as follows:

Reference Variable	Windows Location	Linux® Location
<DB2_HOME>	C:\IBM\SQLLIB	/opt/IBM/SQLLIB
<WPG_HOME>	C:\IBM\WPG61	/opt/IBM/WPG61
<WPG_HUB_SIMPLE_HOME>	C:\IBM\WPG61\wpghubsimple	/opt/IBM/WPG61/wpghubsimple
<WPG_HUB_DISTR_HOME>	C:\IBM\WPG61\wpghubappsprofile	/opt/IBM/WPG61/wpghubappsprofile
<WPG_APPSDB_HOME>	C:\IBM\WPG61\wpgappsdb	/opt/IBM/WPG61/wpgappsdb
<WPG_MASDB_HOME>	C:\IBM\WPG61\wpgmasdb	/opt/IBM/WPG61/wpgmasdb
<WAS_HOME>	C:\IBM\WAS61	/opt/IBM/WAS61
<LDAP_INSTALL_IMAGES>	C:\download\LDAP60\unzip	/opt/download/LDAP60/unzip
<LAB_FILES>	C:\WPG61\Labfiles	/tmp/WPG61\Labfiles
<TEMP>	C:\temp	/tmp

Windows users' note: When directory locations are passed as parameters to a Java™ program such as EJB™ deploy or wsadmin, it is necessary to replace the backslashes with forward slashes to follow the Java convention.

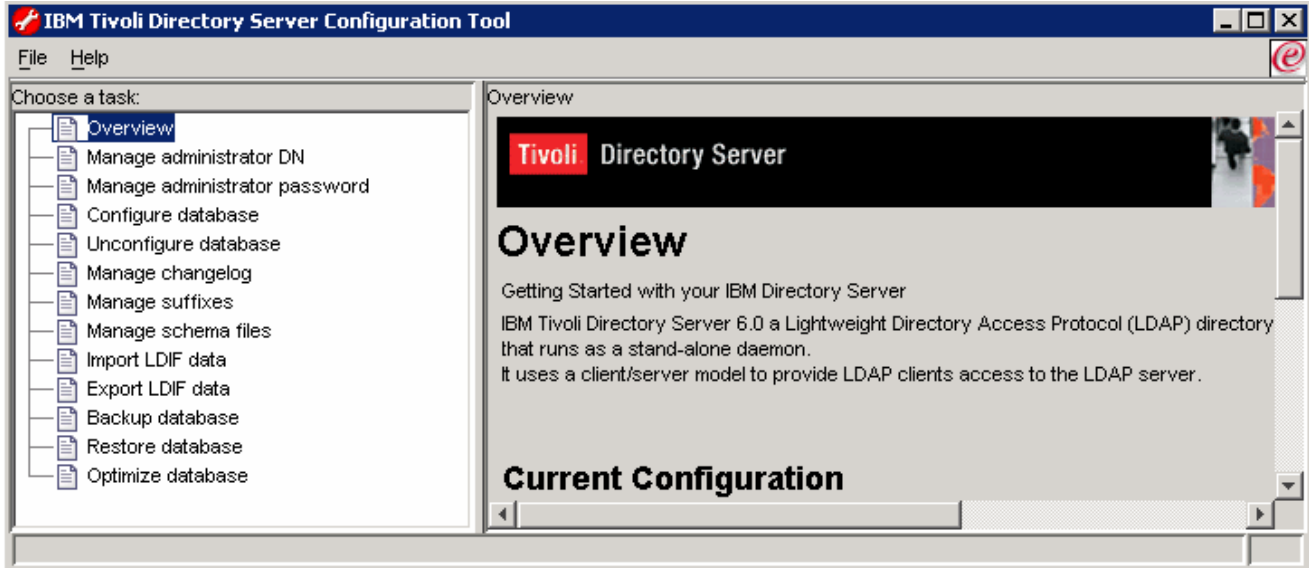
Part 1: Configure Tivoli Directory Server user repository with WebSphere Partner Gateway users

1. Stop the Tivoli Directory Server if it is already started. To stop the IBM Tivoli Directory Server from the Windows Services by right clicking on “IBM Tivoli Directory Server Instance V6.0” .

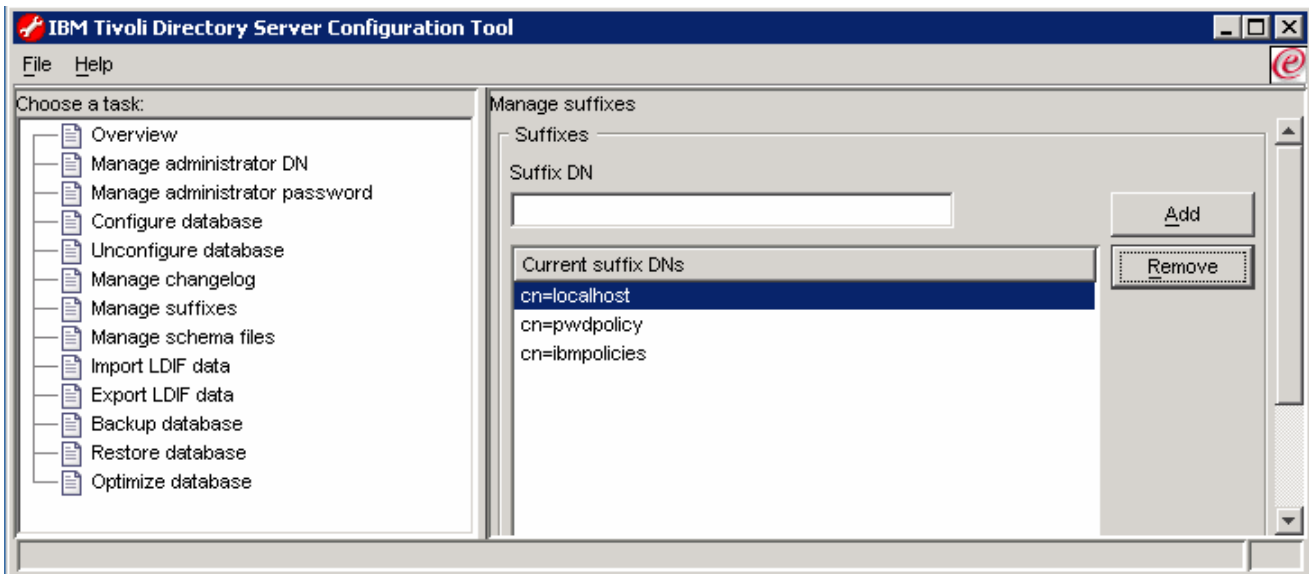


2. To configure the directory server with users and groups by importing the LDIF file, open a command window and type `idsxcfg`. The **IBM Tivoli Directory Server Configuration Tool** opens

