IBM WEBSPHERE BUSINESS MONITOR V6.1– End-to-end security

WebSphere Business Monitor V6.1
End-to-end security with a federated repository (LDAP)

What this exercise is about

The objective of this lab is to show you how to setup end to end security for Monitor Server, Portal Server, and Process Server using a federated repository.

Lab requirements

List of system and software required for the student to complete the lab.

- WebSphere Business Monitor V6.1 installed
- Tivoli Directory Server V6.0
- WebSphere Portal Server installed
- WebSphere Process Server installed

What you should be able to do

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

- Install and configure Tivoli Directory Server
- Setup security for Portal Server, Monitor Server and Process Server

Introduction

When you enable security, you are enabling administrative and application security settings. WebSphere Business Monitor uses many of the security mechanisms provided by the prerequisite products, including WebSphere® Application Server and WebSphere Portal.

For WebSphere Application Server, you must enable administrative and application security. For WebSphere Portal, you can enable security using the configuration wizard.

You can configure access to the monitor model resources using Monitor Data Security in the administrative console. For WebSphere Application Server instances that run the Business Monitor server including Web-based dashboards, you must configure them to use the federated repository, and not a local operating system, stand-alone LDAP registry, or stand-alone custom registry.

Note: If you are not using WebSphere Portal, you can use a file-based repository.

WebSphere Portal must be able to share a user registry with the Business Monitor server, meaning that only LDAP Server registry or custom user registry is supported.

Note: The WebSphere Portal database user registry cannot be used by and is not compatible with the Business Monitor server.

For this lab, you will create an LDAP registry using Tivoli Directory Server

LDAP information (reference)

For reference, these are the LDAP values that were used for this lab. Use appropriate values for your environment.

Property	Parameter
LDAPHostName	Idlsldap.austin.ibm.com
LDAPPort	389
LDAPAdminUId	cn=root
LDAPAdminPwd	ldapadmin
LDAPServerType	IBM Tivoli Directory Server V6.0
LDAPBindID	uid=wpsbind,cn=users,dc=ibm,dc=com
LDAPBindPassword	wpsbind
LDAPSuffix	dc=ibm,dc=com

User names used to complete the end-to-end security configuration

To make it simple, very few users are used to complete the monitor end-to-end security configuration. The following table refers to the users used on different servers in the monitor domain.

Server	User Name	Password
Portal Server (Dashboard)	wpsadmin	wpsadmin
WebSphere Application Server V6.1 (Monitor Server)	was61admin	was61admin
Process Server (BPEL)	wpsrvadmin	wpsrvadmin

Reference: 1

```
dn: uid=wpsadmin,cn=users,dc=ibm,dc=com
objectclass: organizationalPerson
objectclass: person
objectclass: top
objectclass: inetOrgPerson
uid: wpsadmin
userpassword: wpsadmin
sn: admin
givenName: wps
cn: wps admin
```

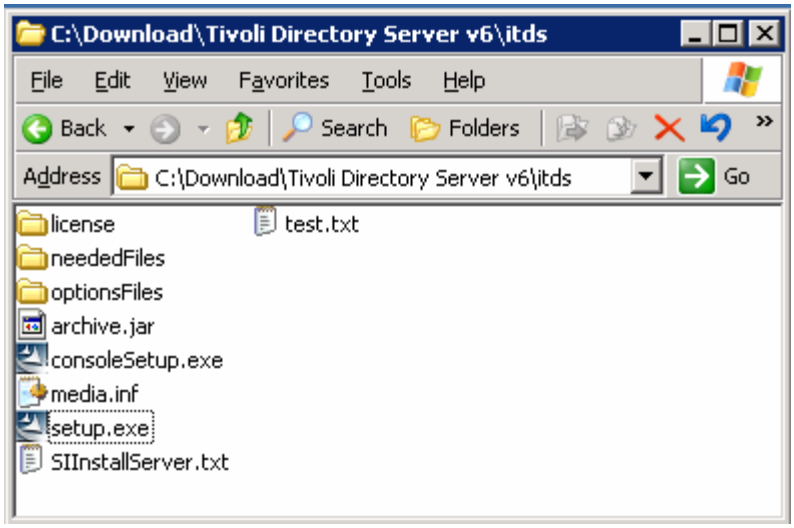
Reference: 2

```
dn: cn=wpsadmins,cn=groups,dc=ibm,dc=com
objectclass: groupOfUniqueNames
objectclass: top
uniquemember: uid=wpsadmin,cn=users,dc=ibm,dc=com
cn: wpsadmins
```

Part 1: Installing and configuring Tivoli Directory Server V6.0

This part of the lab provides instructions on how to install and configure the Tivoli Directory Server V6.0.

____ 1. Run the Tivoli Directory Server Launchpad by double clicking on **setup.exe**



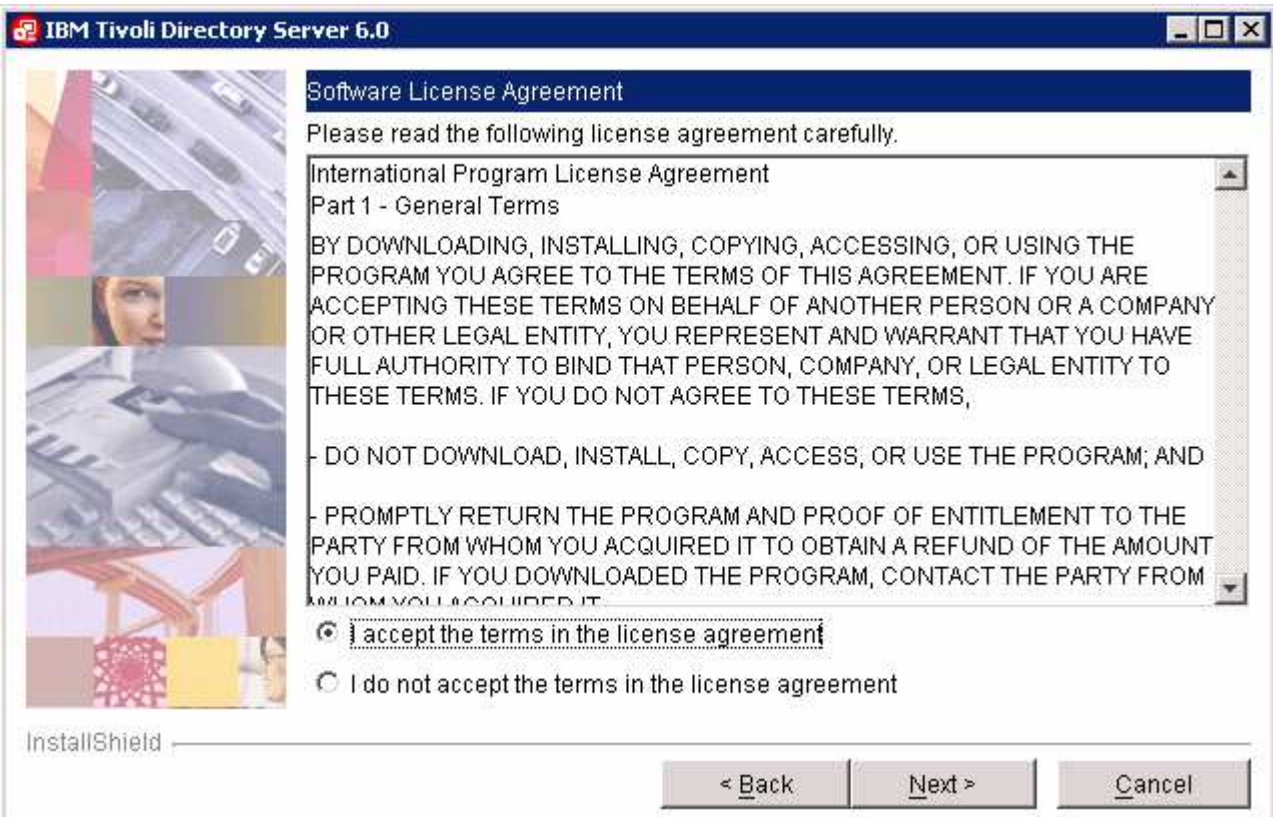
____ 2. Select **English** as the language to be used for this wizard

____ 3. Click **OK**

____ 4. Read the instructions on the Tivoli Directory Server V6.0 Welcome panel

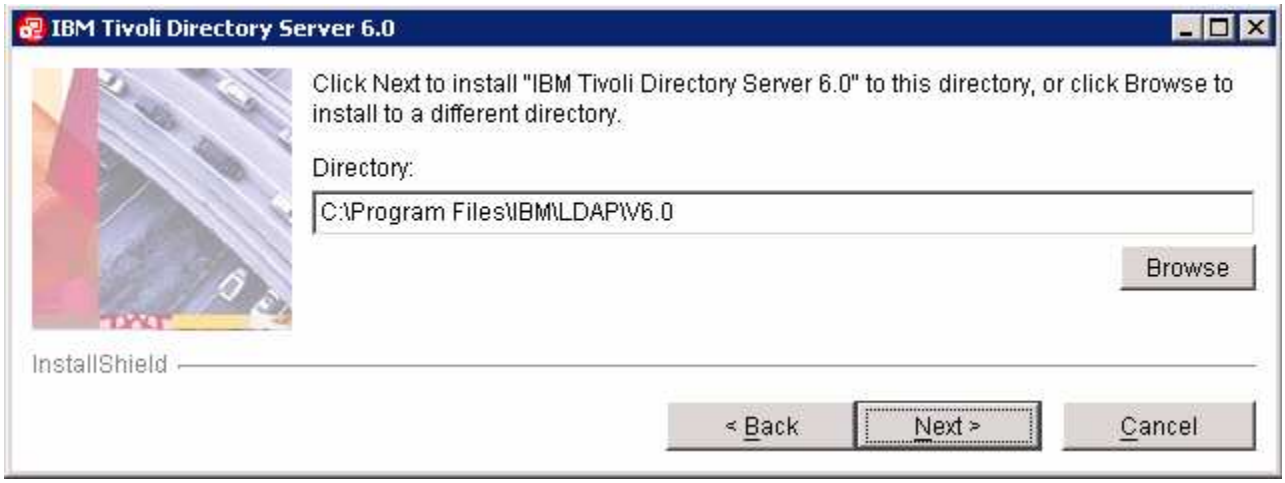
____ 5. Click **Next**

____ 6. Read the License agreement and accept it



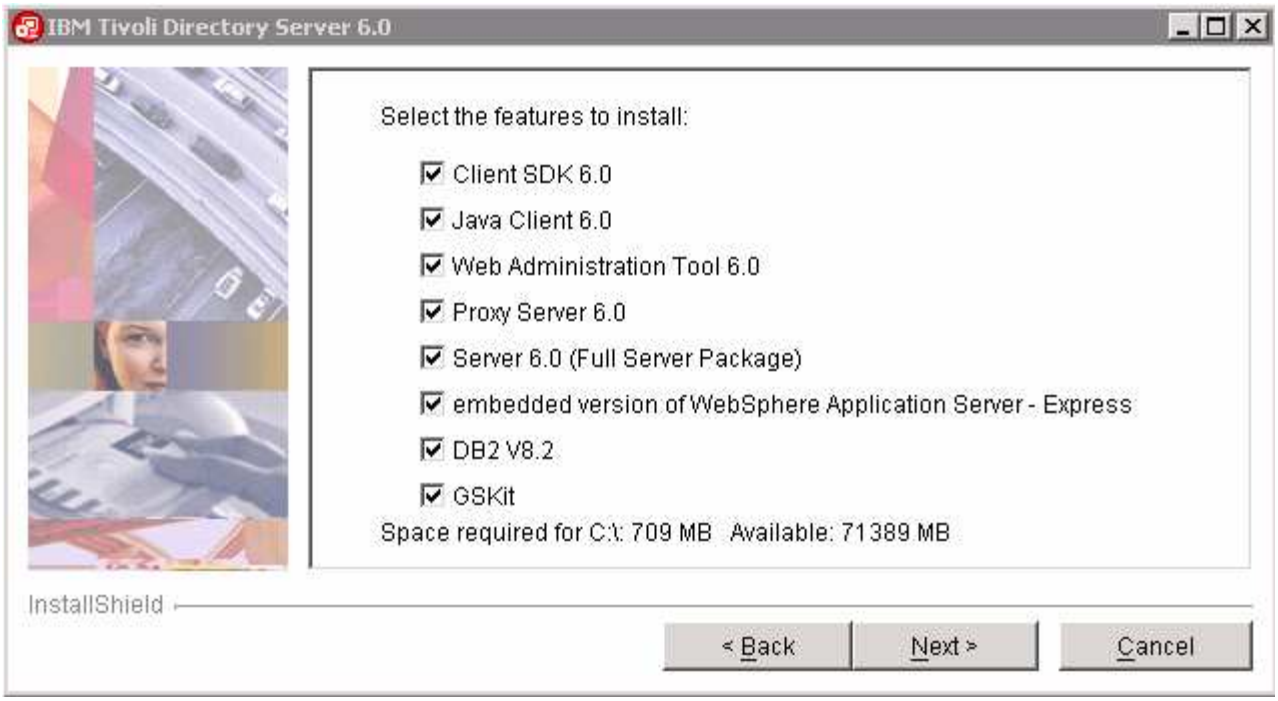
____ 7. Click **Next**

____ 8. In the following panel, accept the default **Directory Name** for the target install directory



____ 9. Click **Next**

____ 10. In the following "**Select the features to install**" panel, accept the defaults (all features)



____ 11. Click **Next**

____ 12. Enter the DB2 **User ID** and **Password**

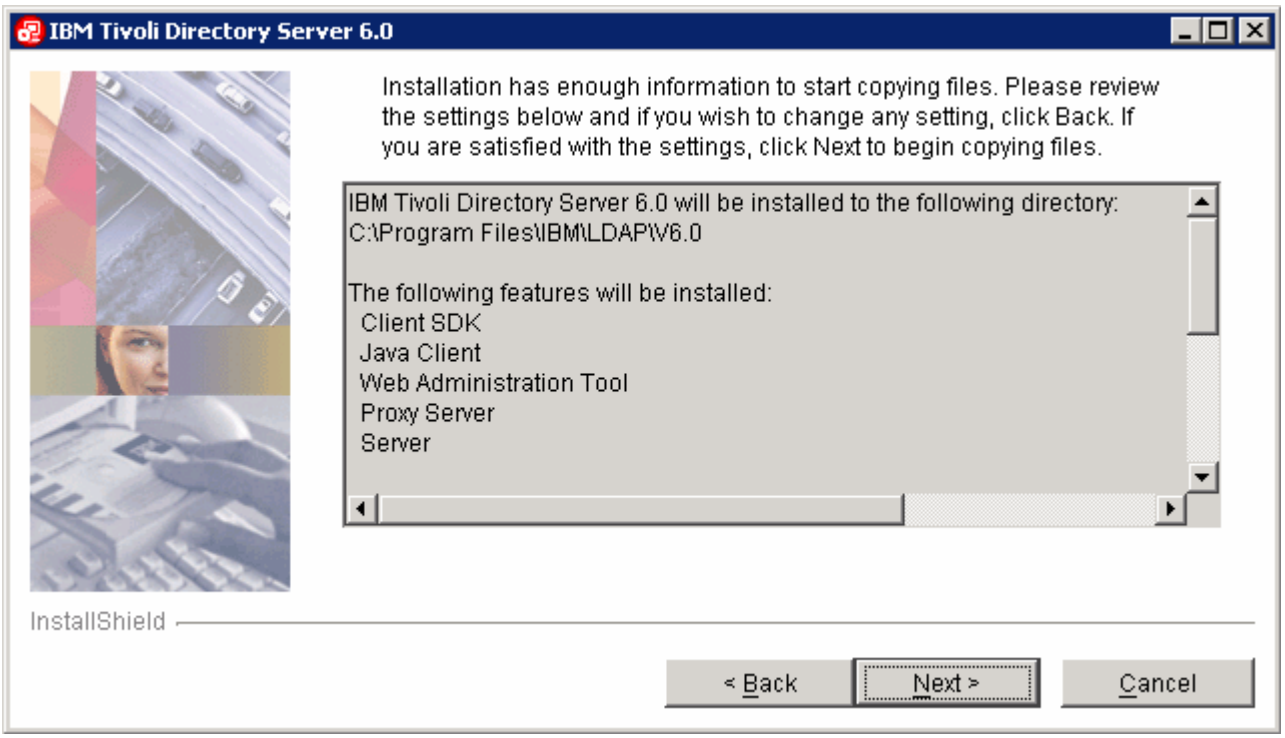
__ a. **User ID** **:** db2admin

__ b. **Password** **:** db2admin

__ c. **Confirm Password :** db2admin

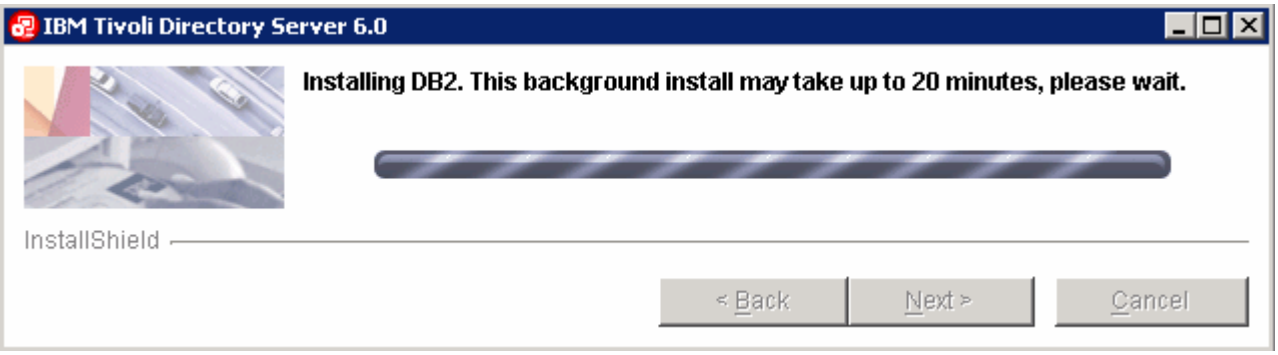
____ 13. Click **Next**

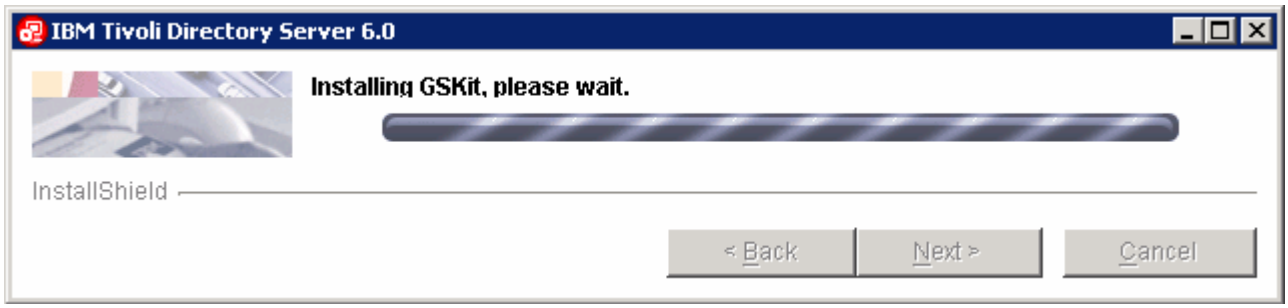
____ 14. Review the installation **Summary**

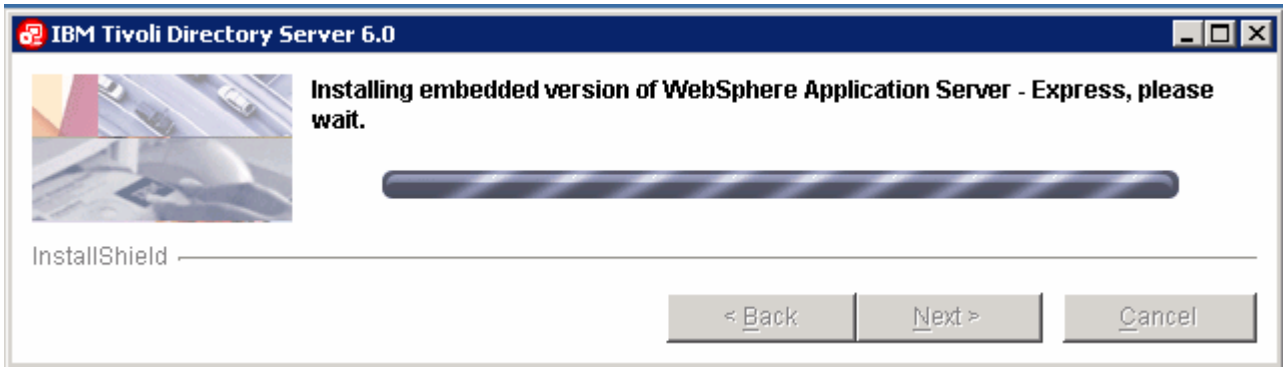


____ 15. Click **Next**

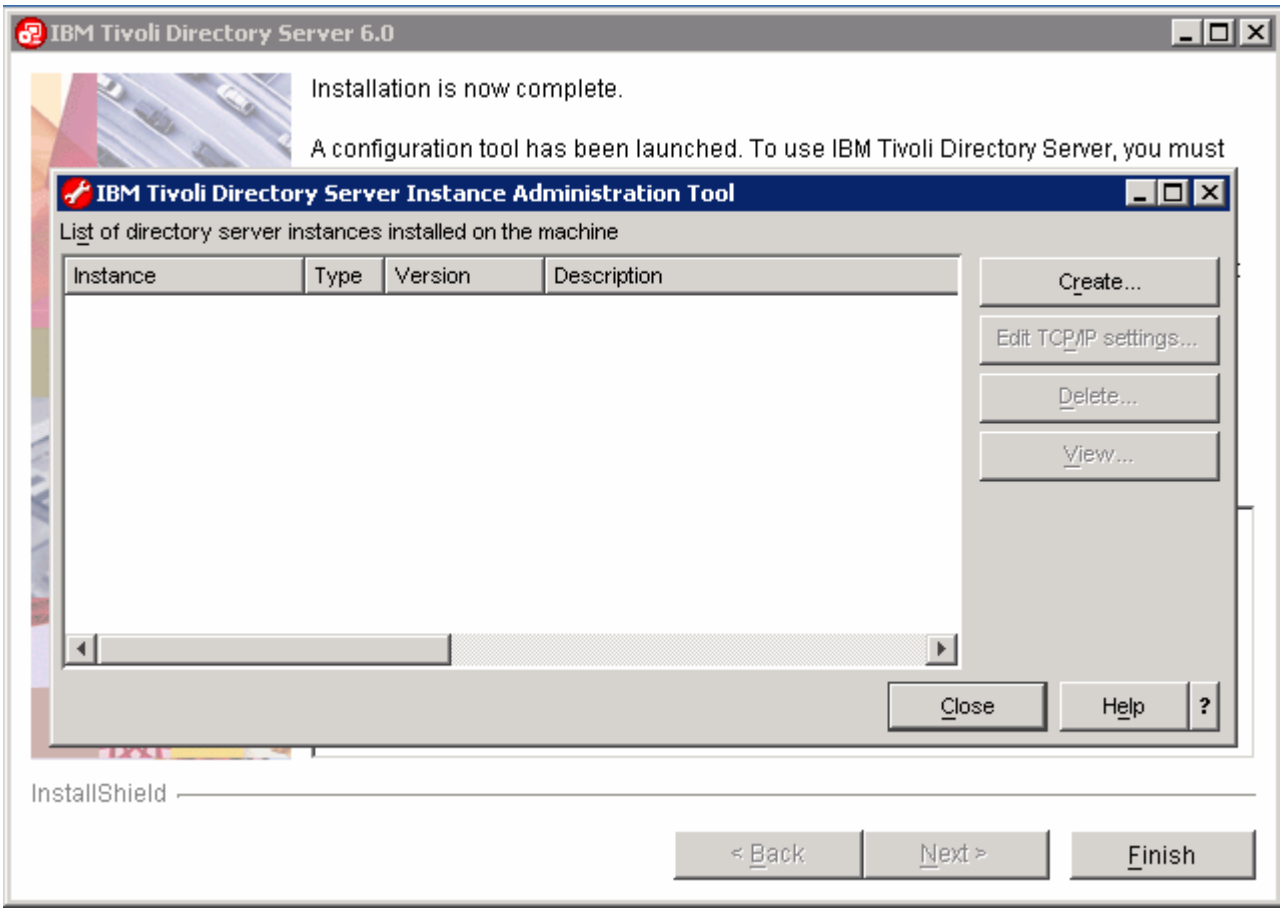
____ 16. The installation progresses starting with DB2 as shown below:







____ 17. Once the Installation is complete, the IBM Tivoli Directory Server instance Administration Tool is launched. You can close it at this point and launch it later.