WebSphere Partner Gateway V6.1 – Configure LDAP based security

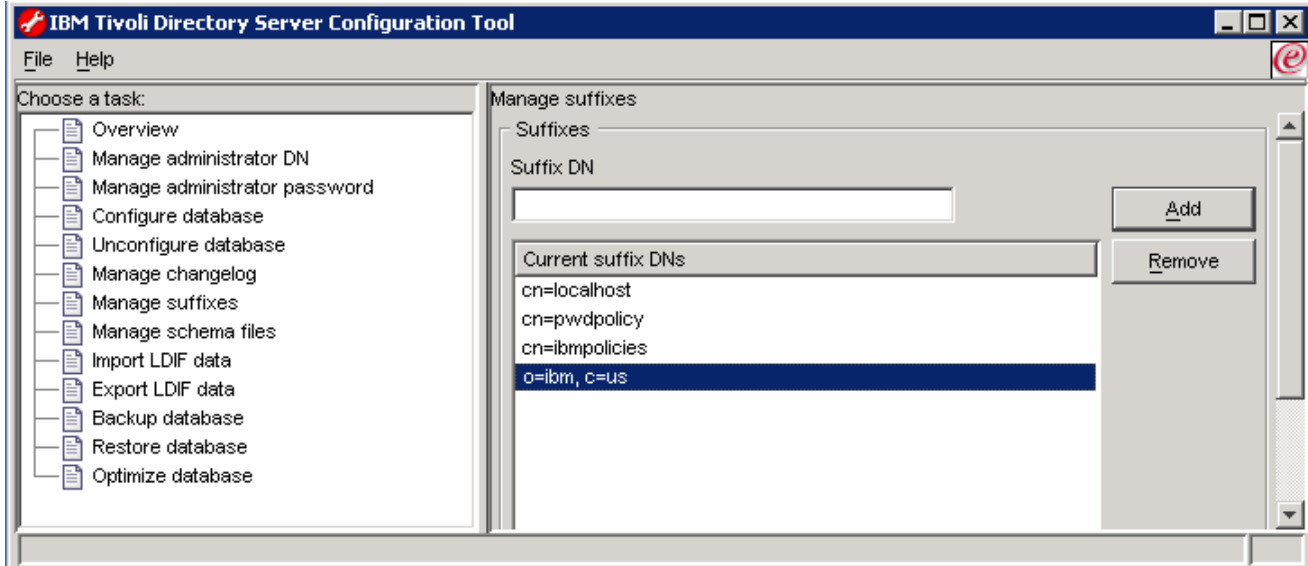


- 3. Click the **Manage suffixes** link to choose the manage suffix task over the left navigation pane. The **Manage suffixes** window opens in the Right pane

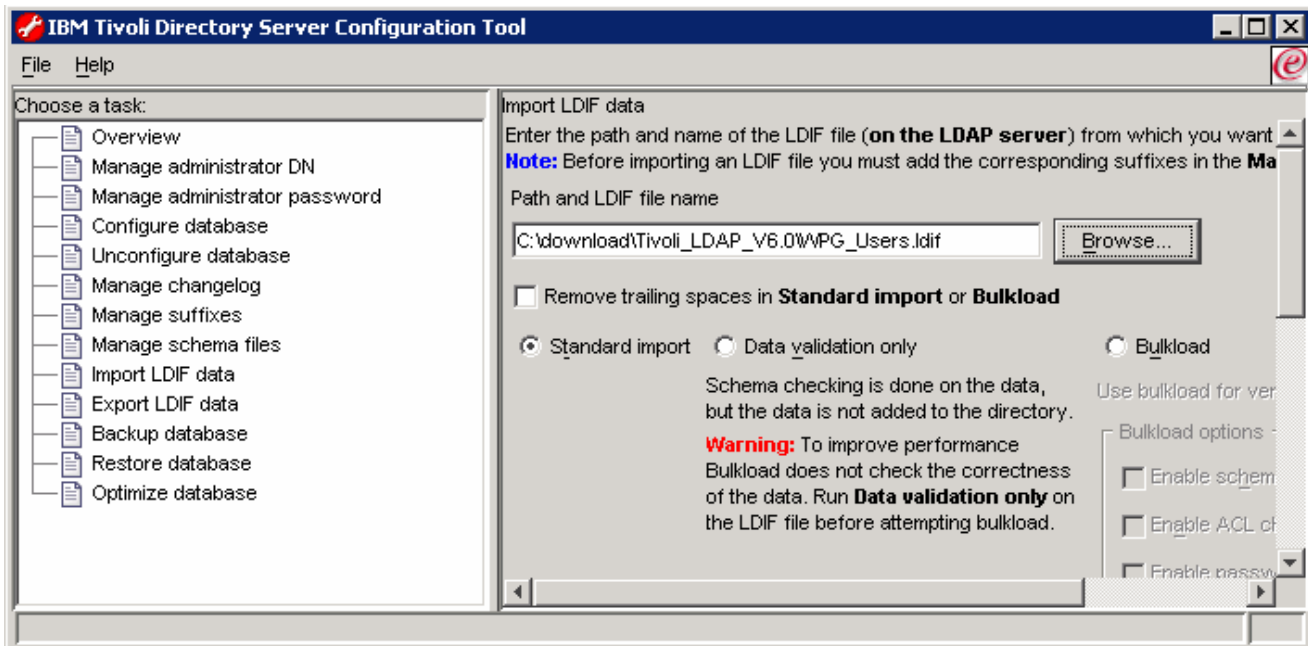


- 4. For the **Suffix DN** field, enter the value as **o=ibm,c=us** and click the **Add** button. The value must reflect under the **Current suffix DNs** text area as shown below:

WebSphere Partner Gateway V6.1 – Configure LDAP based security

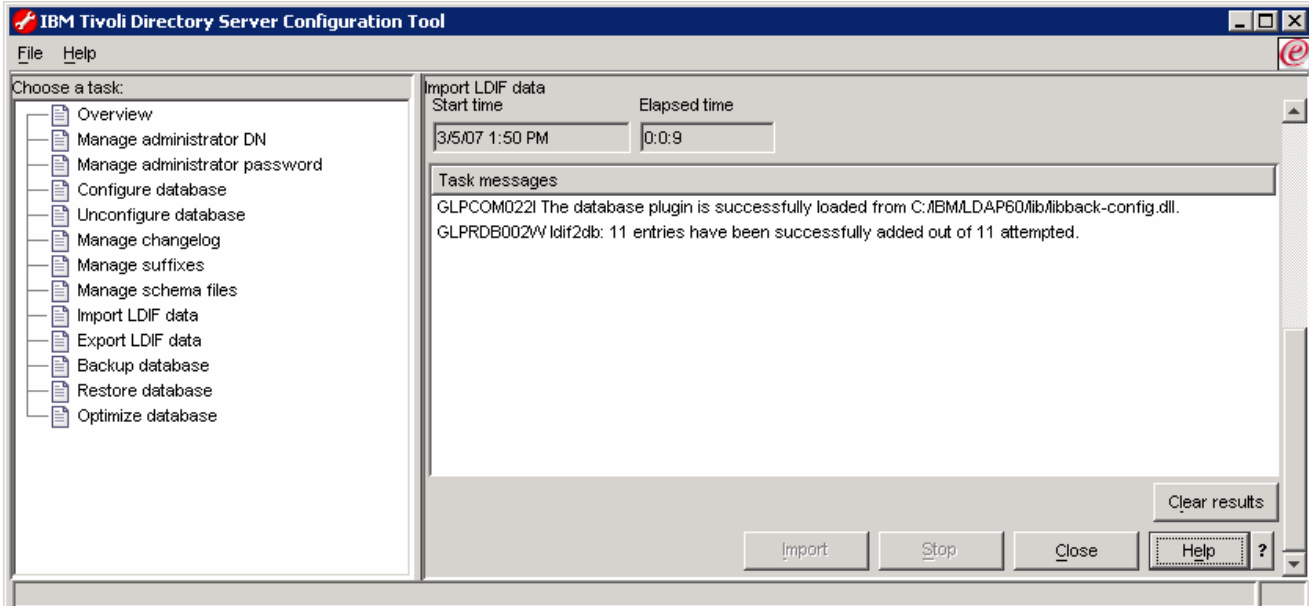


5. Scroll down for the Manage suffixes window in the right pane and click **OK**
6. To import the users and groups, click on the **Import LDIF data** over the left pane of the window. The **Import LDIF data screen** opens. Click the **Browse** button for the "Path and LDIF file name" and navigate to the LDIF file in <LAB_FILES>/Security/WPG_Users.ldif. Also ensure that the radio button next to **Standard import** is selected



7. Scroll down for the Import LDIF data window in the right pane and click **Import**

WebSphere Partner Gateway V6.1 – Configure LDAP based security



- ___ 8. On a successful message, click the **Clear** button to clear the results and then the **Close** button
- ___ 9. Close the **IBM Tivoli Directory Server Configuration Tool**
- ___ 10. Start the Tivoli Directory Server. To start the IBM Tivoli Directory Server from the Windows **Services** by right clicking on “**Tivoli Directory Server Instance V6.0**”
- ___ 11. The Tivoli Directory Server Configuration is complete

Part 2: Enable LDAP security for WebSphere Application Server V6.1

To enable LDAP security for the WebSphere Application Server V6.1, complete the following steps:

- ___ 1. Start the WebSphere Application Server
 - ___ a. Open a command window and change the directory to **C:\IBM\WPG61\wpghubsimple\bin**
 - ___ b. `cd C:\IBM\WPG61\wpghubsimple\bin`
 - ___ c. Run the following command: **bcgStartServer.bat**

```

C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\bcguser>cd C:\IBM\WPG61\wpghubsimple\bin
C:\IBM\WPG61\wpghubsimple\bin>bcgStartServer.bat_
  
```

- ___ 2. Open WebSphere Application Server Administrative console in a Web browser using the following URL:
<http://localhost:58090/ibm/console/>
- ___ 3. In the Welcome screen of the Administrative console, enter a user ID of your choice and click the **Login** button

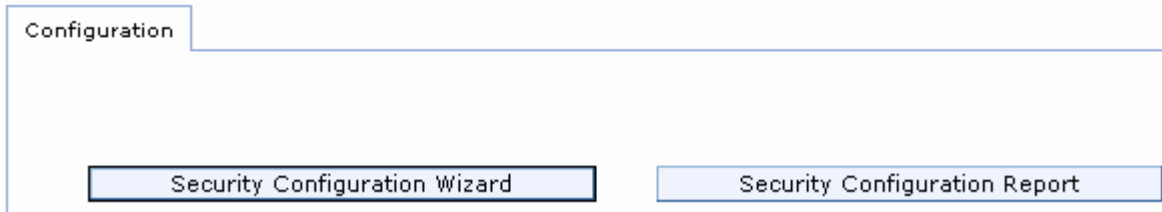
Welcome, enter your information.

User ID:

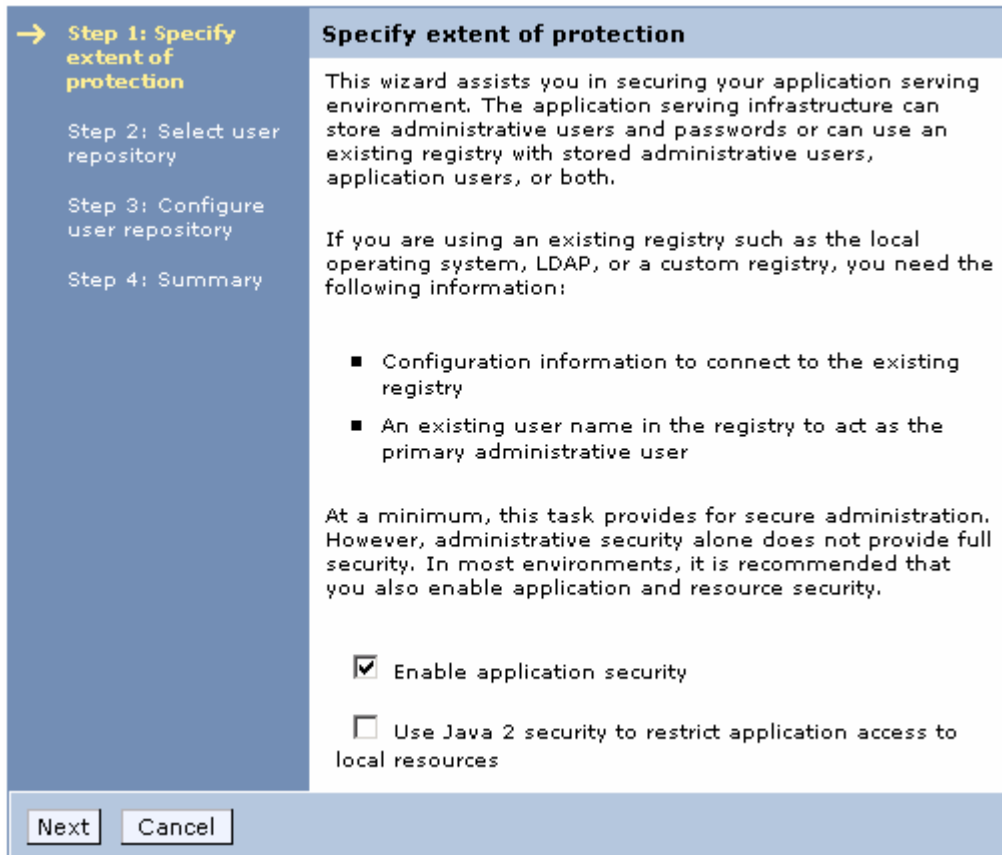
- ___ 4. On a successful login to the Administrative console, expand **Security** and click the **“Secure administration, applications, and infrastructure”** link in the left navigation pane. The **Secure administration, applications, and infrastructure** screen opens in the right pane



- ___ 5. In the **Secure administration, applications, and infrastructure** screen, click the **“Security Configuration Wizard”** button to start the security configuration wizard



6. In the following screen, select the check box next to **“Enable application security”** for Step1 **Specify extent of protection**



7. Click **Next**
8. In the following screen, select the radio button next to **“Standalone LDAP registry”** for Step2 i.e **Select user repository**

WebSphere Partner Gateway V6.1 – Configure LDAP based security

Step 1: Specify extent of protection → Step 2: Select user repository Step 3: Configure user repository Step 4: Summary	Select user repository
	<p>The user account repository stores users and group names that are used for authentication and authorization. The default repository is built into the application serving system and can be federated with one or more external Lightweight Directory Access Protocol (LDAP) repositories. You can also select a standalone external repository.</p> <p> <input type="radio"/> Federated repositories <input checked="" type="radio"/> Standalone LDAP registry <input type="radio"/> Local operating system <input type="radio"/> Standalone custom registry </p>
<input type="button" value="Previous"/> <input type="button" value="Next"/> <input type="button" value="Cancel"/>	

___ 9. Click **Next**

___ 10. In the following screen, enter the following user repository information:

- ___ a. **Primary administrative user name** : wasadmin
- ___ b. **Type of LDAP server** : IBM Tivoli Directory Server
- ___ c. **Host** : <IP address or Fully Qualified host name of the LDAP server machine>
- ___ d. **Port** : 389 (default)
- ___ e. **Base distinguished name (DN)** : o=ibm,c=us
- ___ f. **Bind distinguished name (DN)** : cn=root
- ___ g. **Bind password** : ldapadmin

WebSphere Partner Gateway V6.1 – Configure LDAP based security

Configure user repository

The repository stores users and group names that are used for authentication and authorization. The application server infrastructure can register users and groups. If security was previously enabled using this repository, provide the name of a user with administrator privileges that is in the repository.

* Primary administrative user name
wasadmin

* Type of LDAP server
IBM Tivoli Directory Server

* Host
aimcp097.austin.ibm.com

Port
389

Base distinguished name (DN)
o=ibm,c=us

Bind distinguished name (DN)
cn=root

Bind password

Previous Next Cancel

____ 11. Click **Next**

Note: On clicking '**Next**' in the above step, the Security Configuration Wizard connects to LDAP server to verify the information provided. On a successful verification, the Security Configuration Wizard lists the values selected during the wizard in the following screen.

____ 12. Review the **Summary** screen

WebSphere Partner Gateway V6.1 – Configure LDAP based security

Step 1: Specify extent of protection

Step 2: Select user repository

Step 3: Configure user repository

→ **Step 4: Summary**

Summary

Displays the list of values that are selected during the wizard and are used to enable security.

Options	Values
Enable administrative security	true
Enable application security	true
Use Java 2 security to restrict application access to local resources	false
User repository	Standalone LDAP registry
Primary administrative user name	wasadmin
Type of LDAP server	IBM Tivoli Directory Server
Host	aimcp097.austin.ibm.com
Port	389
Base distinguished name (DN)	o=ibm,c=us
Bind distinguished name (DN)	cn=root
Bind password	*****

Previous
Finish
Cancel

___ 13. Click **Finish**

___ 14. In the following screen, click the **Save** link to save the changes to the master configuration

☐ Messages

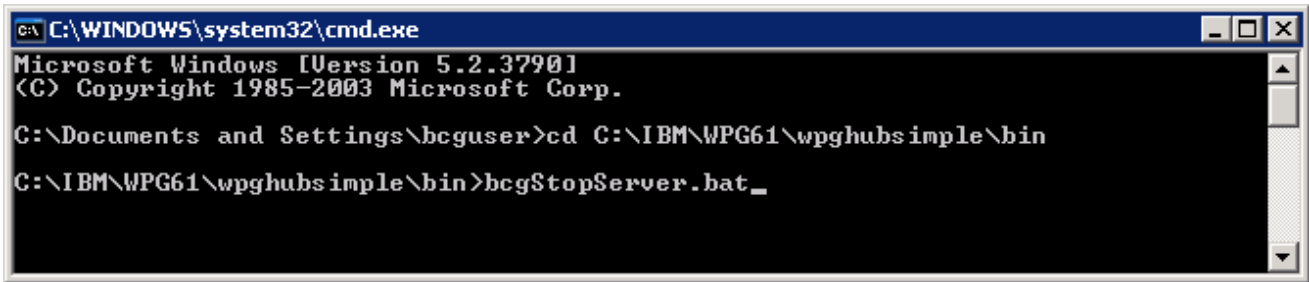
- ⚠ Changes have been made to your local configuration. You can:
 - [Save](#) directly to the master configuration.
 - [Review](#) changes before saving or discarding.
- ⚠ The server may need to be restarted for these changes to take effect.