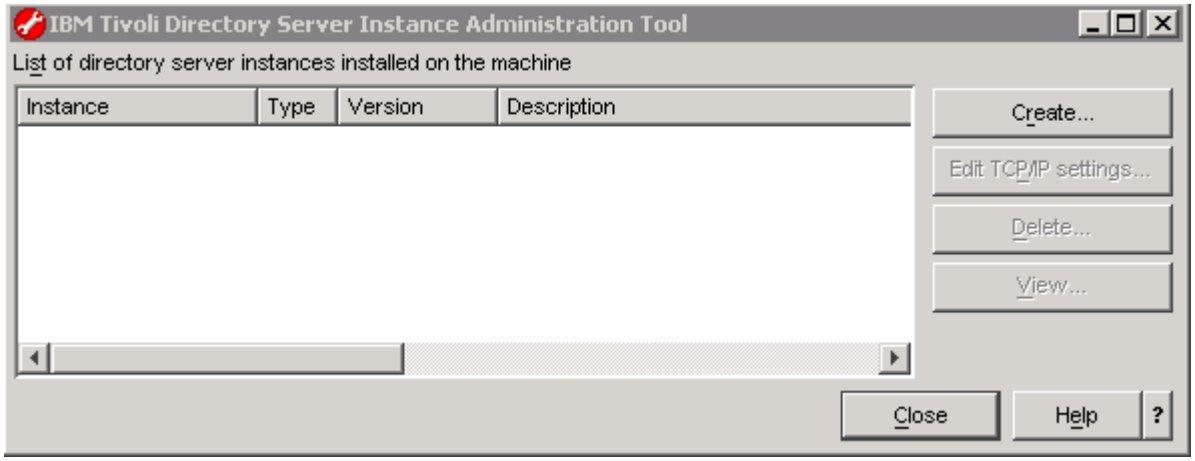
____ 18. Click the **Close** button to quit the IBM Tivoli Directory Server Instance Administration Tool. Click the **Yes** button to confirm

____ 19. Click the **Finish** button to exit the Tivoli Directory Server V6.0 installation wizard

→ Creating a new Tivoli Directory Server Instance

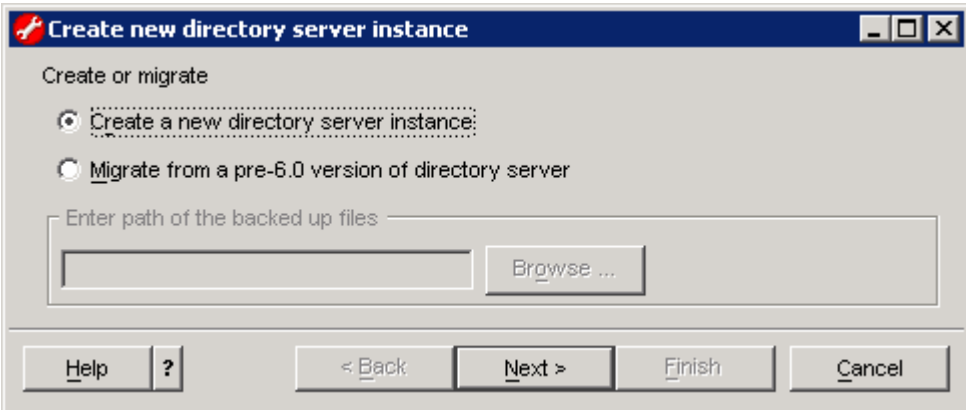
In the part of the lab, you will create a Tivoli Directory Server instance and then configure it.

____ 1. Launch the IBM Tivoli Directory Server Instance Administration Tool, from Start → Programs → IBM Tivoli Directory Server 6.0 → Instance Administration tool (Instance Administration Tool)



____ 2. Click the **Create** button

____ 3. The **Create new directory server instance** wizard is launched. Select the radio button next to **Create a new directory server instance**



____ 4. Click **Next**

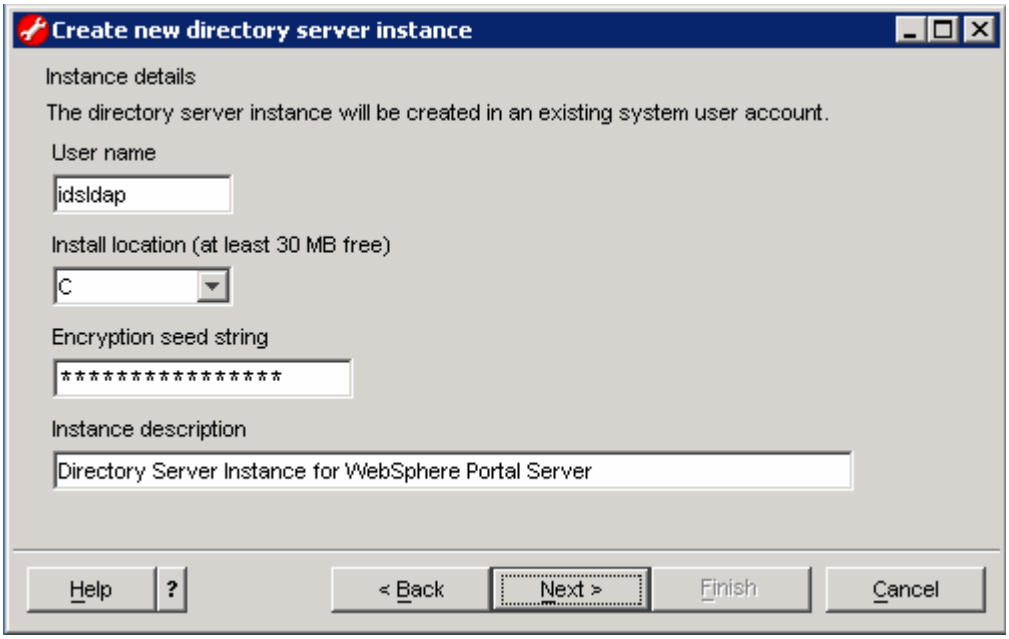
____ 5. In the following **instance details** panel, enter the following information:

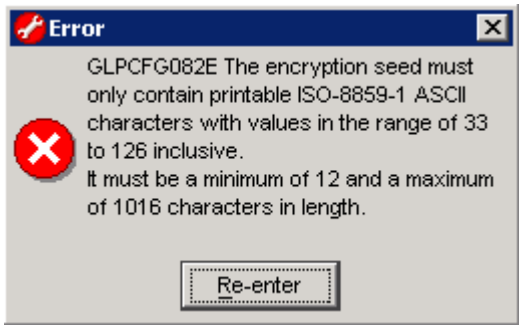
__ a. User name : **idsldap**

__ b. Install location : **C** (default)

__ c. Encryption seed string : **monitorserversecurity** (Note : 13 chars or more)

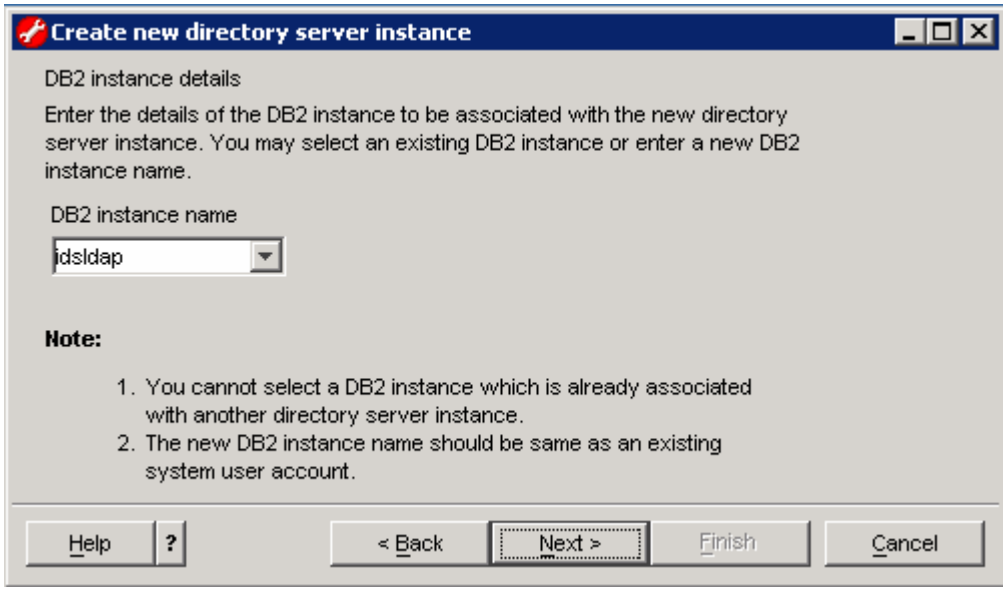
__ d. Instance Description : Directory Server Instance for WebSphere Portal Server





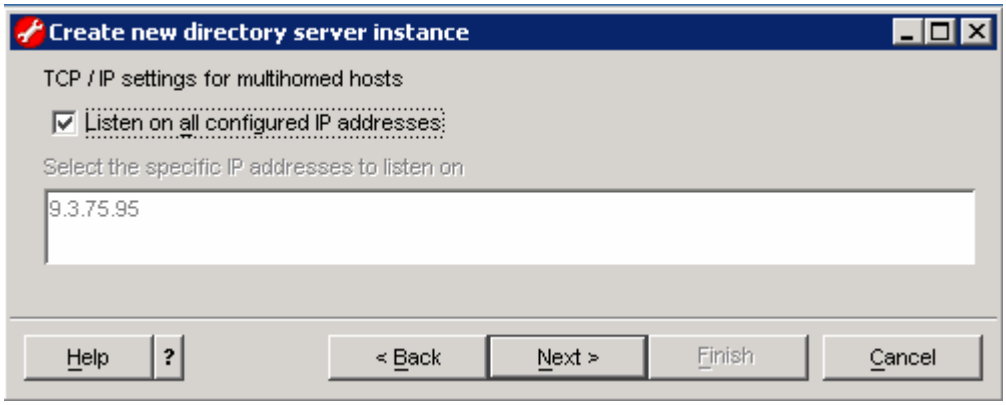
____ 6. Click **Next**

____ 7. In the following **DB2 instance details** panel, select **idsldap** as the **DB2 instance name** from the drop down list



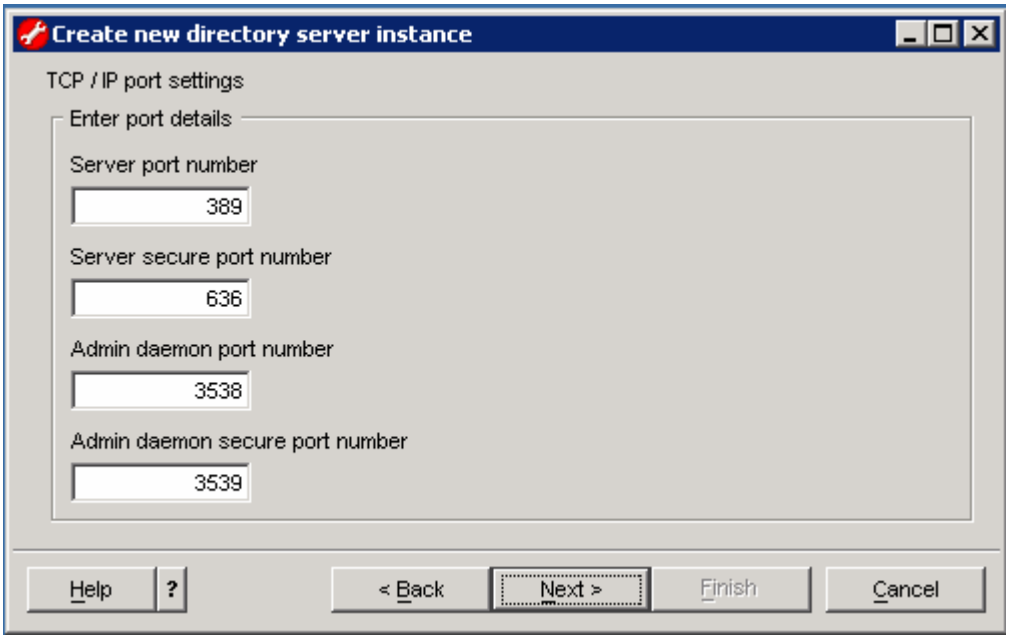
____ 8. Click **Next**

____ 9. Accept the defaults in the following **TCP/IP settings for multihomed** hosts panel



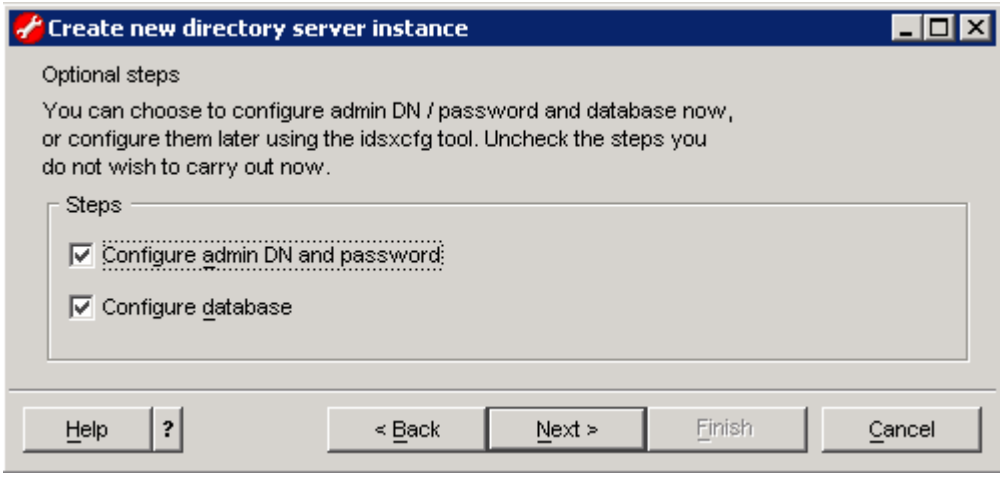
____ 10. Click **Next**

____ 11. In the following **TCP/IP ports settings** panel, accept the default port numbers



____ 12. Click **Next**

____ 13. In the following **Optional steps** panel, ensure the two check boxes are selected



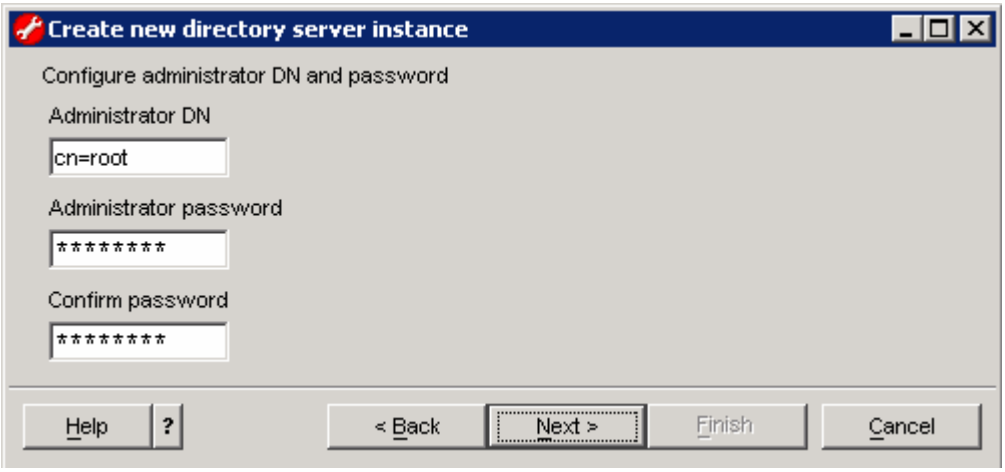
____ 14. Click **Next**

____ 15. In the following **Configure administrator DN and password** panel, enter the following information:

__ a. Administrator DN : **cn=root**

__ b. Administrator password : **ldapadmin**

__ c. Confirm password : **ldapadmin**



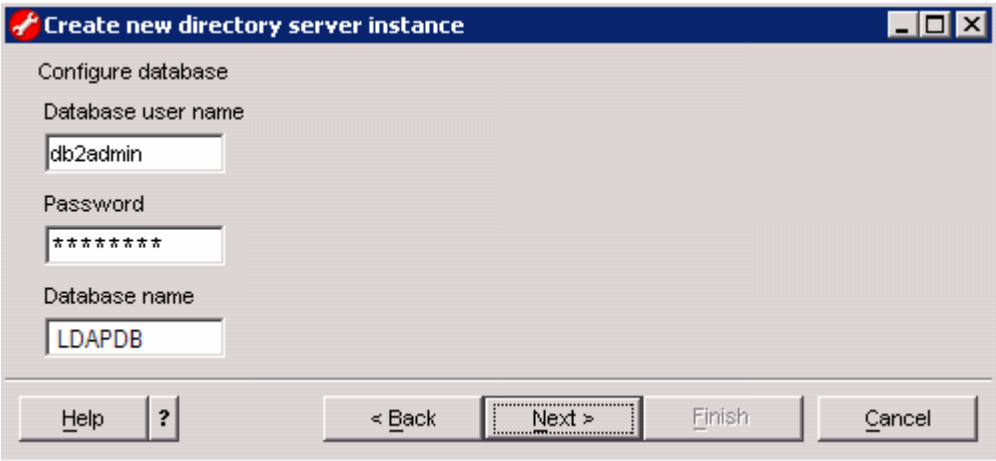
____ 16. Click **Next**

____ 17. In the following **Configure database** panel, enter the following information:

__ a. Database user name : **db2admin**

__ b. Password : **db2admin**

__ c. Database name : **LDAPDB**

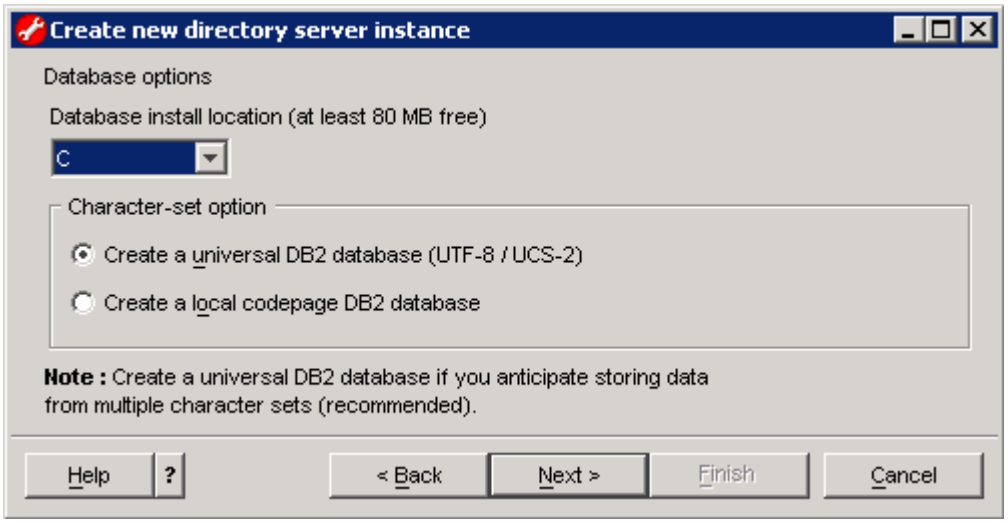


____ 18. Click **Next**

____ 19. In the following **Database options** panel, complete the following instructions:

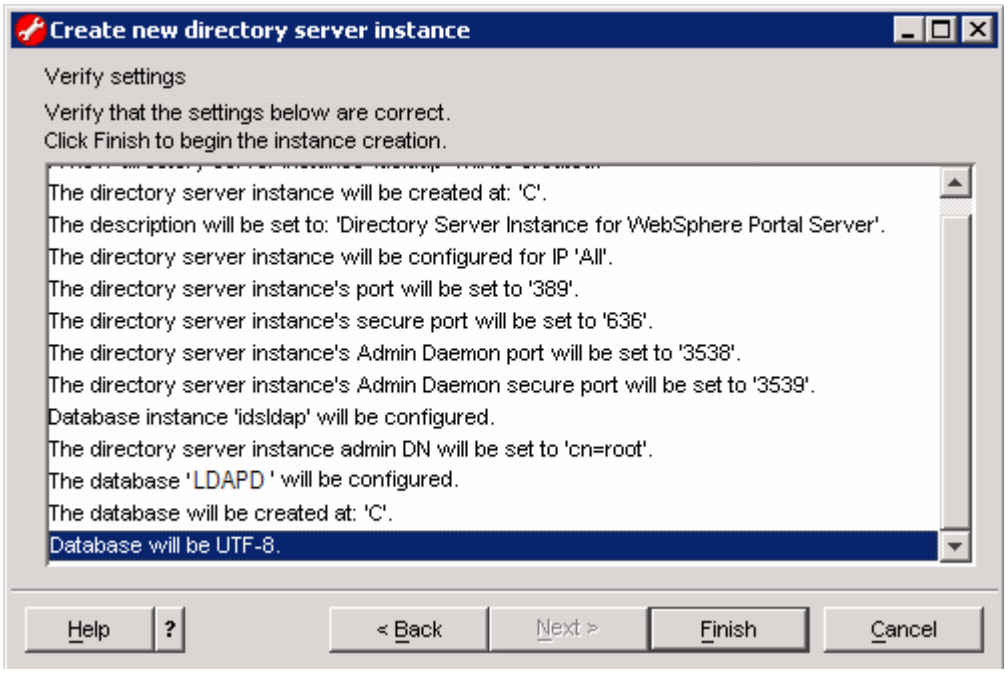
__ a. Select **C** drive as the **Database install location**