___ 15. Logoff from the Administrative console

___ 16. The security enablement for the WebSphere Application Server V6.1 is complete. Restart the application server

___ 17. Stop the WebSphere Application Server from command window as shown below using the following command: **bcgStopServer.bat**

WebSphere Partner Gateway V6.1 – Configure LDAP based security



```
C:\WINDOWS\system32\cmd.exe
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\Documents and Settings\bcguser>cd C:\IBM\WPG61\wpghubsimple\bin
C:\IBM\WPG61\wpghubsimple\bin>bcgStartServer.bat_
```

___ 18. Start the WebSphere Application Server from command window using the following command:
bcgStartServer.bat

___ 19. Once the application server has started, open the Administrative console in a Web browser using the following URL to test if the security enablement is successful:

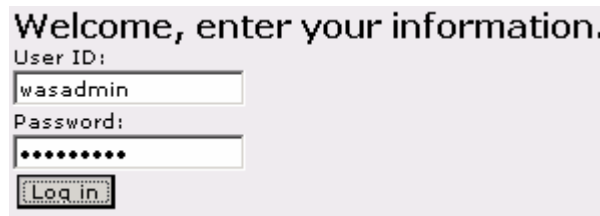
http://localhost:58090/ibm/console/

___ 20. Click **Yes** over the security certificate

___ 21. In the Welcome screen of the Administrative console, enter,

___ a. **User ID** : wasadmin

___ b. **Password** : wasadmin



___ 22. Click the **Login** button. A successful login to the Administrative console states that the valid credentials are provided

Part 3: Logging into WebSphere Partner Gateway community console

WebSphere Partner Gateway console allows the users to create and configure the partners, receivers, destinations, business-to-business capabilities, interactions and connections

___ 1. Open a Web browser and type the following URL:

Unsecured: **http://<host name>.<domain>:58080/console**

Secure: **https://<host name>.<domain>:58443/console**

Where <host name> and <domain> are the name and location of the computer hosting the Community Console component.

Note: WebSphere Partner Gateway Community Console requires cookie support to be turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

___ 2. The Web browser displays the Welcome page.

___ 3. If this is the first time logging into the console, use the following steps to log in and reset the temporary password.

___ a. In the “**User Name**” field, type: **hubadmin**

___ b. In the “**Password**” field, type: **Pa55word**

___ c. In the “**Company Login Name**” field, type: **Operator** Click **Login**.

___ d. When you log in for the first time, you must create a new password.

Enter a new password as **hub1admin**,

then enter the new password **hub1admin** a second time in the **Verify** field.

___ e. Click **Save**.

___ f. The system displays the console’s initial entry window.

___ 4. If you have previously logged into the console and reset the password, then use the appropriate credentials to log into the console

Part 4: Create participants & users


By default hubadmin user already exists after WebSphere Partner Gateway installation. You will now create user hubadmin2 and add him to Hubadmin group. Also a new Partner Partner1 is created with users partner1user and partner1user2.

All the users that are created for partners should be part of your LDAP directory. If not they cannot log in to the community console when LDAP based authentication is enabled.

In the Idif file you imported to create the users directory in LDAP the users that you are going to create and the hubadmin user are already specified. So when LDAP authentication is enabled, all the users that exist in the LDAP and exist in the WebSphere Partner Gateway partner profiles can be configured to be able to login to community console.

- ___ 1. Create the **hubadmin2** user for Hub Operator and add to **Hubadmin Group**
 - ___ a. In the WebSphere Partner Gateway Community Console, navigate to **Account Admin → Profiles → Partner**
 - ___ b. Click on the **Users** on the menu
 - ___ c. Click Create to create a new user for Hub Operator
 - ___ d. Provide the following details and click Save
 - 1) **User Name** : hubadmin2
 - 2) **Given Name** : hubadmin2
 - 3) **Password** : pa55word
 - 4) **Re-enter Password** : pa55word

Profile ▾ Hub Operator ▾ User Detail ▾

 User Name *

Status Enabled Disabled

Given Name

Family Name

E-Mail

Telephone

Fax Number

Language Locale ▾

Format Locale ▾

Time Zone ▾

Alert Status Enabled Disabled


Subscribed

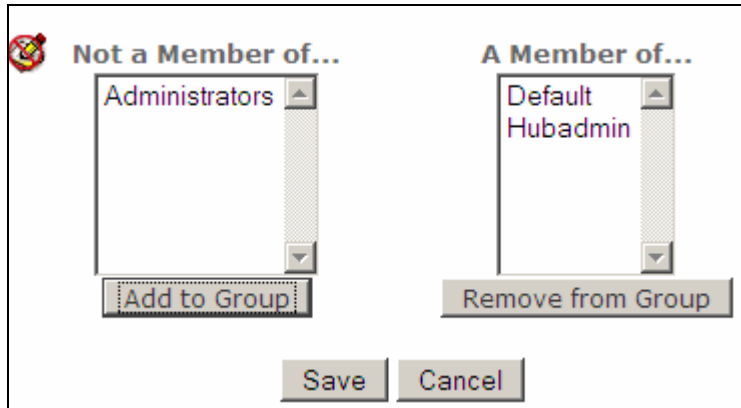
Visibility Global Local

Password *

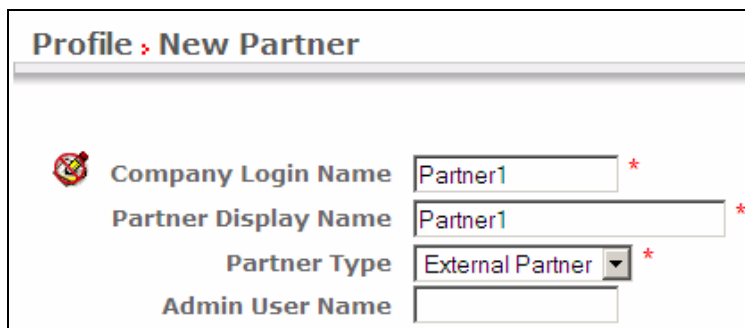
Re-enter Password *

WebSphere Partner Gateway V6.1 – Configure LDAP based security

- ___ e. On the next screen, click on the **Memberships** link on the right corner.
- ___ f. Click on the  icon
- ___ g. Select **Hubadmin** and click the **Add to Group** button