__ b. Select the radio button next to **Create a universal DB2 database** for the Character-set option



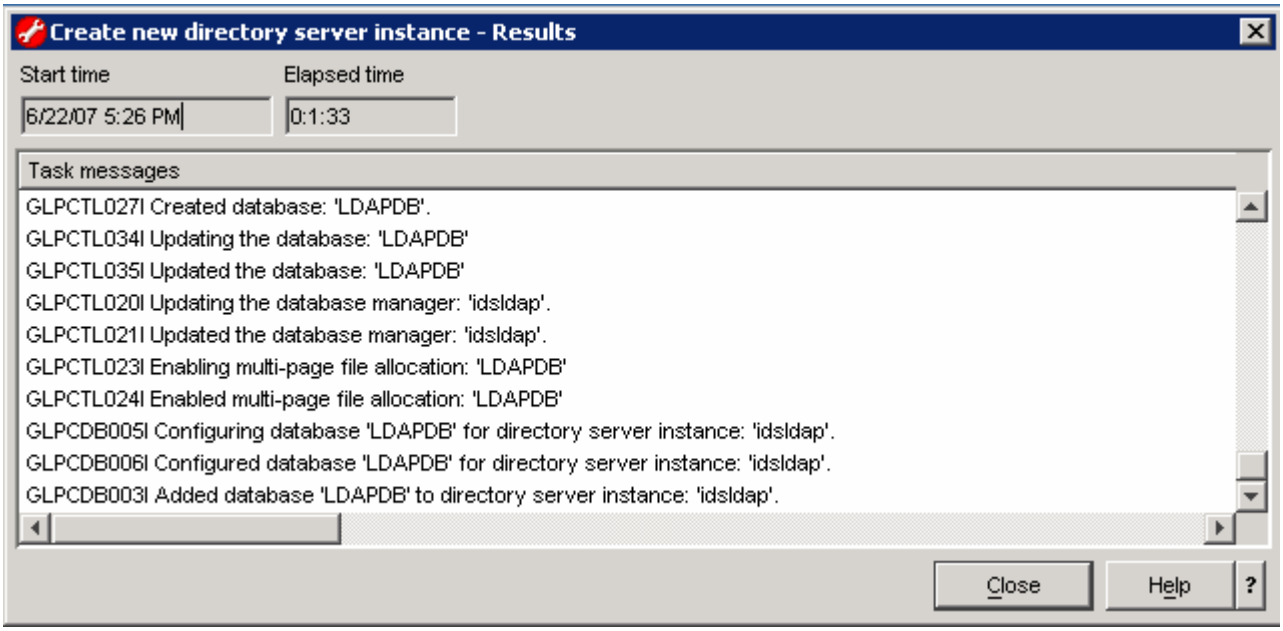
____ 20. Click **Next**

____ 21. Verify the settings in the following panel

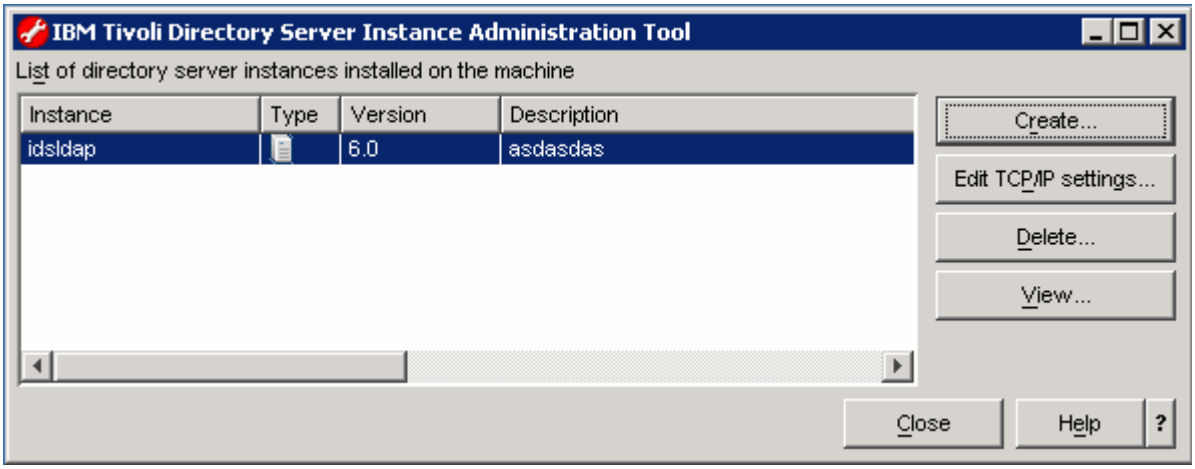


____ 22. Click the **Finish** button

____ 23. Ensure the Directory Server Instance is successfully created



____ 24. Click the **Close** button



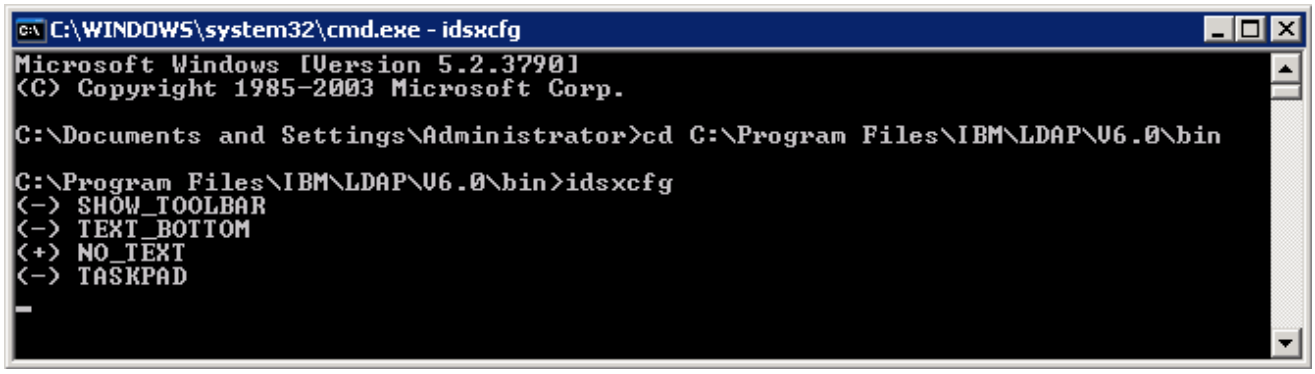
____ 25. Close the IBM Tivoli Directory Server instance Administration Tool

→ Configuring IBM Tivoli Directory Server

____ 1. To configure the directory server with Portal users, you will import the LDIF file.

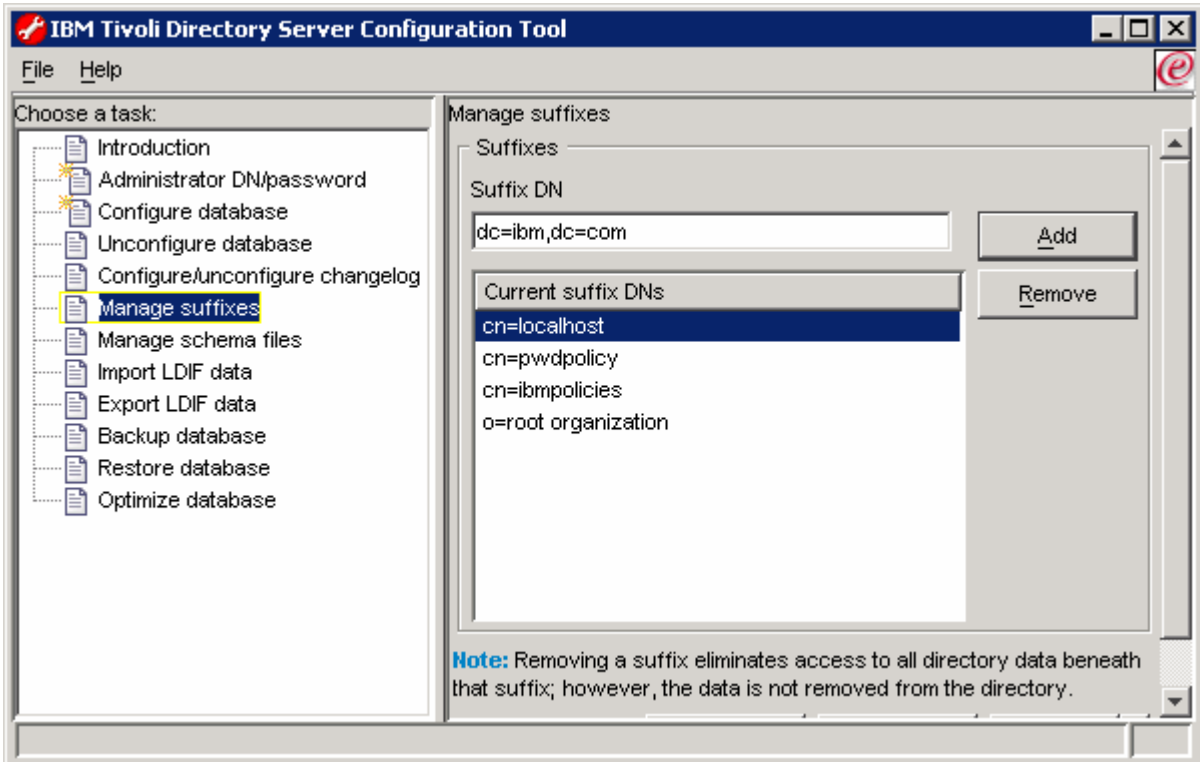
__ a. Open a command line window and change the directory to **C:\Program Files\IBM\LDAP\V6.0\bin**

__ b. Run the **idsxcfg** command to open the IBM Tivoli Directory Server Configuration Tool

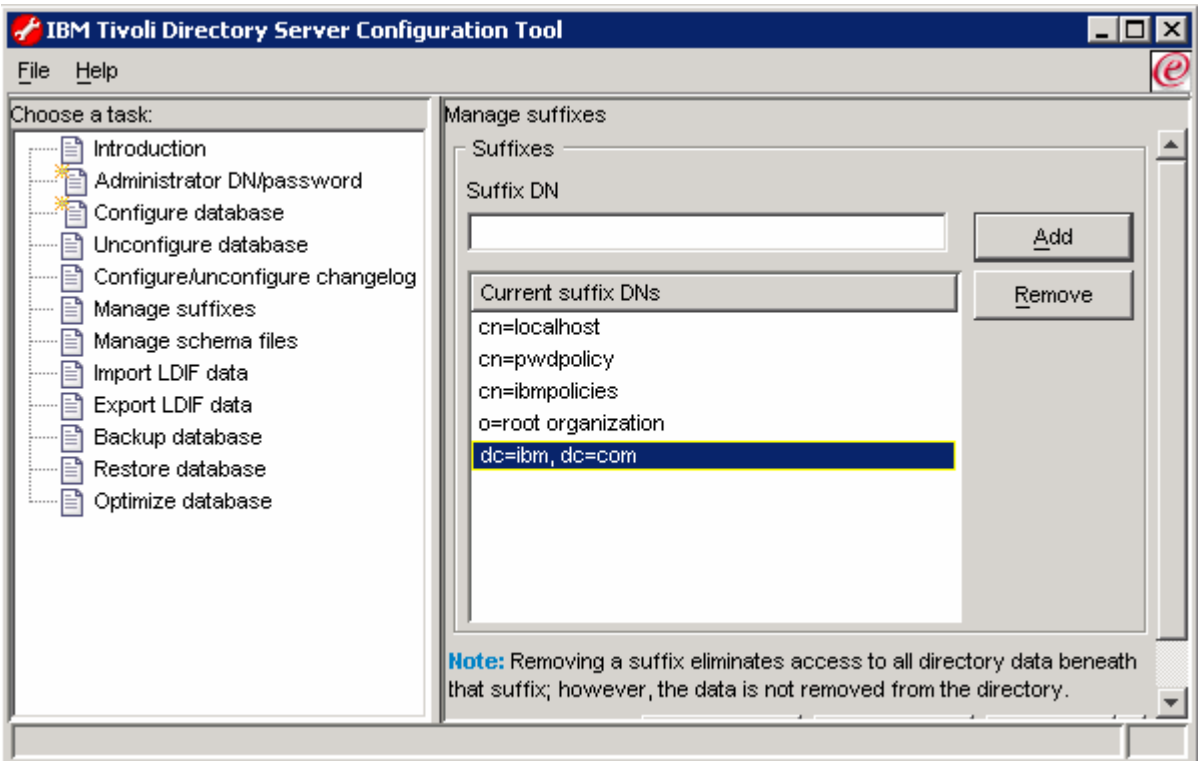


__ c. In the configuration Tool, click **Manage suffixes** in the task list on the left pane. The **Manage suffixes** window opens in the Right pane

__ d. In the **Manage Suffixes** window, type **dc=ibm,dc=com** in the **Suffix DN** field and click the **Add** button



Note: When you click the **Add** button, the suffix is added to the list in the **Current suffix DNs** text box; however, the suffix is not actually added to the directory until you click **OK**



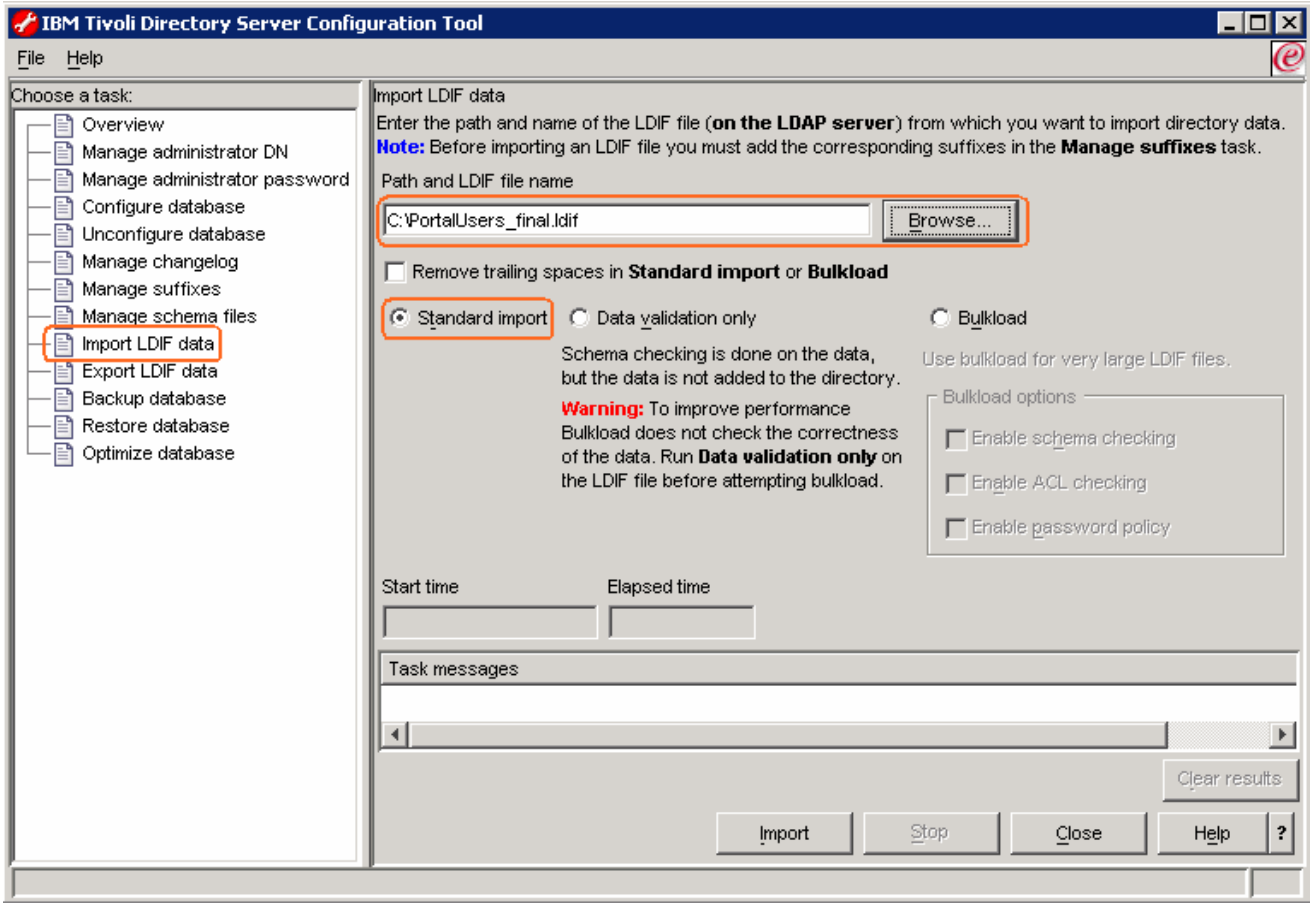
__ e. Click the **OK** button

____ 2. To import the Portal users, complete the following instructions:

__ a. In the Configuration Tool, click **Import LDIF data** in the task list on the left pane. The **Import LDIF data** window opens in the Right pane

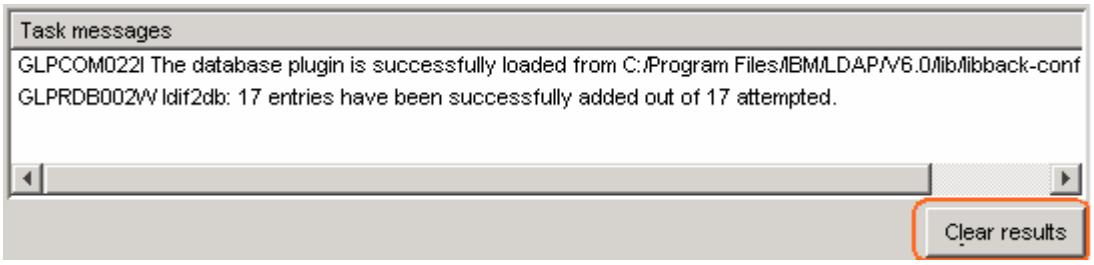
__ b. In the **Import LDIF data** window on the right, click the **Browse** button to locate the LDIF file that consists of the portal users

__ c. Ensure the radio button next to **Standard Import** is selected



__ d. Click the **Import** button

__ e. Ensure that all the entries in the LDIF file are imported successfully as shown in the **Task Messages** text area and click the **Clear results** button



__ f. Close the IBM Tivoli Directory Server Configuration Tool by selecting **File → Close** from the main menu. Click the **Yes** button to confirm

____ 3. Start the Tivoli Directory Server. To start the IBM Tivoli Directory Server from the Windows **Services** by right clicking on "IBM Tivoli Directory Server"

____ 4. The Configuration is complete

Part 2: Securing the Portal Server with Tivoli Directory Server V6.0

If WebSphere Application Server global security is enabled, you must disable it before modifying your security configuration. By default the WebSphere Application Server Global Security and Portal Server security is enabled internally during the installation for security reasons. So before trying to enable LDAP security for Portal Server, the WebSphere Application Server global security and the Portal Security turned off.

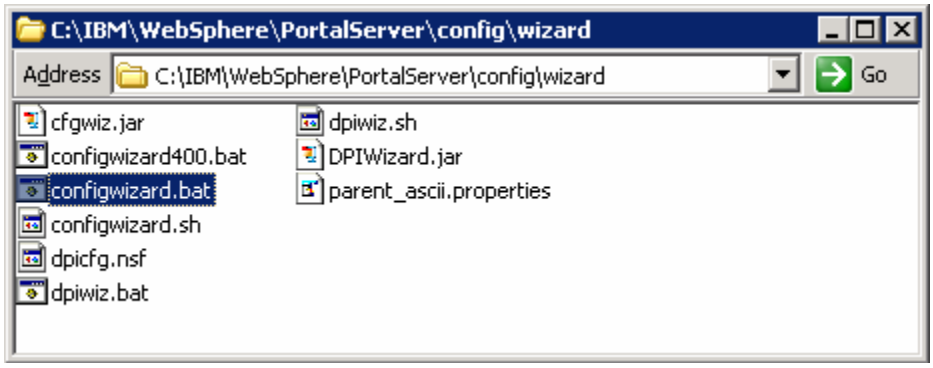
The following are the steps to turn off WebSphere Application Server Global Security and disable WebSphere Portal security.

→ Disable WebSphere Application Server and Portal security:

The following steps must be completed on the machine designated for Portal Server:

____ 1. Start the WebSphere Application Server (**server1**) and the WebSphere Portal Server (**WebSphere_Portal**)

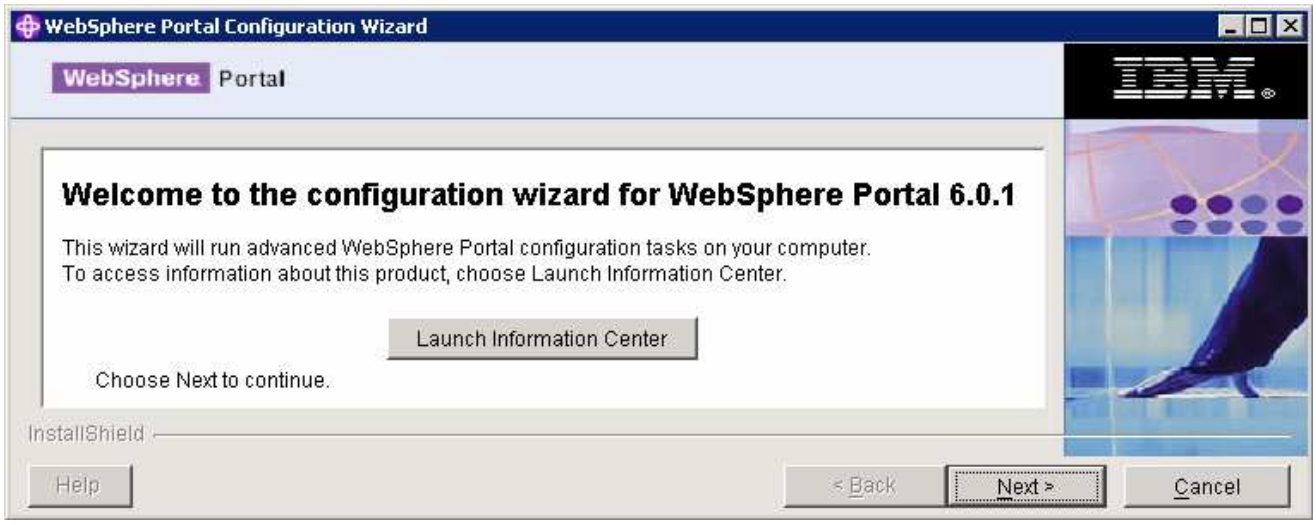
__ a. On the Portal Server machine, locate the **config/wizard** directory (**C:\IBM\WebSphere\PortalServer\config\wizard**)



__ b. Double click the **configwizard.bat** to launch the Portal Server Configuration Wizard

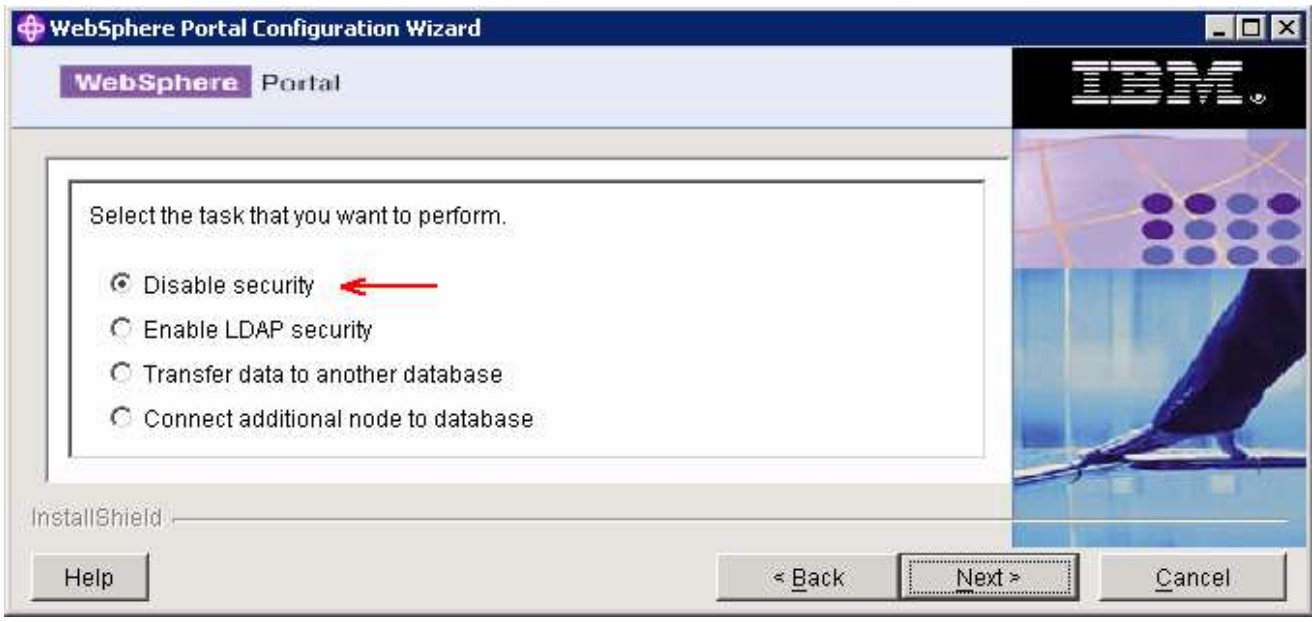
__ c. Select **English** as language

__ d. Click **OK**. The Configuration Wizard is launched



__ e. Click **Next** over the Welcome Screen

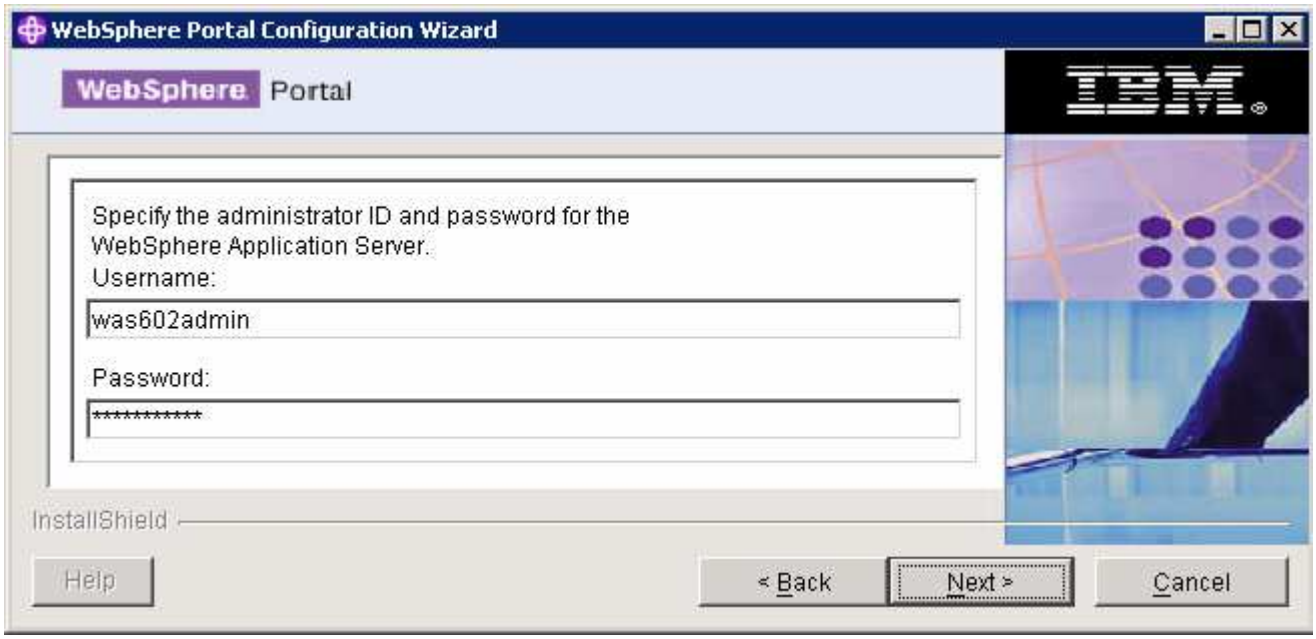
__ f. In the following panel, select the radio button next to **Disable Security**



__ g. Click **Next**

__ h. In the following panel, enter the WebSphere Application Server User ID and Password

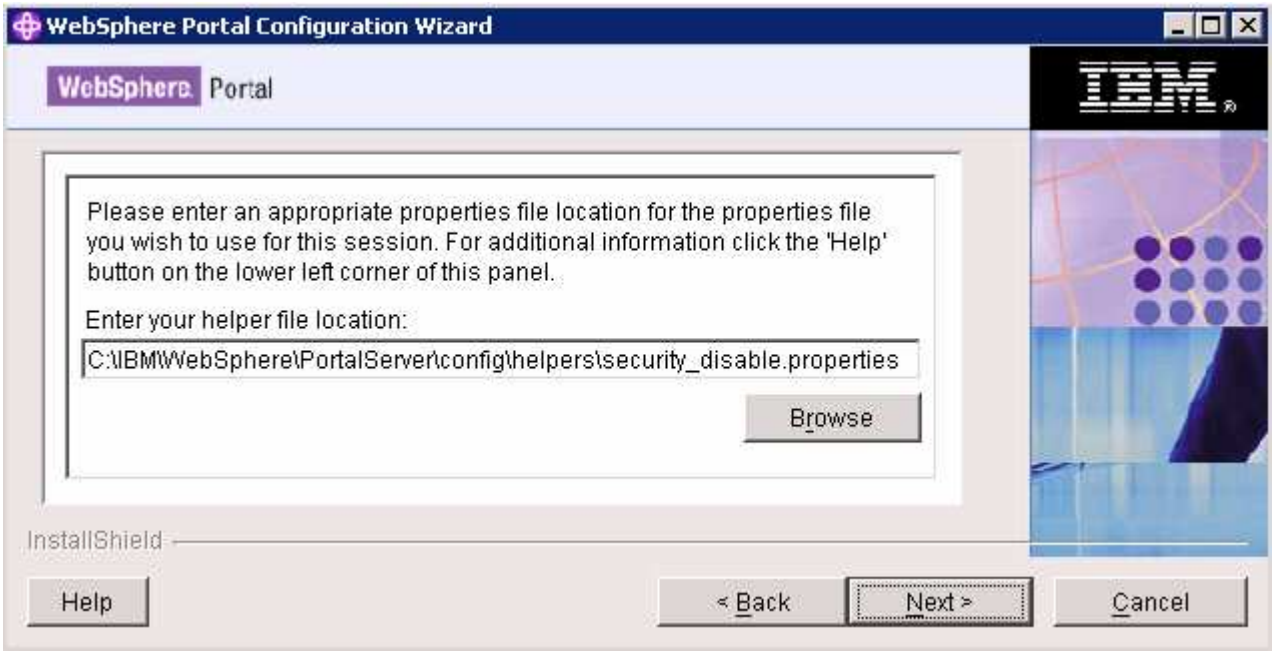
- **User ID :** was602admin
- **Password :** was602admin



__ i. Click **Next**

__ j. On a successful validation of the WebSphere Application Server, User and password, provide the **disable_security** helper file. This file is located at **<PORTAL_HOME>\config\helpers\security_disable.properties**

By default **<PORTAL_HOME>** is **C:\IBM\WebSphere\PortalServer**

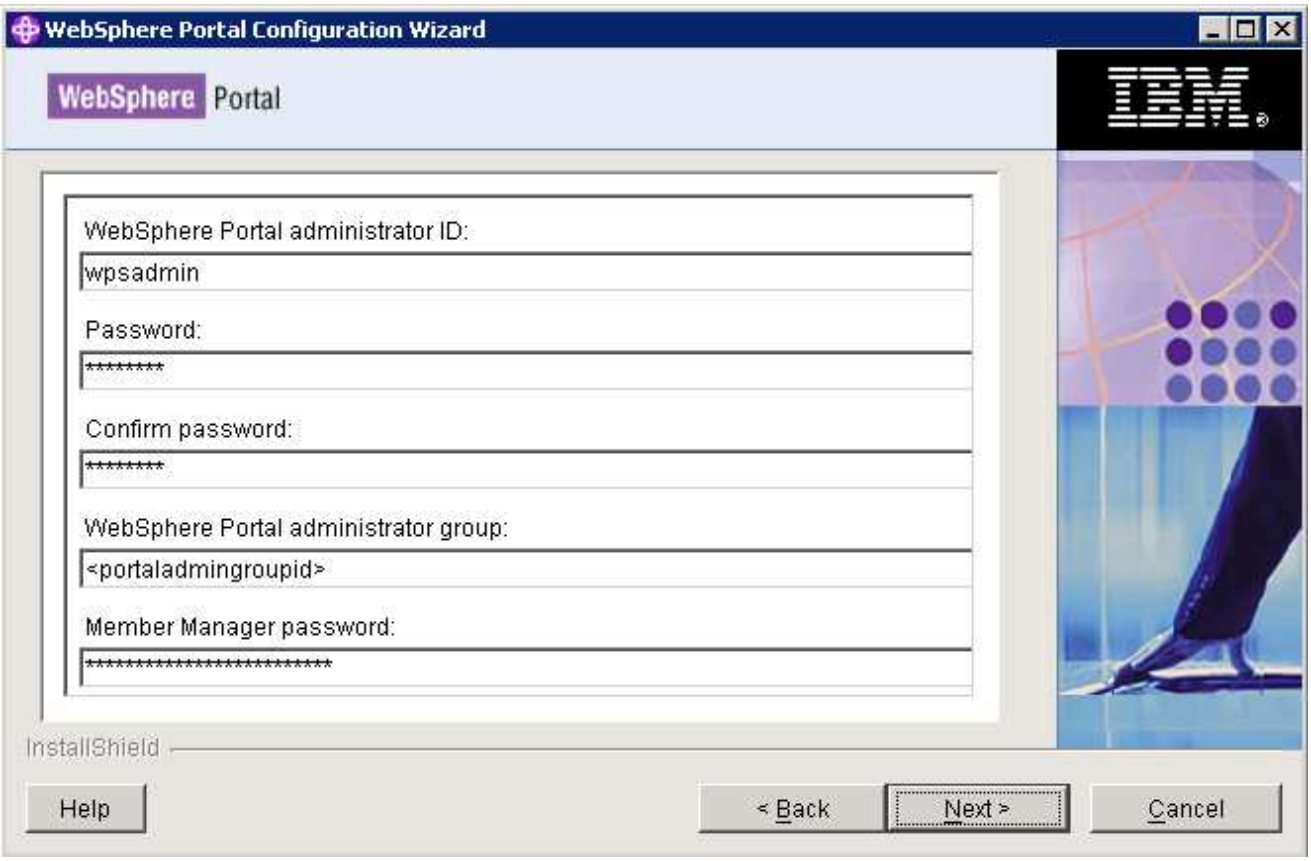


__ k. Click **Next**

__ l. In the following panel, enter the following values

- WebSphere Portal Administrator ID **: wpsadmin**

- Password **: wpsadmin**
- Confirm Password **: wpsadmin**
- WebSphere Portal administrator group **:** <Accept the default >
- Member Manager password : <Accept the default>

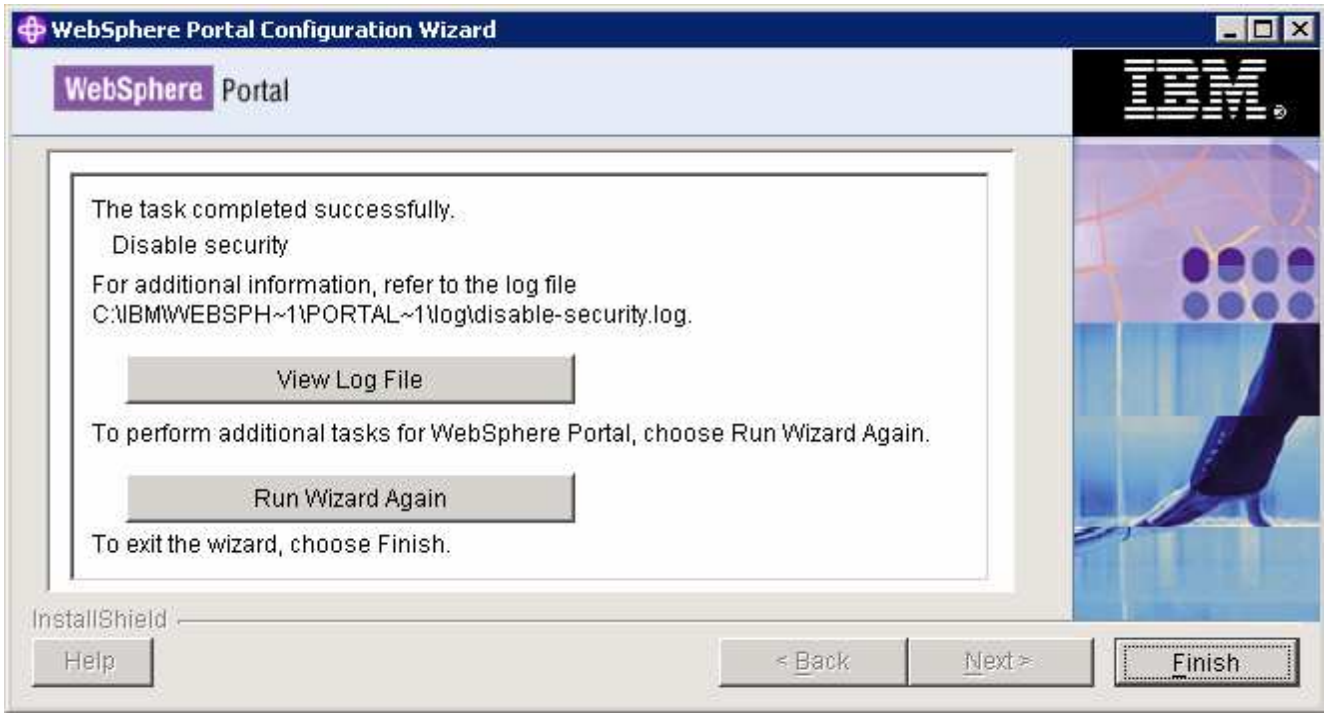


__ m. Click **Next**

__ n. Review the Summary

__ o. Click **Next**

__ p. The **Disable Security** task progresses. Monitor the configuration log file for any failure messages. The configuration log file is located at **<WPS_HOME>\logs\ConfigTrace.log**



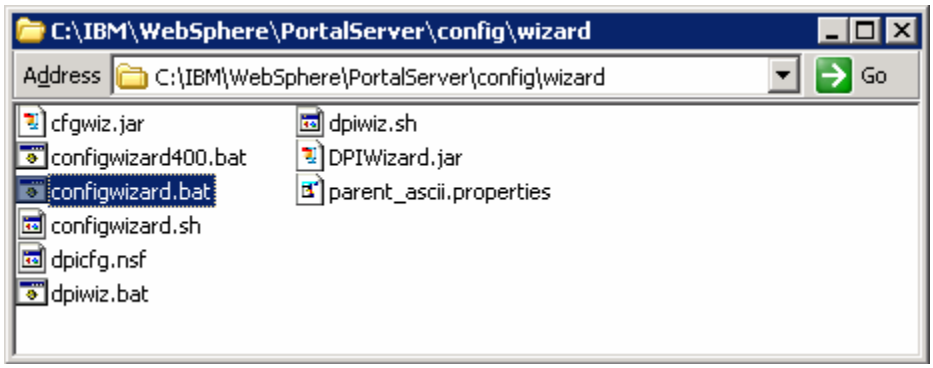
____ 2. Click **Finish**

____ 3. You have now disabled the WebSphere Application Server security and Portal Server security

→ Enable WebSphere Portal Security with LDAP:

____ 4. Start the WebSphere Application Server (**server1**) and the WebSphere Portal Server (**WebSphere_Portal**)

____ 5. On the Portal Server machine, locate the **config/wizard** directory (**C:\IBM\WebSphere\PortalServer\config\wizard**)