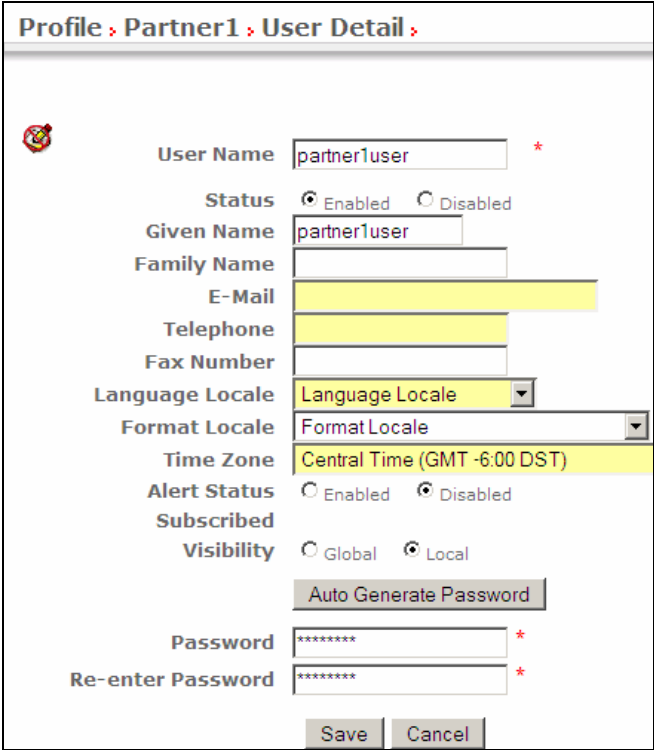
- ___ h. Click **Save**
- ___ 2. Create a new Community Partner **Partner1**
 - ___ a. In the WebSphere Partner Gateway Community Console, navigate to **Account Admin → Profiles → Partner**
 - ___ b. Click on the **Create** link on the right corner
 - ___ c. Provide the following details and click **Save**
 - 1) **Company Login Name:** Partner1
 - 2) **Partner Display Name:** Partner1



- ___ 3. Create users for the new Community Partner **Partner1**
 - ___ a. In the WebSphere Partner Gateway Community Console, navigate to **Account Admin → Profiles → Partner**
 - ___ b. Click **Search**


WebSphere Partner Gateway V6.1 – Configure LDAP based security

- __ c. Select **Partner1** by clicking on the  Icon
- __ d. Click on the **Users** menu option
- __ e. Click **Create** link on the right corner
- __ f. Provide the following details and click **Save**
 - 1) **User Name** : partner1user
 - 2) **Given Name** : partner1user
 - 3) **Password** : pa55word
 - 4) **Re-enter Password** : pa55word




The screenshot shows a web form titled "Profile : Partner1 : User Detail". It contains the following fields and options:

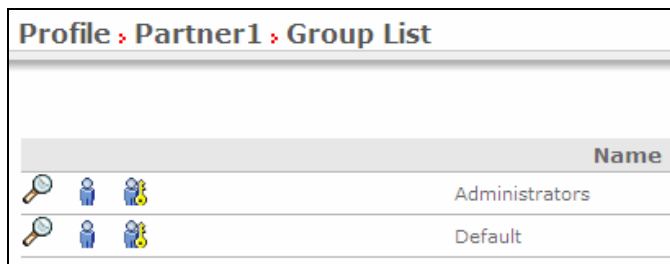
- User Name**: Input field with "partner1user" and a red asterisk.
- Status**: Radio buttons for "Enabled" (selected) and "Disabled".
- Given Name**: Input field with "partner1user".
- Family Name**: Empty input field.
- E-Mail**: Yellowed-out input field.
- Telephone**: Yellowed-out input field.
- Fax Number**: Empty input field.
- Language Locale**: Dropdown menu with "Language Locale" selected.
- Format Locale**: Dropdown menu with "Format Locale" selected.
- Time Zone**: Dropdown menu with "Central Time (GMT -6:00 DST)" selected.
- Alert Status**: Radio buttons for "Enabled" and "Disabled" (selected).
- Subscribed**: Radio buttons for "Global" and "Local" (selected).
- Visibility**: Radio buttons for "Global" and "Local" (selected).
- Auto Generate Password**: Button.
- Password**: Input field with "*****" and a red asterisk.
- Re-enter Password**: Input field with "*****" and a red asterisk.
- Save** and **Cancel**: Buttons at the bottom.



- __ g. In the WebSphere Partner Gateway Community Console, navigate to **Account Admin** → **Profiles** → **Partner**
- __ h. Click **Search**
- __ i. Select **Partner1** by clicking on the  Icon
- __ j. Click on the **Users** menu option
- __ k. Click **Create** link on the right corner
- __ l. Provide the following details and click **Save**

WebSphere Partner Gateway V6.1 – Configure LDAP based security


- 1) **User Name** : partner1user2
- 2) **Given Name** : partner1user2
- 3) **Password** : pa55word
- 4) **Re-enter Password** : pa55word

- ___ 4. Assign users for the new Community Partner **Partner1** to groups
- ___ a. In the WebSphere Partner Gateway Community Console, navigate to **Account Admin** → **Profiles** → **Partner**
 - ___ b. Click **Search**
 - ___ c. Select **Partner1** by clicking on the  Icon
 - ___ d. Click on the **Groups** menu option



- ___ e. Click on the  icon next to **Administrators**
- ___ f. Click on the  icon
- ___ g. Select **partner1user** and click the **Add to Group** button
- ___ h. Click **Save**, **partner1user** is now part of the **Partner1's Administrator** group
- ___ i. By default when a user is created for a partner, they are assigned to Default group. So **partner1user2** is part of the Default group,

Part 5: Enable LDAP container based authentication for WebSphere Partner Gateway console

- ___ 1. Log into the Community console as hubadmin
- ___ 2. Navigate to **System Administration** → **Common Properties**
- ___ 3. Click on the  icon
- ___ 4. Change the value of the property **bcg.ldap.containerauth** to **True**.