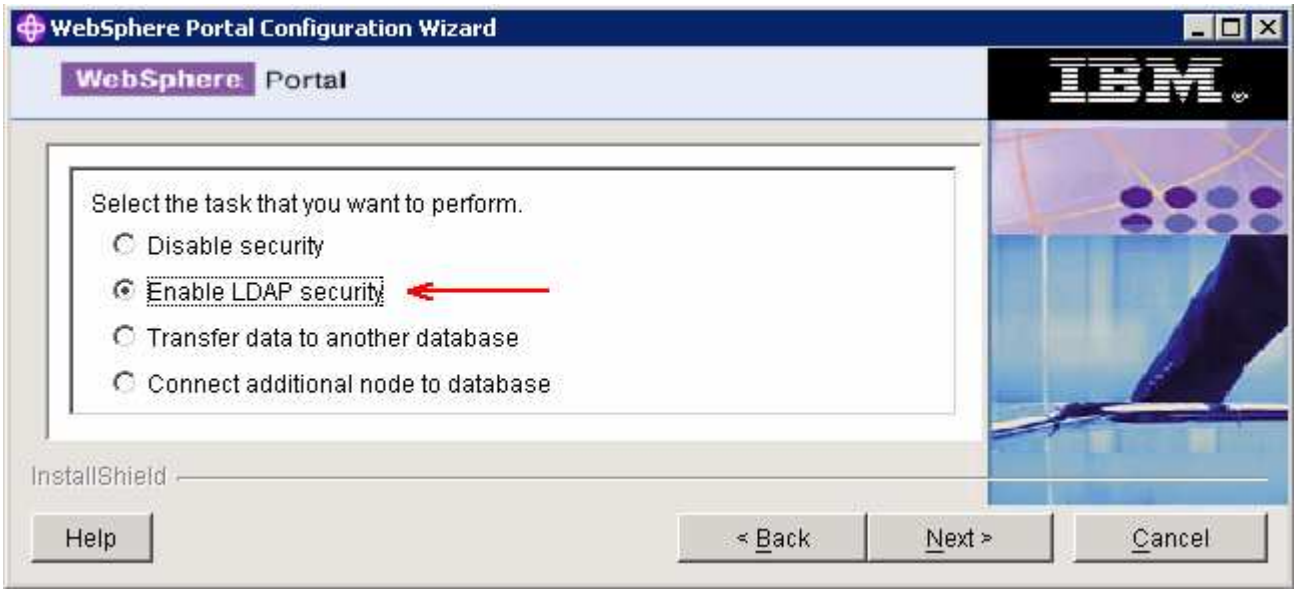


____ 6. Double click the **configwizard.bat** to launch the Portal Server Configuration Wizard

____ 7. Select **English** as language and click **OK**

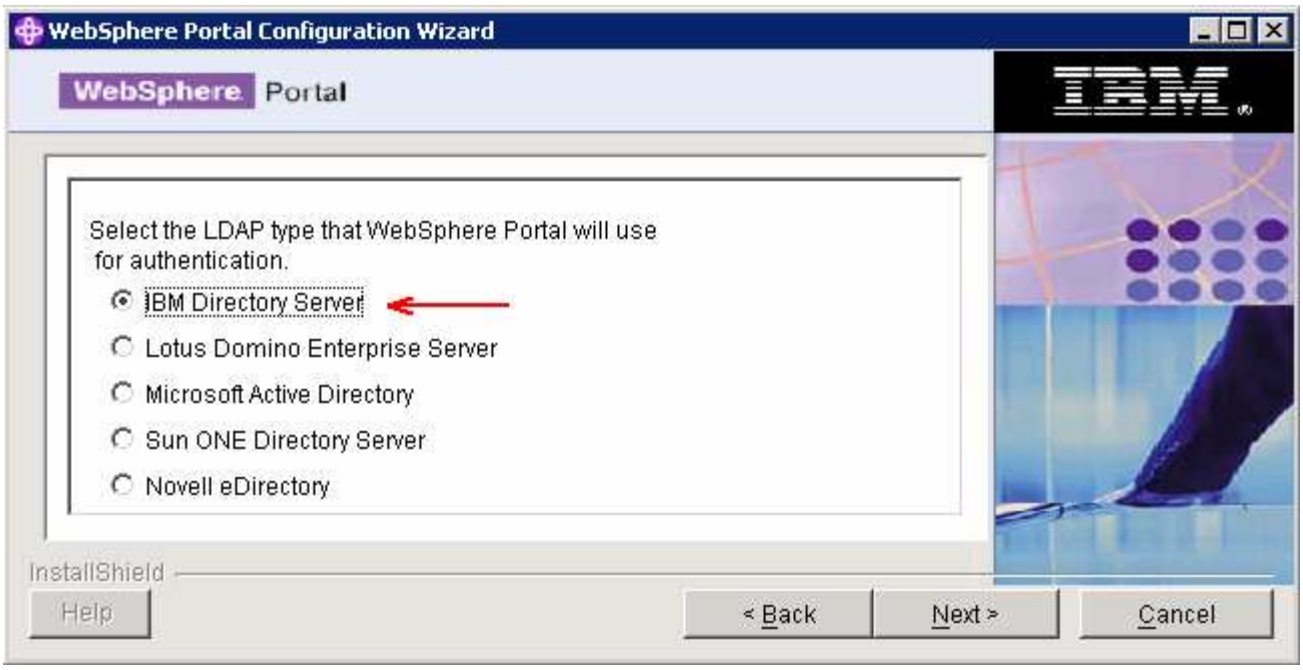
____ 8. Click **Next** over the Welcome Screen

____ 9. In the following panel, select the option, **Enable LDAP Security**



____ 10. Click **Next**

____ 11. Select the LDAP type as **IBM Directory Server**



____ 12. Click **Next**

____ 13. In the following panel, specify the LDAP settings to connect WebSphere Portal to LDAP server:

__ a. Host name : **<fully qualified LDAP sever host name>**

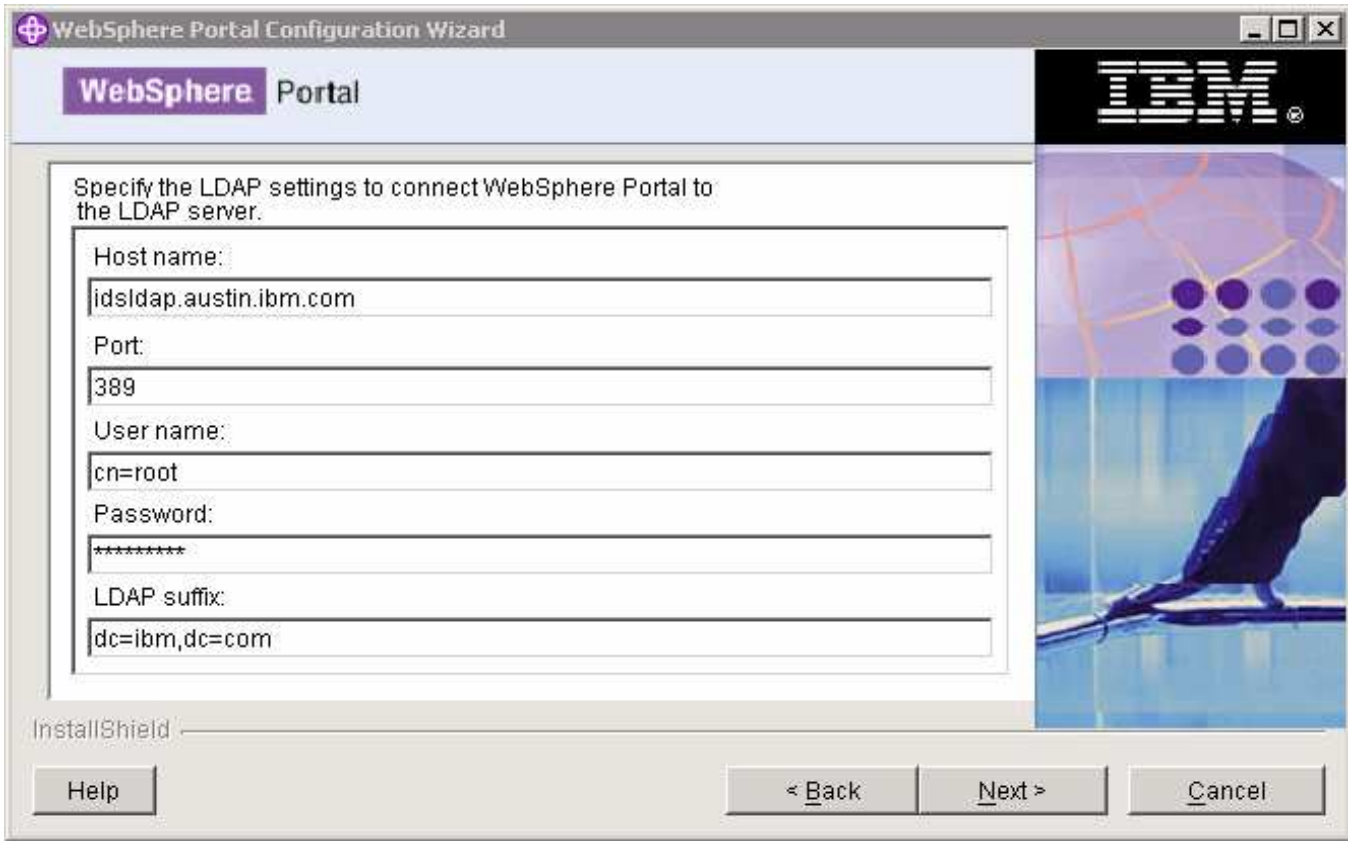
Example: idsldap.austin.ibm.com

__ b. Port : **389**

__ c. User name : **cn=root**

__ d. Password : **ldapadmin**

__ e. LDAP suffix : **dc=ibm,dc=com**



____ 14. Click **Next**

____ 15. In the following panel, specify the LDAP user settings for authenticating with the WebSphere Application Server and Portal Server:

__ a. WebSphere Portal administrator ID : **uid=wpsadmin,cn=users,dc=ibm,dc=com**

__ b. Password : **wpsadmin**

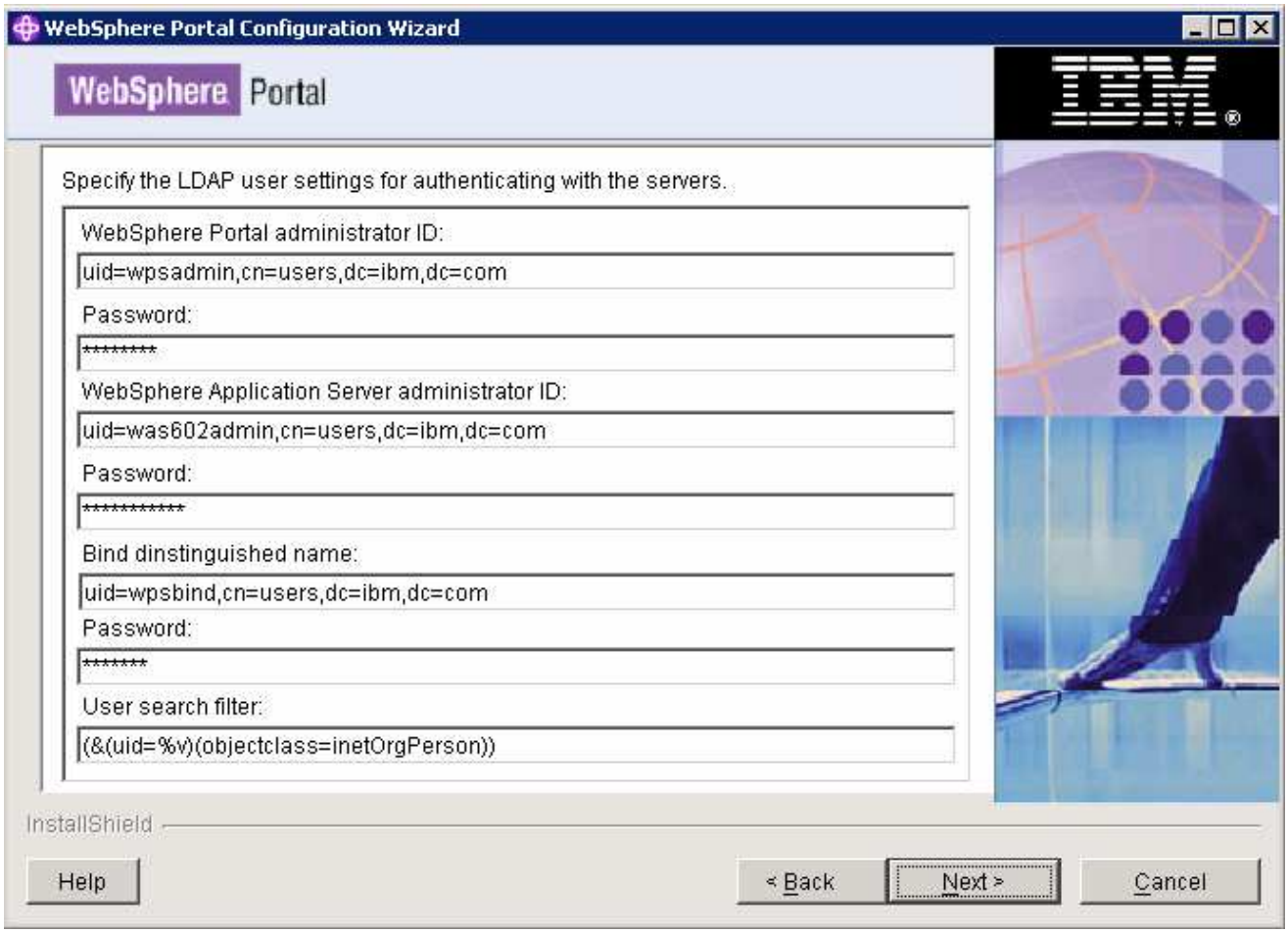
__ c. WebSphere Application Server administrator ID: **uid=was602admin,cn=users,dc=ibm,dc=com**

__ d. Password : **was602admin**

__ e. Bind Distinguished name : **uid=wpsbind,cn=users,dc=ibm,dc=com**

__ f. Password : **wpsbind**

__ g. User search filter : < Depends on your environment >



____ 16. Click **Next**

____ 17. In the following panel, specify the LDAP group settings for authenticating with the server:

__ a. WebSphere Portal administrator group : **cn=wpsadmins,cn=groups,dc=ibm,dc=com**

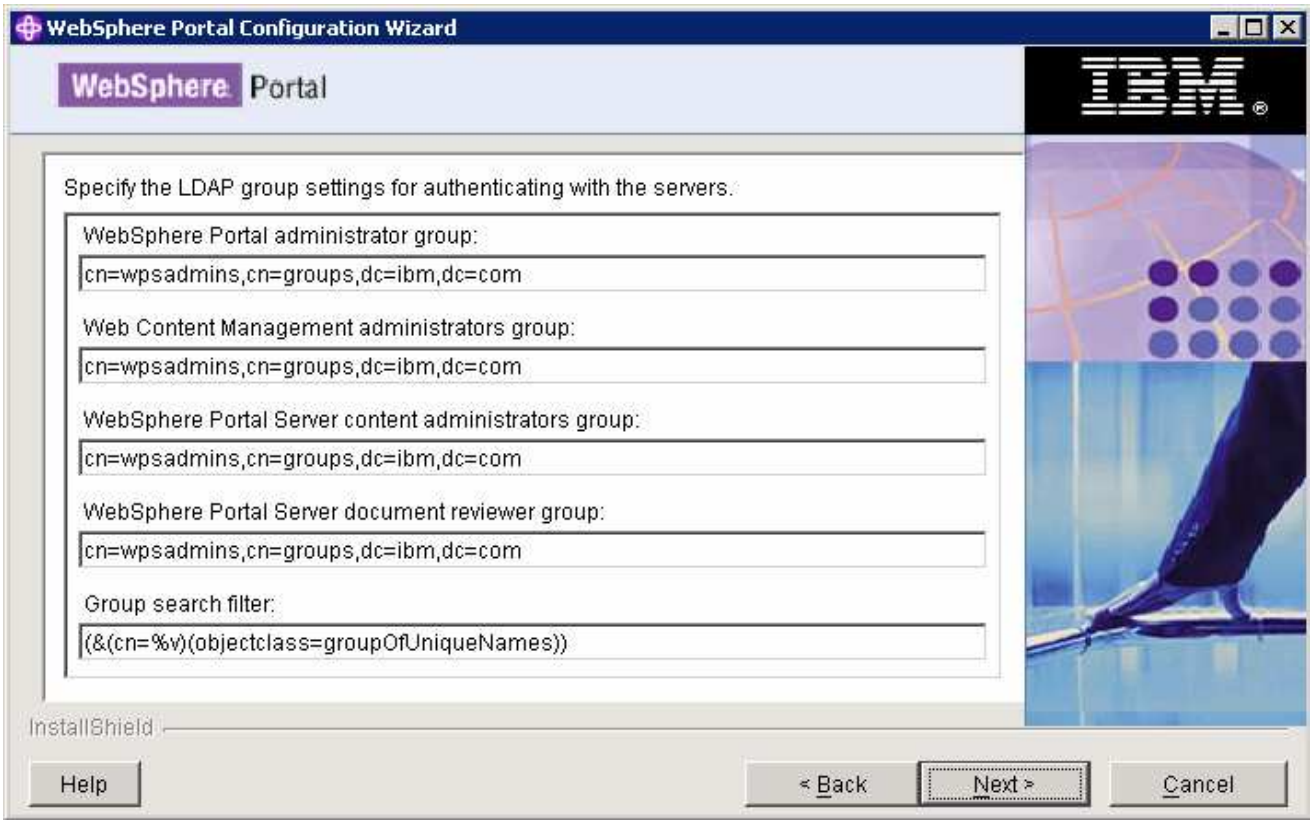
__ b. Web Content Management administrators group : **cn=wpsadmins,cn=groups,dc=ibm,dc=com**

__ c. Portal Server content administrators group : **cn=wpsadmins,cn=groups,dc=ibm,dc=com**

__ d. Portal Server document reviewer group : **cn=wpsadmins,cn=groups,dc=ibm,dc=com**

__ e. Group search filter : <Depends on your environment>

Note: To make it simple only one group, **wpsadmins,** is being used for all the Portal groups.



____ 18. Click **Next**

____ 19. In the following panel, specify the short names for the groups used in Web Content Management:

__ a. Web Content Management administrators group : **wpsadmins**

__ b. WebSphere Portal Server content administrators group : **wpsadmins**

__ c. Portal Server document reviewer group : **wpsadmins**

____ 20. Click **Next**

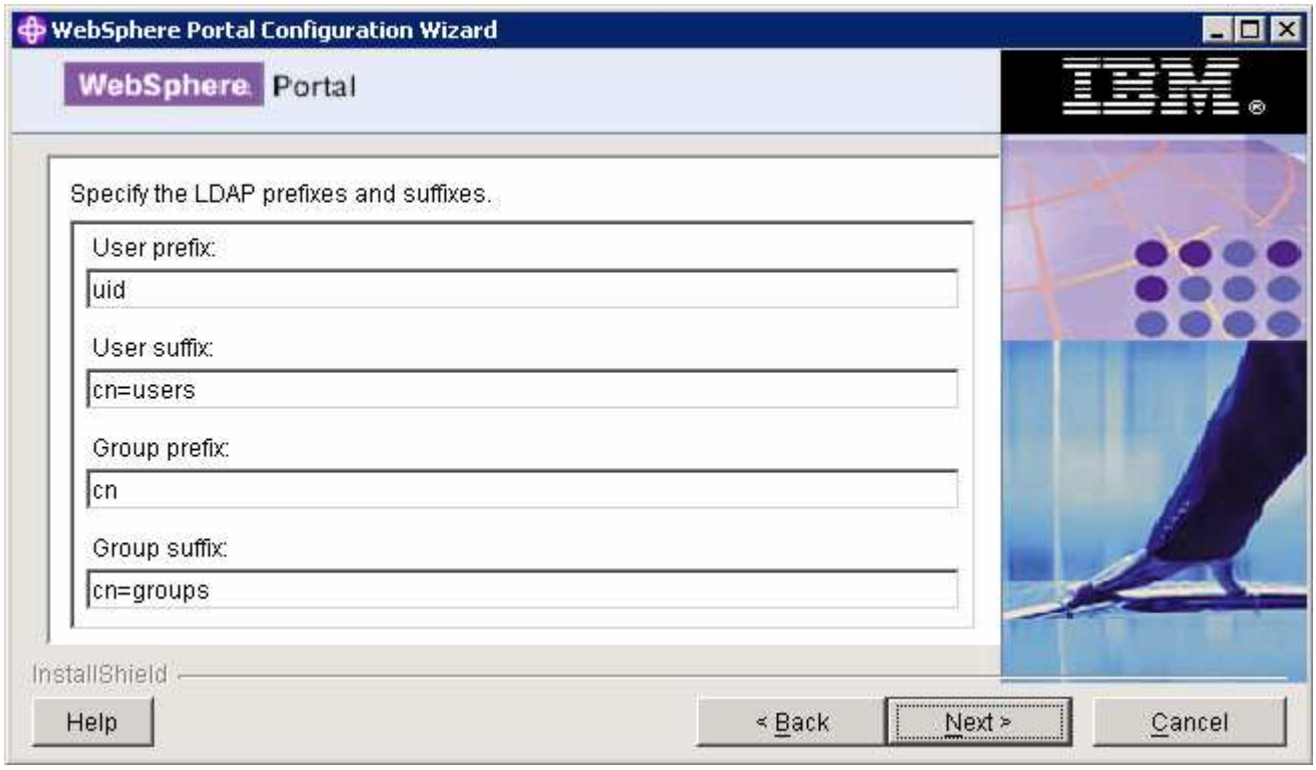
____ 21. In the following panel, specify the LDAP prefixes and suffixes:

__ a. User prefix : **uid**

__ b. User suffix : **cn=users**

__ c. Group prefix : **cn**

__ d. Group suffix : **cn=groups**



____ 22. Click **Next**

____ 23. In the following panel, specify the single sign-on settings:

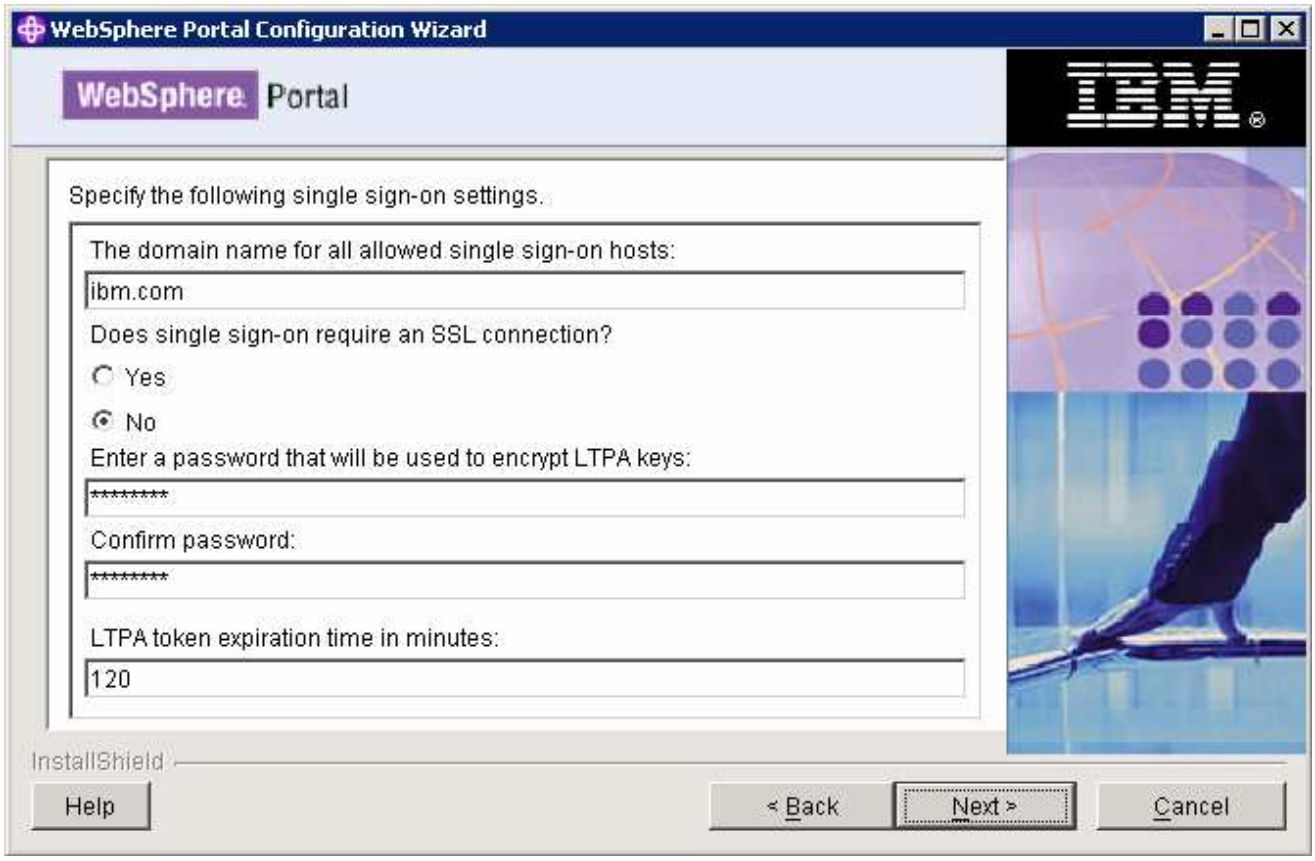
__ a. The domain name for all the single sign-on hosts : **ibm.com**

__ b. Does single sign-on require an SSL connection? : **No**

__ c. Enter a password that will be used to encrypt LTPA keys : **password**

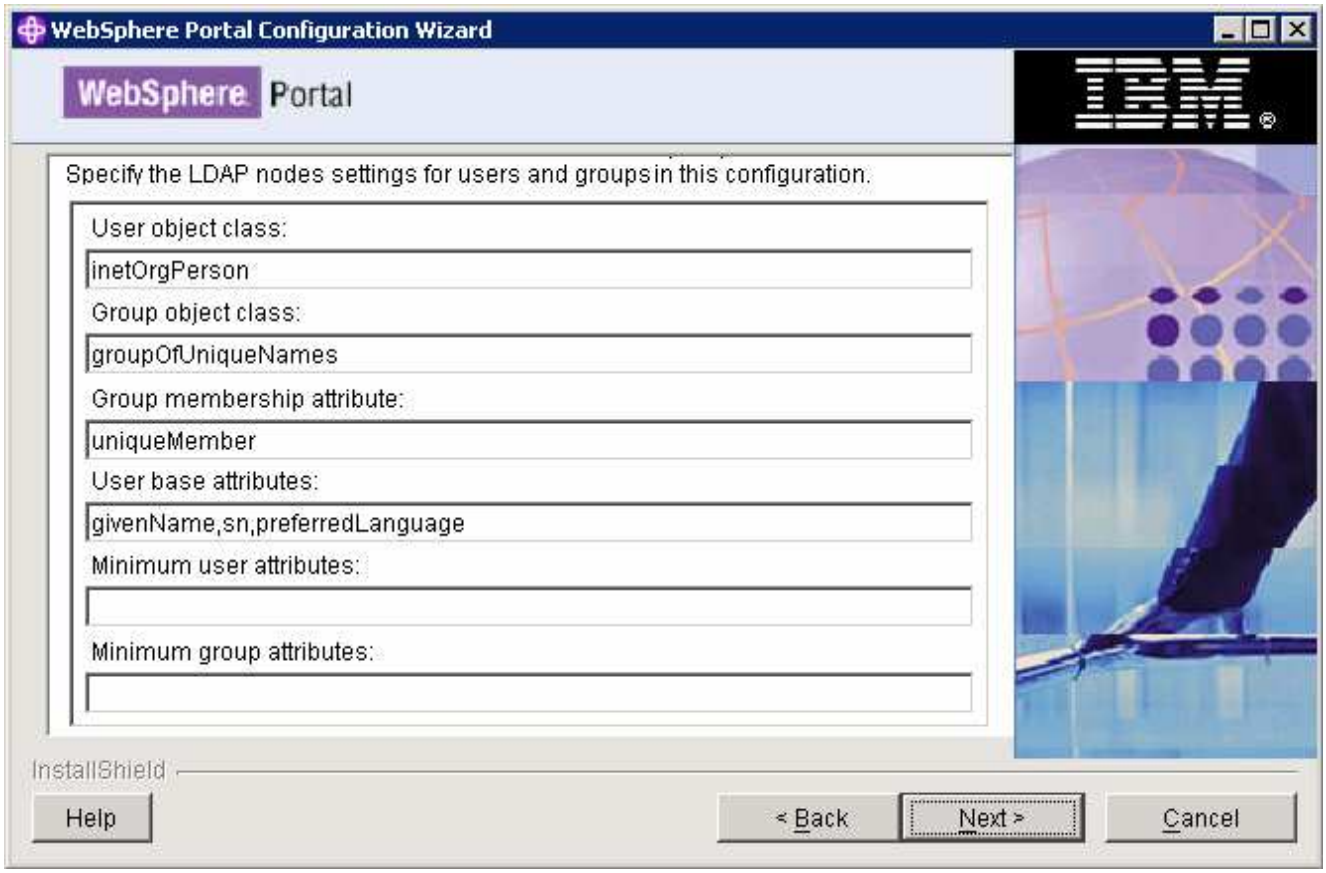
__ d. Confirm password : **password**

__ e. LTPA token expiration time in minutes : **120**



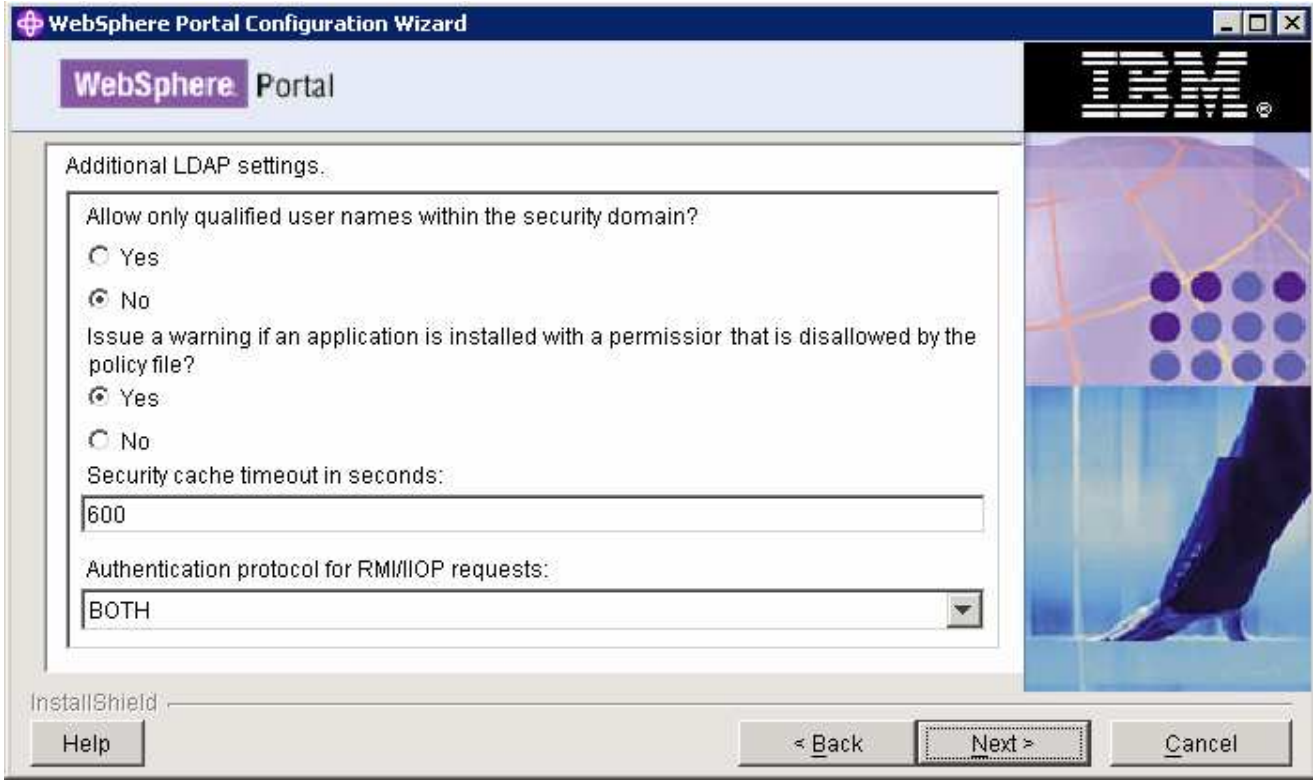
____ 24. Click **Next**

____ 25. In the following panel, accept the default parameters or specify the parameters as per your environment:



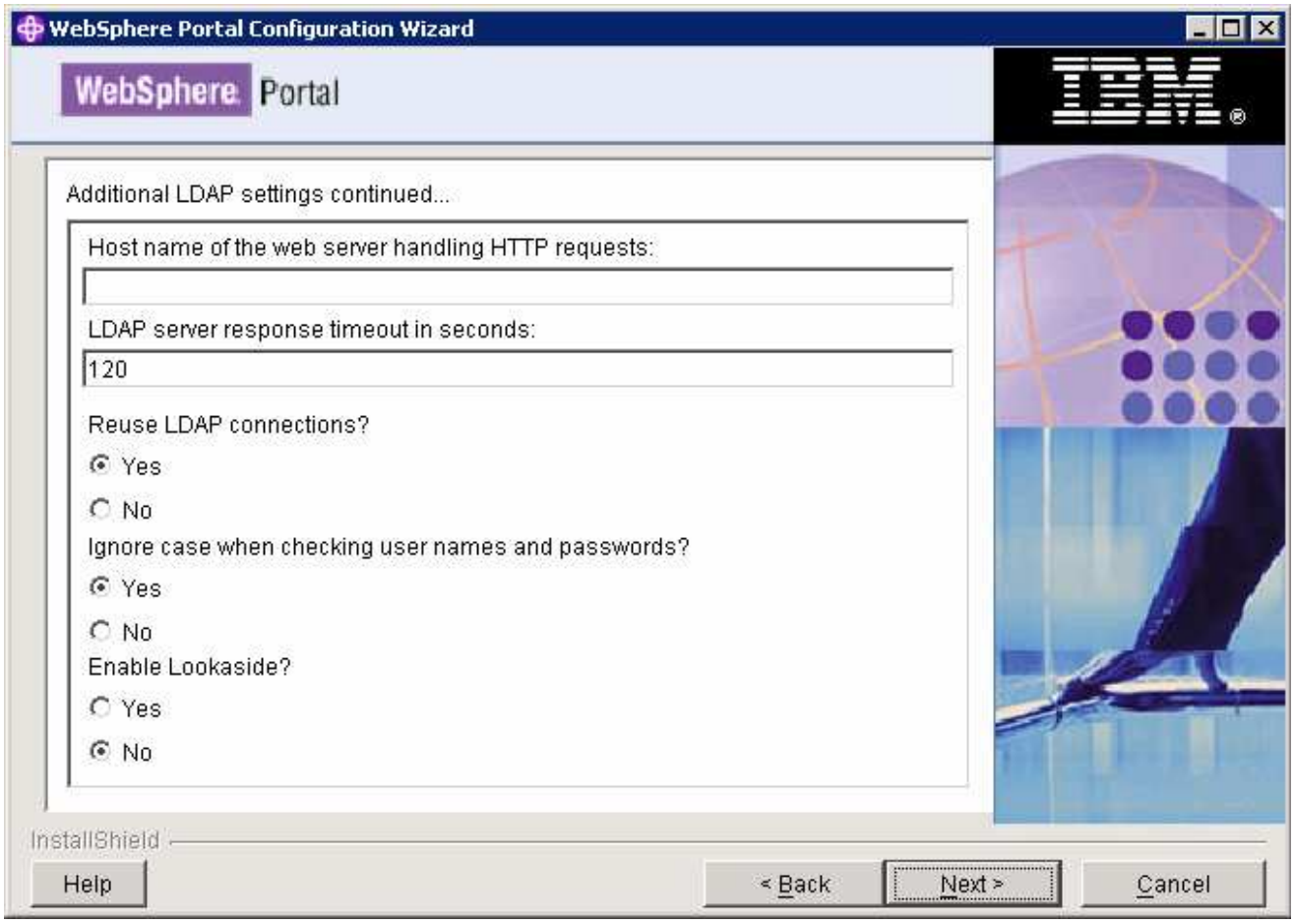
____ 26. Click **Next**

____ 27. In the following ‘Additional LDAP settings’ panel, accept the defaults:



____ 28. Click **Next**

____ 29. In the following panel, accept the defaults:

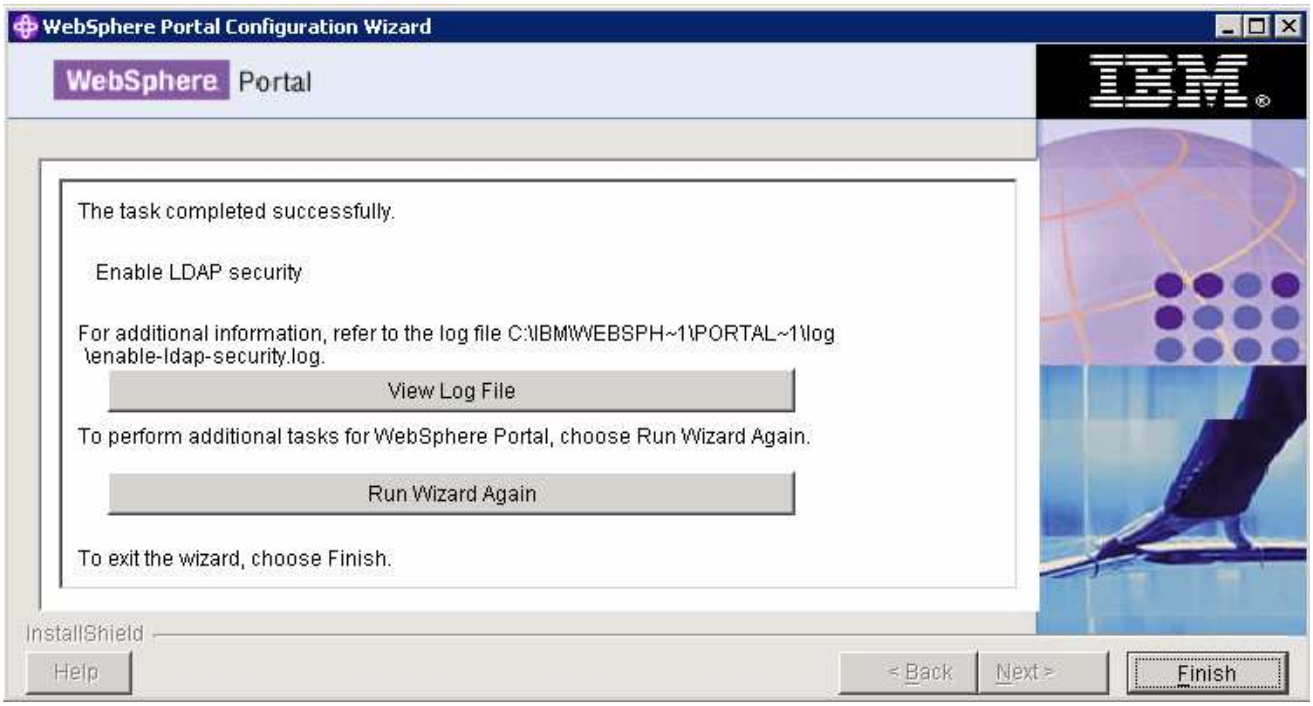


____ 30. Click **Next**

____ 31. In the following panel, review the summary:

____ 32. Click **Next**

____ 33. The **Enable LDAP** task progresses. Monitor the logs for any failure messages. The configuration log is located at **<PORTAL_HOME>\log\ConfigTrace.log**



____ 34. Once the Security configuration is complete, click **Finish**

____ 35. Restart the Portal Server and review the System Out log file and ensure the server is started successfully

____ 36. The Enable Security Task for Portal sever with Tivoli Directory Server is complete

____ 37. Export LTPA key file. You will be importing the exported key file across all the servers in the monitor domain

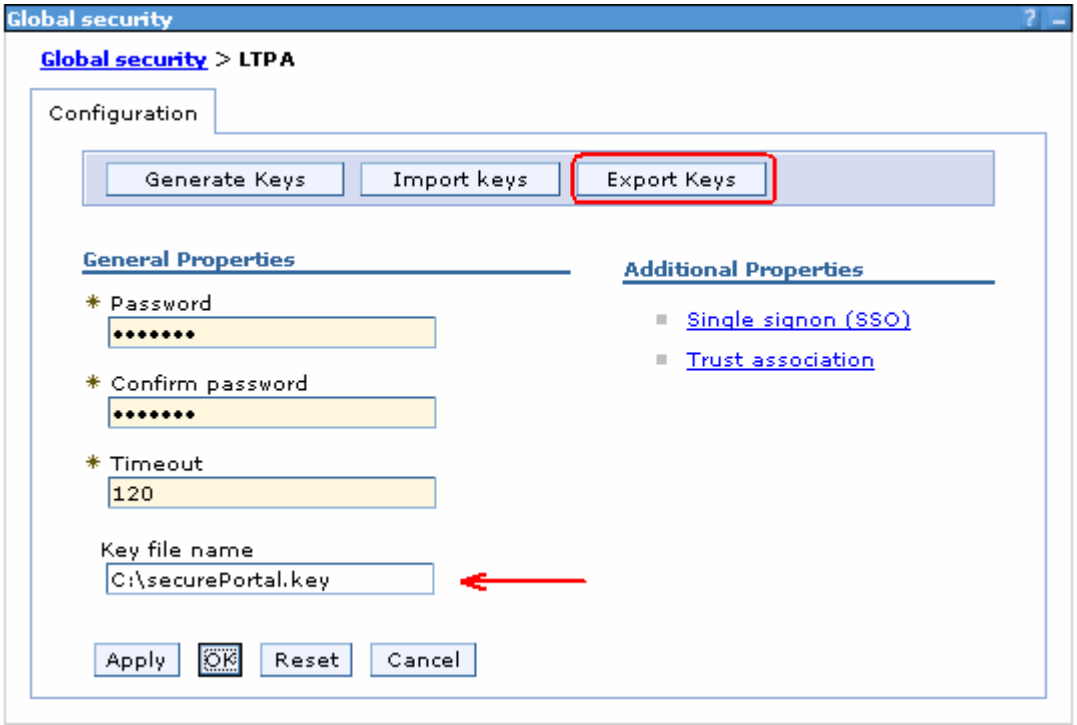
__ a. Launch the WebSphere Application Server admin console for the wp_profile: https://hostname:10039/ibm/console

__ b. Login to the administrative console using the user name and password (was602admin and was602admin)

__ c. In the left navigation pane of the administrative console, expand '**Security**' and click the '**Global security**' link

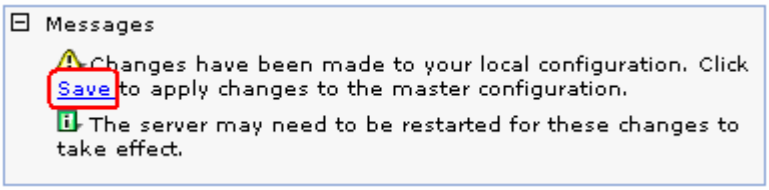
__ d. In the following panel, expand '**Authentication mechanisms**' under the '**Authentication**' category and click the '**LTPA**' link

__ e. In the following '**LTPA**' panel, enter the '**Key file name**' (Example: **C:\securePortal.key**)



__ f. Click the '**Export Keys**' button. This action exports a key file to the specified location

__ g. Click the **Save** link, to save the configuration



__ h. Click the **Save** button

____ 38. Close the administrative console

Part 3: Enable security for Monitor Server profile (WebSphere Application Server V6.1)

In this part of the lab, you will enable the LDAP security for Monitor Server which includes Web-based Dashboard and REST Server. In this process, you will configure WebSphere Application Server V6.1 to use LDAP in a federated repository.