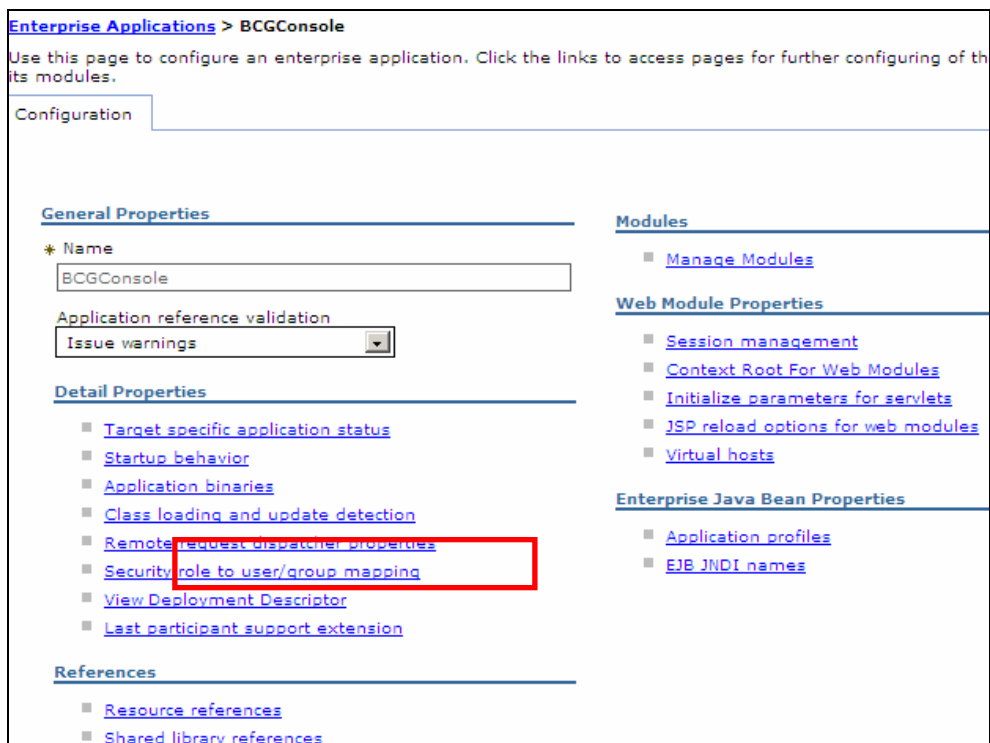
bcg.ldap.containerauth	True
bcg.ldap.jaaslogin	WSLogin
bcg.receiver.persistpath	C:/IBM/WPG61/wpghub

- ___ 5. Click **Save**
- ___ 6. Log out of the community console

Part 6: Map WebSphere Partner Gateway user roles

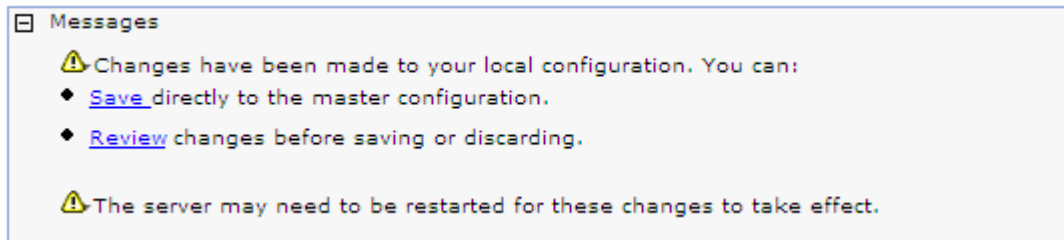
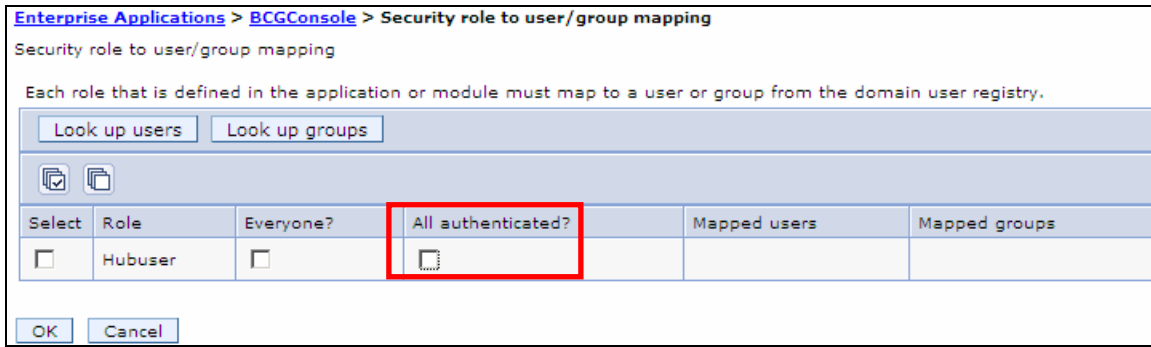
After authentication in LDAP server, you must associate the LDAP user with the Hubuser role. Only users who are members of this role can enter the application after authentication. To define LDAP users as a member of this role:

- ___ 1. Start the WebSphere application server that has the Console application deployed
 - ___ a. Go to <WPG_HOME>\wpghubsimple\bin and run the bcgstartserver.bat file
- ___ 2. Log into the WebSphere Administrative console by providing the Administrator user id and password (wasadmin/wasadmin). The url for the Administrative console is <http://<host name>:58090/admin>
- ___ 3. Select Applications → Enterprise Applications and then click on the BCGConsole application

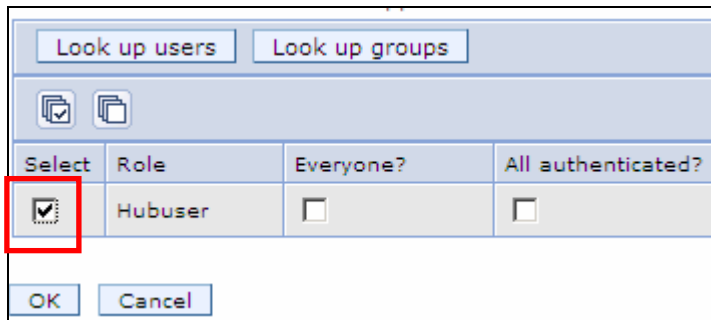



- ___ 4. Click Security roles to user/group mapping link
- ___ 5. In the next screen, uncheck the **All authenticated?** Click **Ok** button and save the changes by clicking on the **Save** link

WebSphere Partner Gateway V6.1 – Configure LDAP based security



- ___ 6. Select Applications → Enterprise Applications and then click on the BCGConsole application
- ___ 7. Click **Security roles to user/group mapping** link
- ___ 8. In the next screen, select the check box next to click the **Look up Users** button



- ___ 9. Click the **Search** button. This will list all the users defined in the LDAP user repository configured.
- ___ 10. Select all the users one by one in the **Available** and move them to **Selected** by clicking on the  icon.
- ___ 11. Click **Ok**. And then the **save** link to save changes.