Prerequisite:-

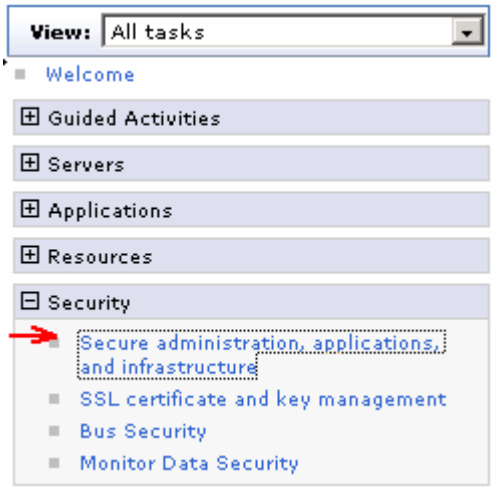
Copy the **securePortal.key** file that you have exported to a temporary location on to the Monitor Server machine

Complete the following instructions to enable LDAP security for the WebSphere Application Server, which is the Monitor Server profile

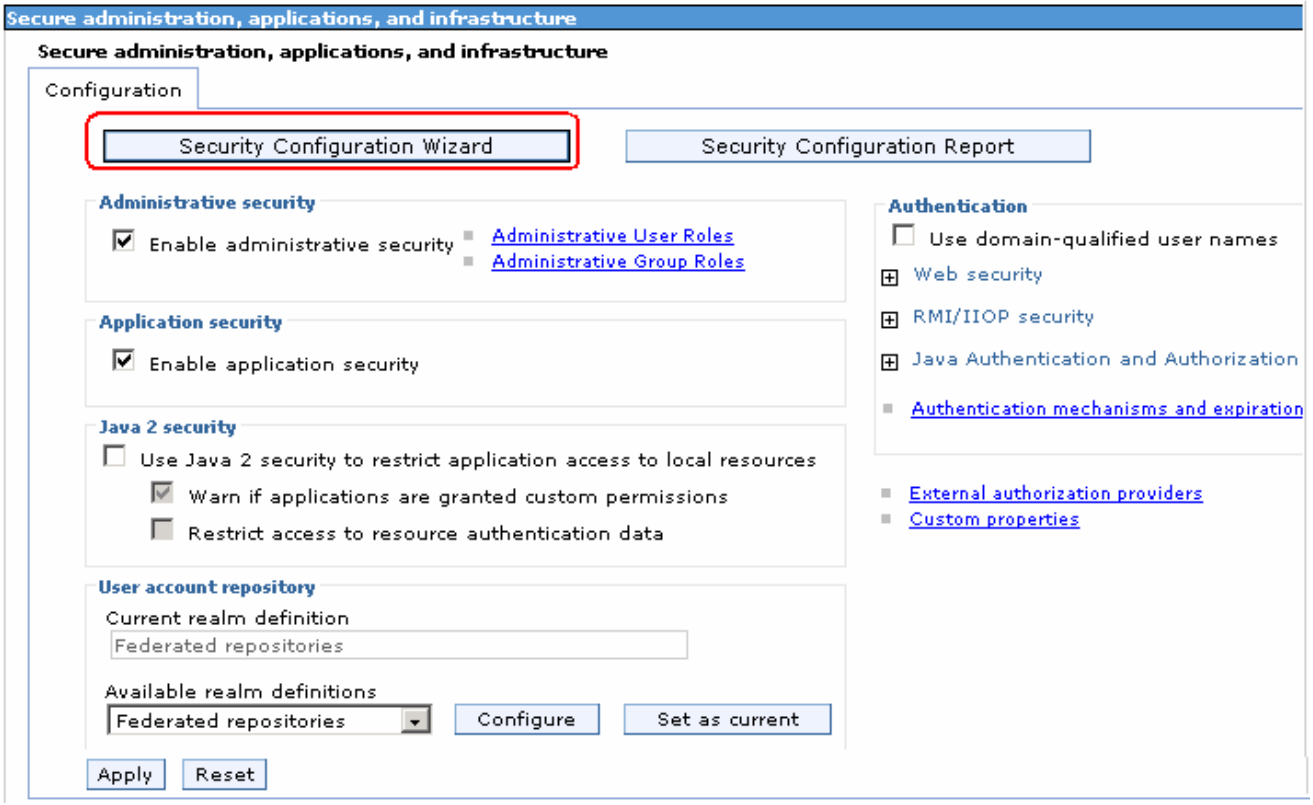
____ 1. Start the monitor server profile and launch the administrative console

____ 2. Login to the administrative console using the user name and password if the default security is enabled

____ 3. In the administrative console's left navigation pane, expand '**Security**' and click the '**Secure administration, applications and infrastructure**' link



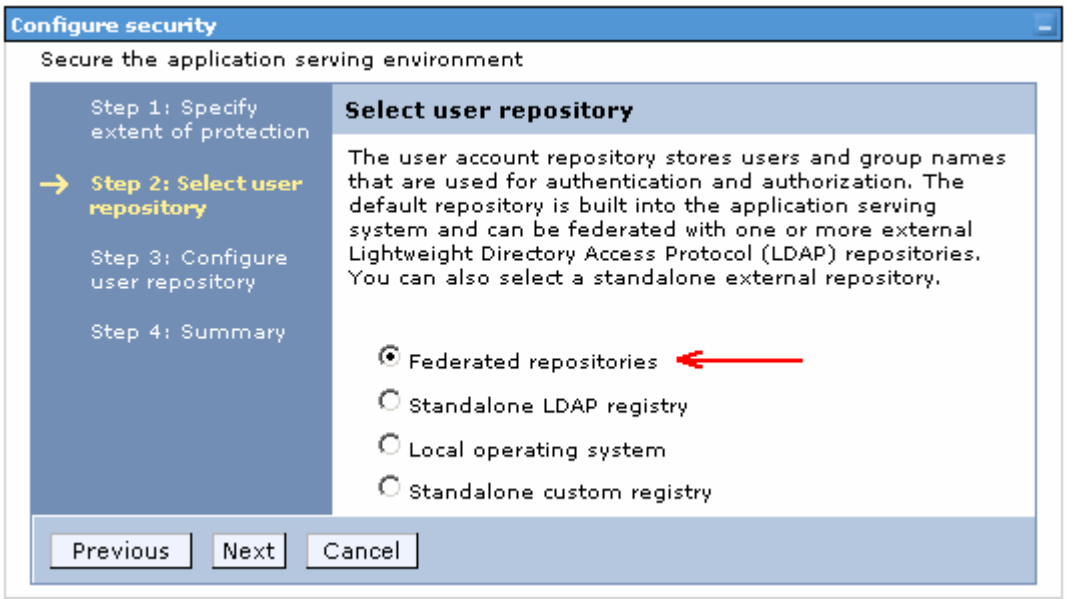
____ 4. In the following '**Secure administration, applications and infrastructure**' panel to the left, click the '**Security Configuration Wizard**' button



____ 5. In the following '**Step1: Specify extent of protection**' panel, ensure the check box for '**Enable application security**' is selected

____ 6. Click **Next**

____ 7. In the following '**Step2: Select user repository**' panel, ensure the radio button for '**Federated repositories**' is selected



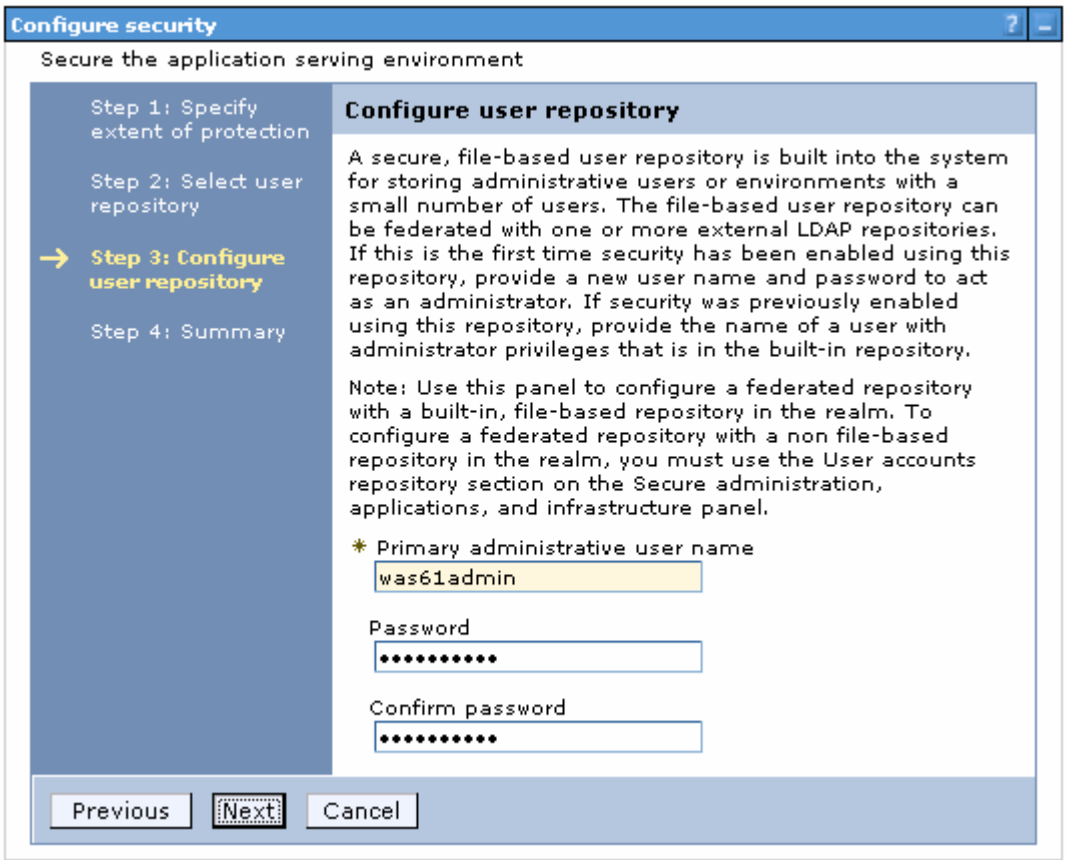
____ 8. Click **Next**

____ 9. In the following '**Step 3: Configure user repository**' panel, enter the primary administrative user name and password

__ a. Primary administrative user name : **was61admin**

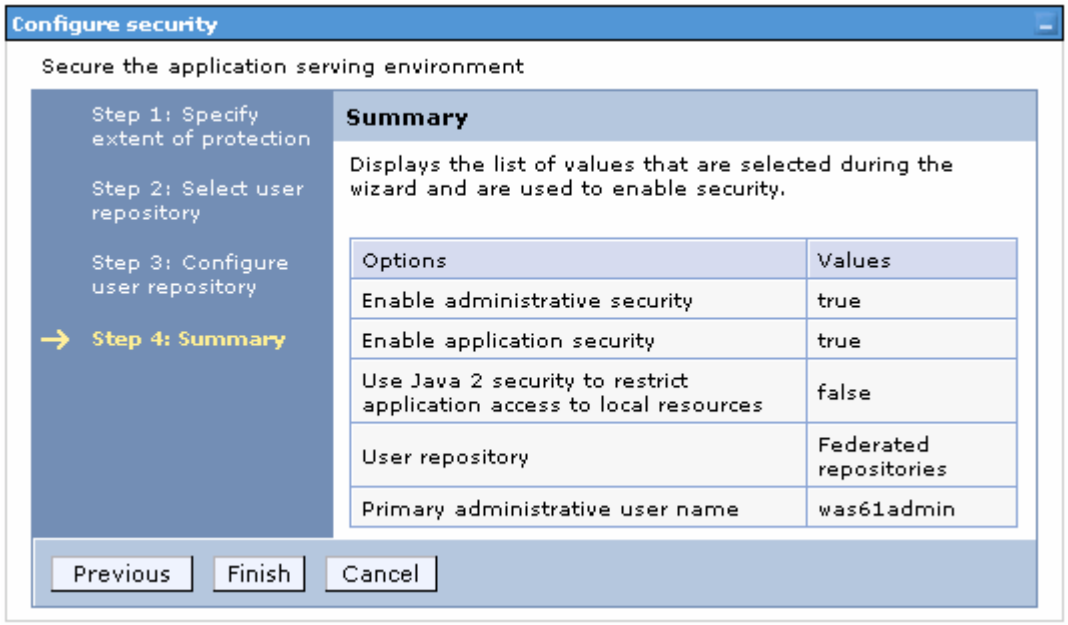
__ b. Password : **was61admin**

__ c. Confirm password : **was61admin**



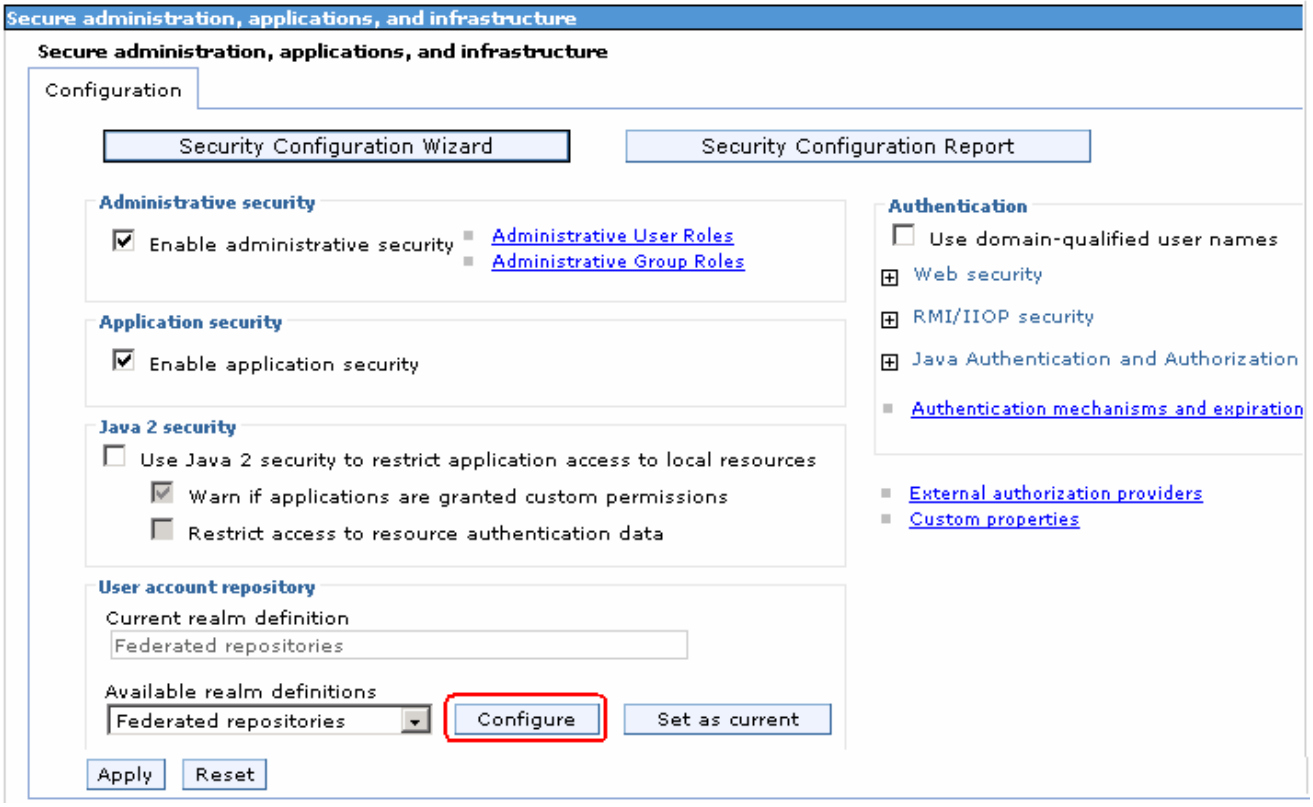
____ 10. Click **Next**

____ 11. In the following '**Step 4: Summary**' panel, review the summary information



____ 12. Click **Finish.** You will see the following '**Secure administration, applications and infrastructure**' panel

__ a. Select '**Federated repositories**' from the drop down list for the '**Available realm definitions**'



____ 13. Click the **Configure** button

____ 14. In the following '**Configuration**' panel for '**Federated repositories**', enter the following under the '**General Properties**' category

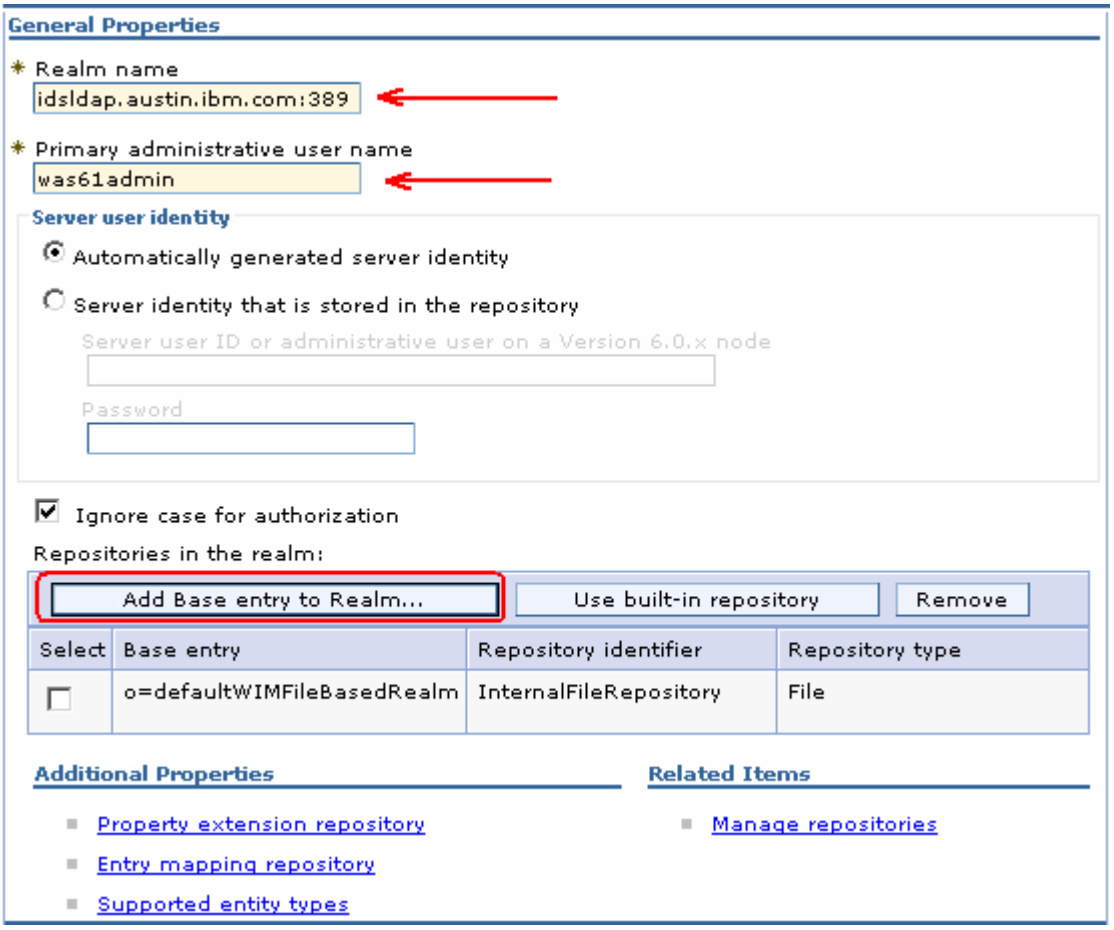
__ a. Realm name : **<fully qualified LDAP server host name>: <LDAP Port>**

: Example: **idsldap.austin.ibm.com:389**

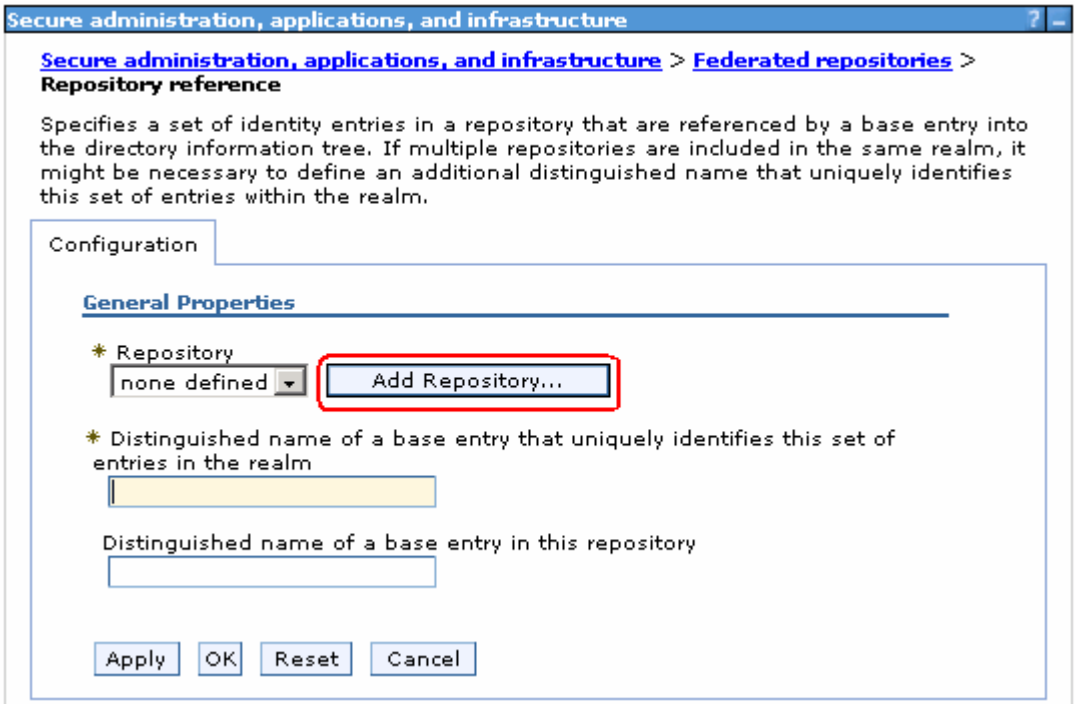
Note: The realm name for Portal is typically the fully qualified LDAP hostname:portNumber (example: "idsldap.austin.ibm.com:389") to verify this, you can open C:\ WebSphere\profiles\wp_profile\config\cells\<your-cell-name>\security.xml and look for <userRegistries xmi:type="security:LDAPUserRegistry" …. – there is a "realm=" entry on that line