WebSphere Partner Gateway V6.1 – Configure LDAP based security

[Enterprise Applications](#) > [BCGConsole](#) > [Security role to user/group mapping](#) > [Look up users or groups](#)

Specifies whether to look up users or groups.

The following roles are mapped to the items in the selected list.

■ Hubuser

To search for users or groups, enter a **limit** (number) and a **search pattern** (such as a*) and click **Search**:

limit (number of items)
20

Search String
*

Select users or groups in the Available list. Move them to the Selected list by clicking >>.

Available:		Selected:
cn=wasadmin,o=ibm,c=us cn=hubadmin,o=ibm,c=us cn=hubadmin2,o=ibm,c=us cn=partner1user,o=ibm,c=us cn=partner1user2,o=ibm,c=us cn=testuser,o=ibm,c=us	>> <<	cn=wasadmin,o=ibm,c=us cn=hubadmin,o=ibm,c=us cn=hubadmin2,o=ibm,c=us cn=partner1user,o=ibm,c=us cn=partner1user2,o=ibm,c=us

____ 12. Log out of the Administrative Console.

Part 7: Logging into community console with LDAP authentication enabled

- ___ 1. Open a Web browser and type the following URL:

Unsecured: **http://<host name>.<domain>:58080/console**

Secure: **https://<host name>.<domain>:58443/console**

Where <host name> and <domain> are the name and location of the computer hosting the Community Console component.

Note: WebSphere Partner Gateway Community Console requires cookie support to be turned on to maintain session information. No personal information is stored in the cookie, and it expires when the browser is closed.

- ___ 2. The Web browser displays the Welcome page. Notice that the Log in page displayed is different from the one displayed when using the database based authentication



- ___ 3. You can now use the LDAP credentials to log into the community console
- ___ 4. In the user repository you have hubadmin, hubadmin2 who are defined as Hubadmin group members in WebSphere Partner Gateway. So when you log as hubadmin, hubadmin2 you are logged in as super users.
- ___ 5. Log in and check the community console logged in as following users
- Username : hubadmin
- Password : hub1admin

Username : hubadmin2

Password : hub2admin

____ 7. Log out of the community console

____ 6. In the user repository you have partner1user and parner1user2 who are defined as Partner1 members in WebSphere Partner Gateway. Partner1user2 is the Administrator of the Partner1 so when you log as partner1user2 you are logged in as Administrator.

Username : partner1user

Password : partner1user

Username : partner1user2

Password : partner1user2

____ 8. Log out of the community console

Part 8: Disable LDAP based authentication

You might have to stop LDAP authentication under the following circumstances:

- The LDAP server stops or permanently goes down.
- Container based authentication was chosen when installing WebSphere Partner Gateway but the LDAP server is not ready.

Note for UNIX® users: users who use DB2 must log in as the db2instance user and use the db2instance username and password to run the script. Users who use Oracle must log in as the oracle user and use the username and password given at the time of installation to run the scripts

Disabling LDAP based authentication in WebSphere Partner Gateway:

- ___ 1. Open a command prompt window
- ___ 2. Change directories to <WPG_HOME>/wpgappsdb/scripts/DB2.
- ___ 3. Use the command db2cmd. This should open DB2 command window.
- ___ 4. In the DB2 command window , use the following command
 - ___ a. bcgResetAuthentication.bat <database user> <database user password> for Windows
 - ___ b. bcgResetAuthentication.bat <database user> <database user password> for Linux

This script Sets the attribute **bcg.ldap.containerauth** located in the Console **System Administration > Console Properties > Common Attributes** to **False**.

Resets the hubadmin user ID password to the installation default and the database is now used to store passwords.

Note: After these scripts are run, any passwords that were configured in LDAP must be reentered for each defined user using the WebSphere Partner Gateway Console

Disabling LDAP based authentication in WebSphere Application Server:

- ___ 1. Open a command prompt window
- ___ 2. Change directories to <WPG_HOME>/wpghubsimple/wasND/Profiles/bcgprofile/bin
- ___ 3. Use the following commands
 - ___ c. **wsadmin –conntype NONE**
 - ___ d. **securityoff**

___ e. **quit**

- ___ 4. Restart the server for changes to take effect. You need to provide username and password to stop the server.
- ___ 5. Change directories to <WPG_HOME>/wpghubsimple/wasND/Profiles/bcgprofile/bin
- ___ 6. Use the following command

```
stopserver.bat server1 –username <username> -password <password>
```

ex: stopserver.bat server1 –username wasadmin -password wasadmin
- ___ 7. Start the server by using the following command

```
Startserver.bat server1
```

You have successfully completed disabling LDAP based authentication on both WebSphere Application Server and WebSphere Partner Gateway

What you did in this exercise

In the lab exercise, you have

- created a user repository in the LDAP server
- configured application security for the WebSphere Application Server,
- enabled LDAP authentication use in WebSphere Partner Gateway
- Mapped users to Hub user role for the BCGConsole application
- Logged into the console using LDAP authentication and
- Disabled security on WebSphere Partner Gateway and WebSphere Application Server

Trademarks, Copyrights, and Disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM	CICS	IMS	MQSeries	Tivoli
IBM (logo)	Cloudscape	Informix	OS/390	WebSphere
e (logo) business	DB2	iSeries	OS/400	xSeries
AIX	DB2 Universal Database	Lotus	pSeries	zSeries

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

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

Intel, ActionMedia, LANDesk, MMX, Pentium and ProShare are trademarks of Intel Corporation in the United States, other countries, or both.

Other company, product and service names may be trademarks or service marks of others.

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or program(s) described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing

IBM Corporation

North Castle Drive

Armonk, NY 10504-1785

U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

(C) Copyright International Business Machines Corporation 2007. All rights reserved.

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