---

__ b. Primary administrative user name : **was61admin**



____ 15. Scroll down and click the '**Add Base entry to Realm**' button. This action opens the '**Repository reference**' panel as shown below:



____ 16. Click the '**Add Repository**' button

____ 17. In the following new repository reference panel, enter the following:

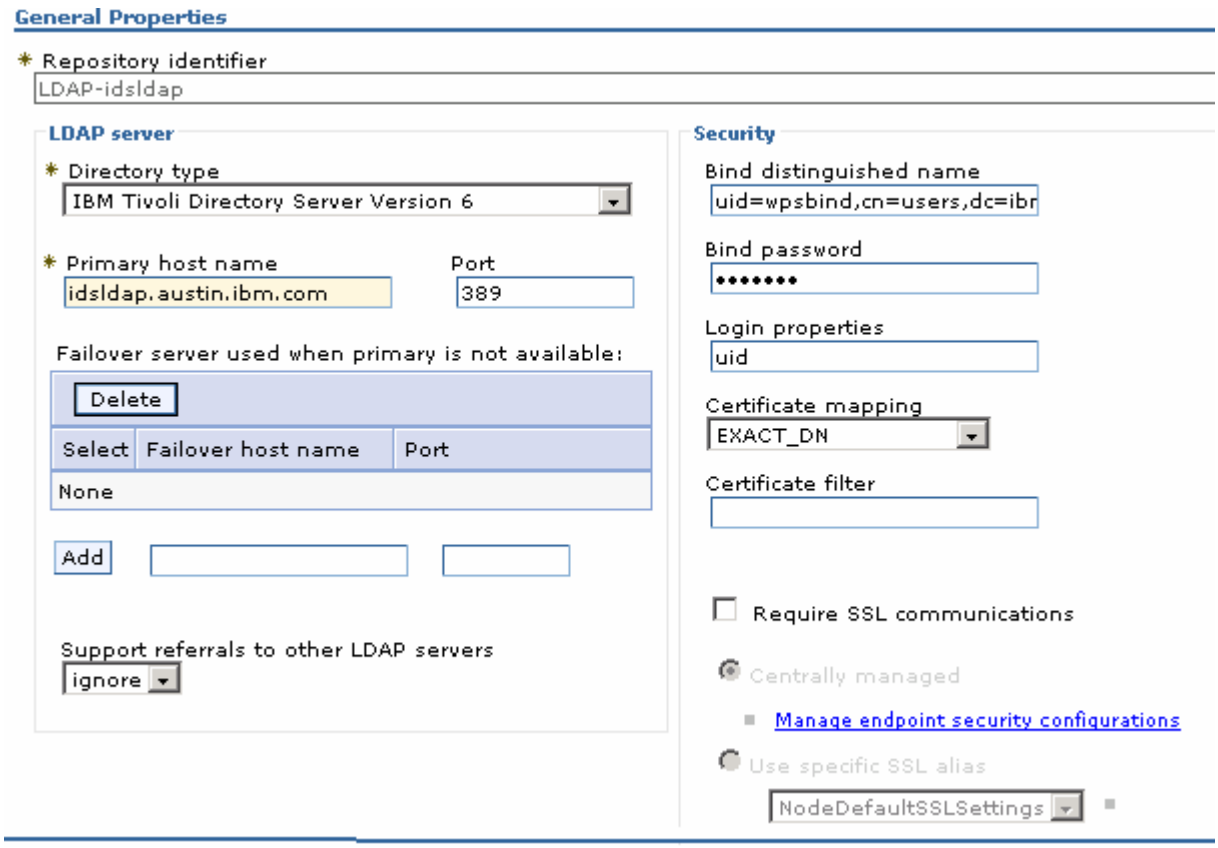
__ a. Repository identifier : **LDAP-idsldap** (Any meaningful identifier)

__ b. LDAP Server

- Directory Type : **IBM Tivoli Directory Server V6.0**
- Primary host name : **idsldap.austin.ibm.com**
- Port : **389**

__ c. Security

- Bind distinguished name : **uid=wpsbind,cn=users,dc=ibm,dc=com**
- Bind password : **wpsbind**
- Login properties : **uid**
- Certificate mapping : Select '**EXACT_DN**' from the drop down list



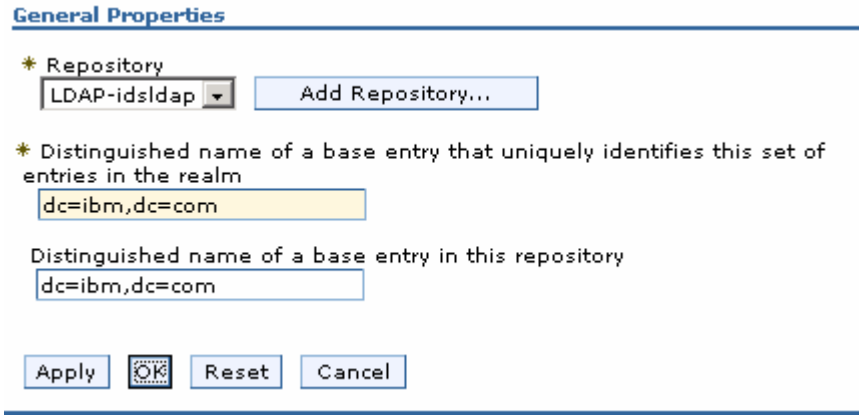
____ 18. Click **OK**. You will be back to the '**Repository reference**' panel again

____ 19. In the '**Repository Reference**' panel, enter the following:

__ a. Repository : Select '**LDAP-idsldap**' from the drop down list

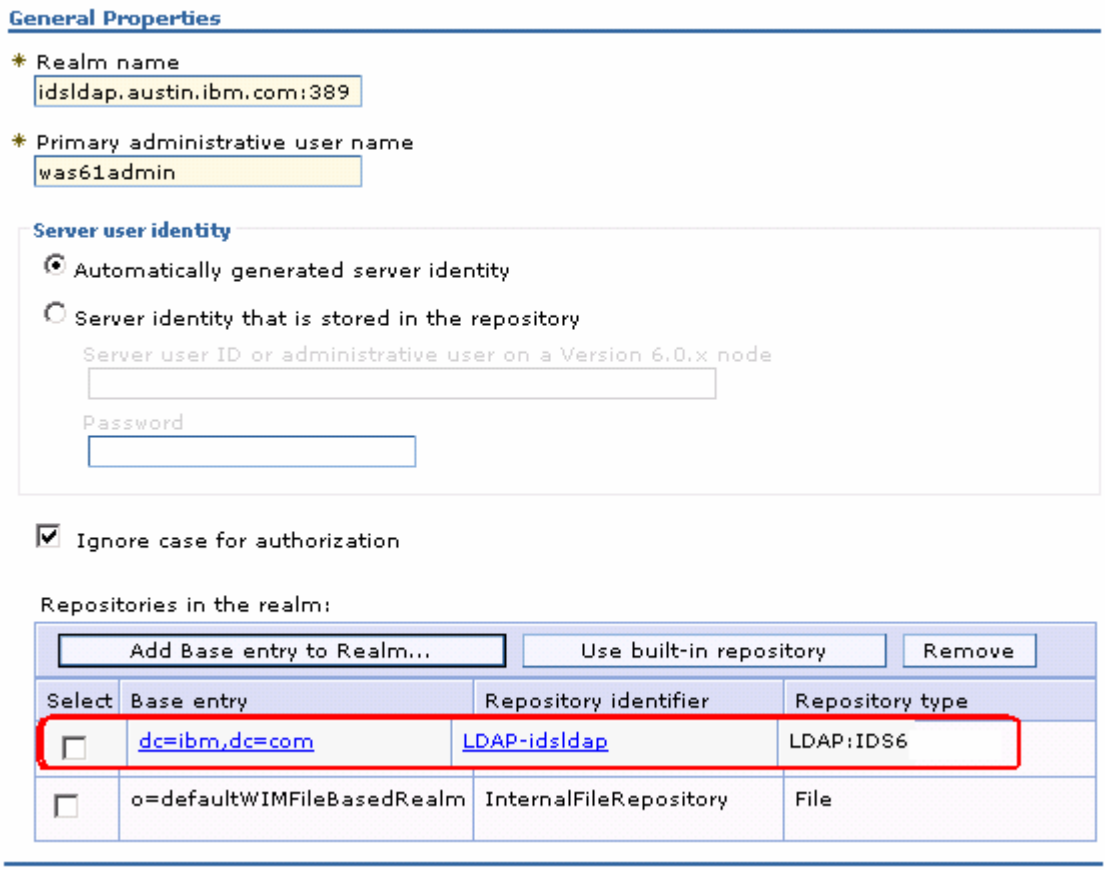
__ b. Distinguished names of a base entry that uniquely identifies this set of entries in the realm : **dc=ibm,dc=com**

__ c. Distinguished name of a base entry in this repository : **dc=ibm,dc=com**

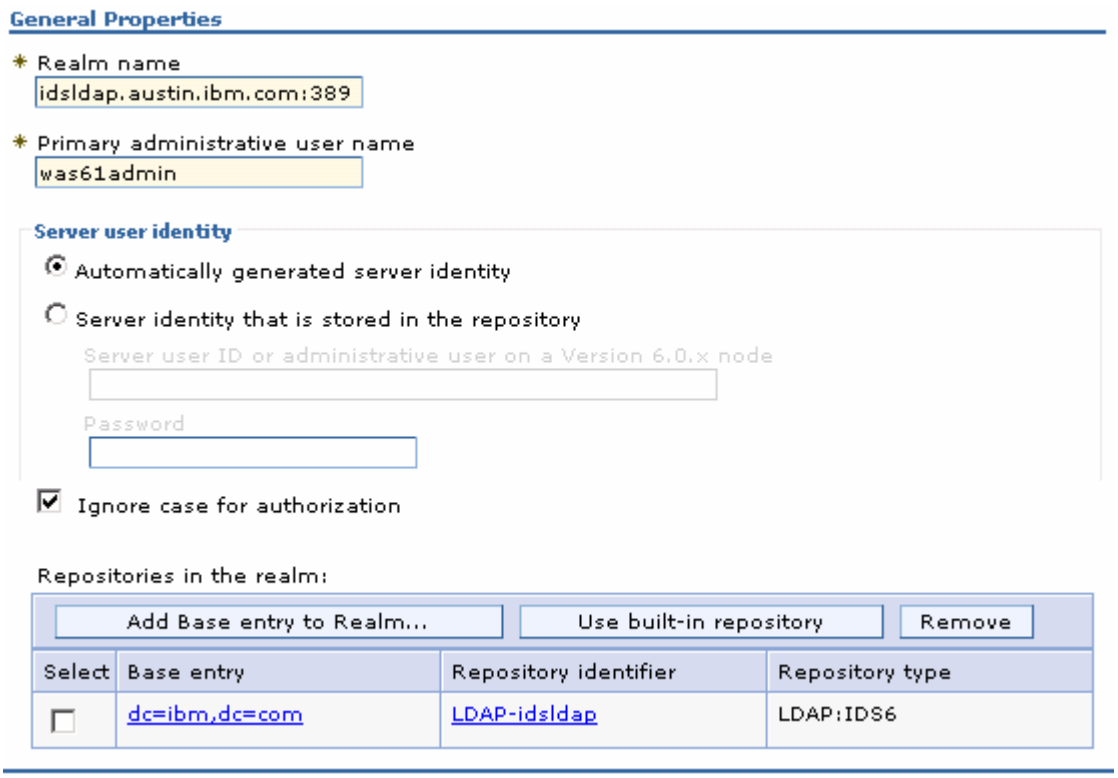


____ 20. Click **OK**

____ 21. The '**Federated repositories**' panel should look like the picture shown below:

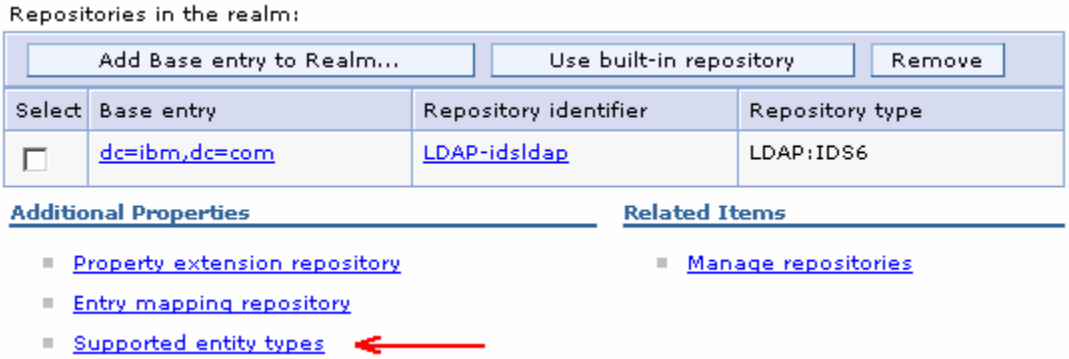


____ 22. Select the check box for '**o=defaultWIMFileBasedRealm**' if it is existing (it exists if the default security is enabled) and click the **Remove** button.

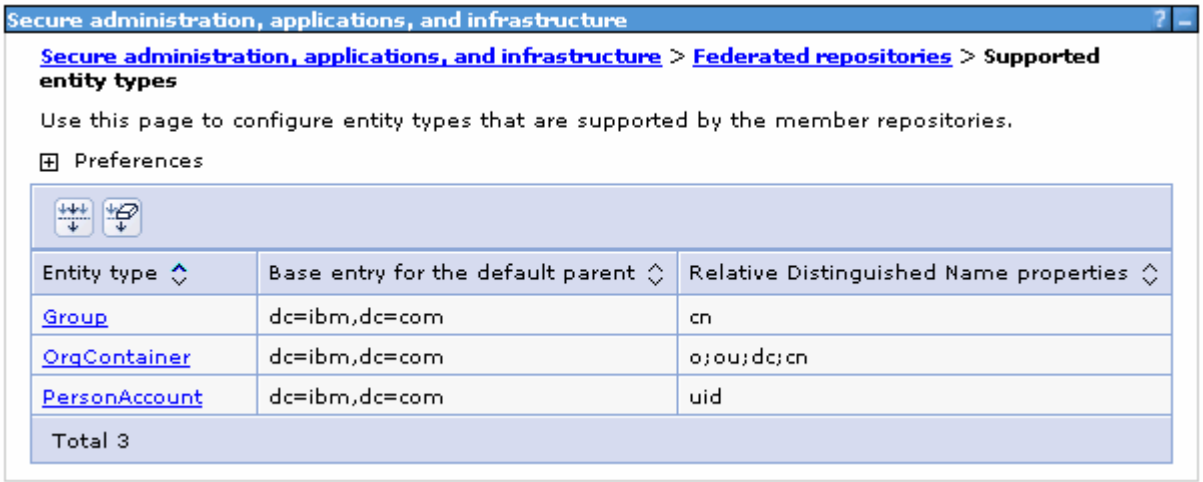


____ 23. Configuring supported entity types in a federated repository configuration

__ a. In the **Federated Repositories** panel, click the '**Supported entity types**' under the '**Additional Properties**' section



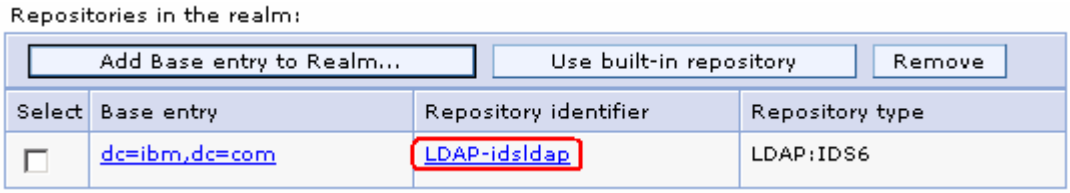
__ b. In the '**Supported entity types**' panel, update the '**Base entry for default parent**' values for **Group**, **OrgContainer** and **PersonAccount** with '**dc=ibm,dc=com**' and accept the defaults for the '**Relative Distinguished Name properties**'. The '**Supported entity types**' panel should look like the picture below:



__ c. Save to the master configuration

____ 24. Configure the LDAP entity types

__ a. While you are in the '**Federated repositories**' panel (**Secure administration, applications and infrastructure → Federated repositories**), click the '**Repository identifier**' link, (Example:- **LDAP-idsldap**)



__ b. In the following panel, scroll to the bottom and click the '**LDAP entity types**' link under the '**Additional Properties**' section

__ c. In the following '**LDAP entity types**' panel, update the following for the **Group**, **OrgContainer** and **PersonAccount** entity types:

1) Group

- Object classes : **groupOfUniqueNames**
- Search bases : **dc=ibm,dc=com**
- Search filter : **(objectclass=groupOfUniqueNames)**

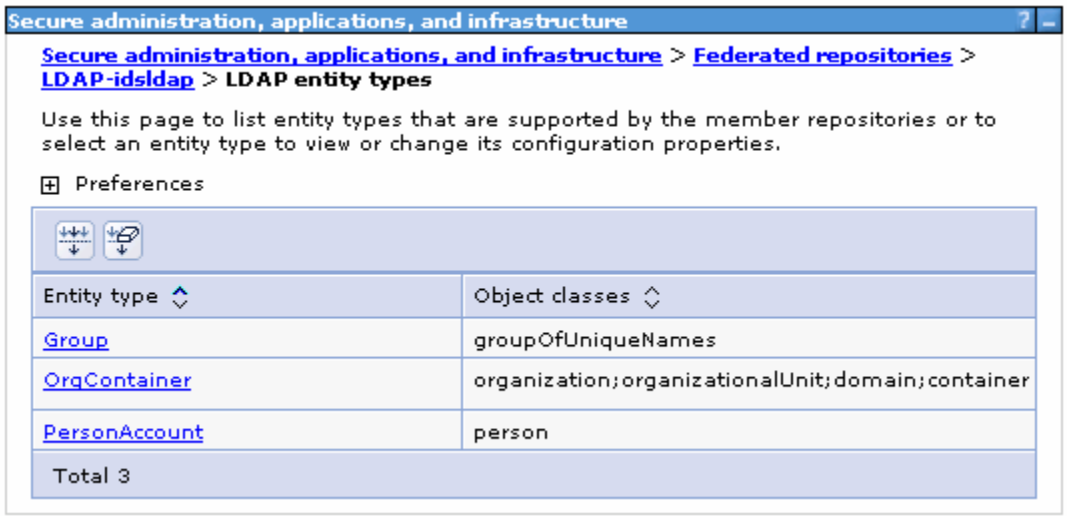
2) **OrgContainer**

- <Accept the defaults>

3) **PersonAccount**

- Object classes : **person**
- Search bases : **dc=ibm,dc=com**
- Search filter : **(objectclass=person)**

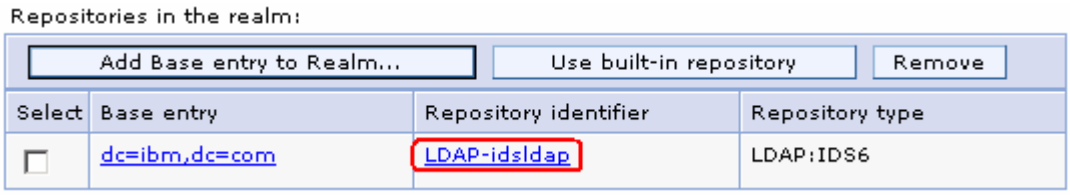
2) The '**LDAP entity**' panel will look like the picture below:



__ b. Save to the master configuration

____ 25. Configure group attribute definition

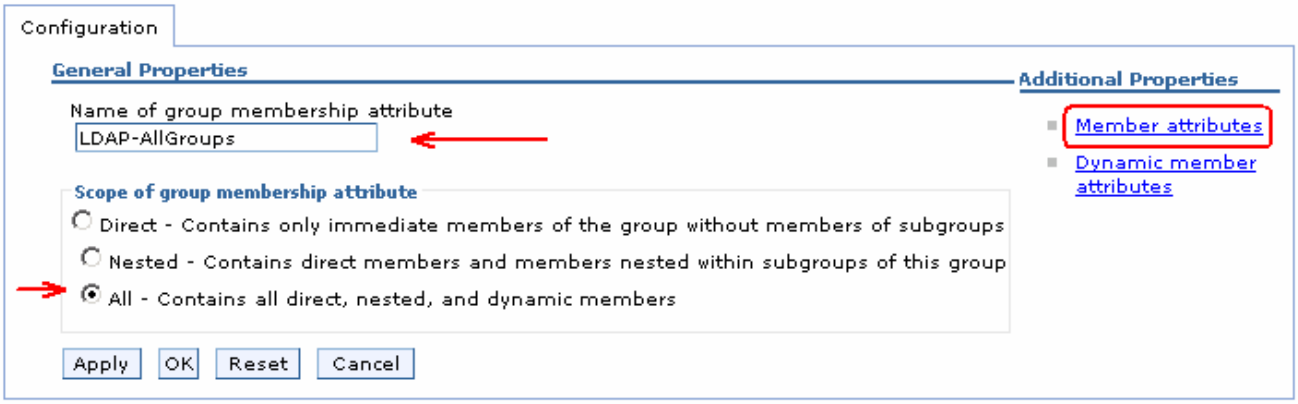
__ a. While you are in the '**Federated repositories**' panel (**Secure administration, applications and infrastructure → Federated repositories**), click the '**Repository identifier**' link, (Example:- **LDAP-idsldap**)



__ b. In the following panel, scroll to the bottom and click the '**Group attribute definition**' link under the '**Additional Properties**' section

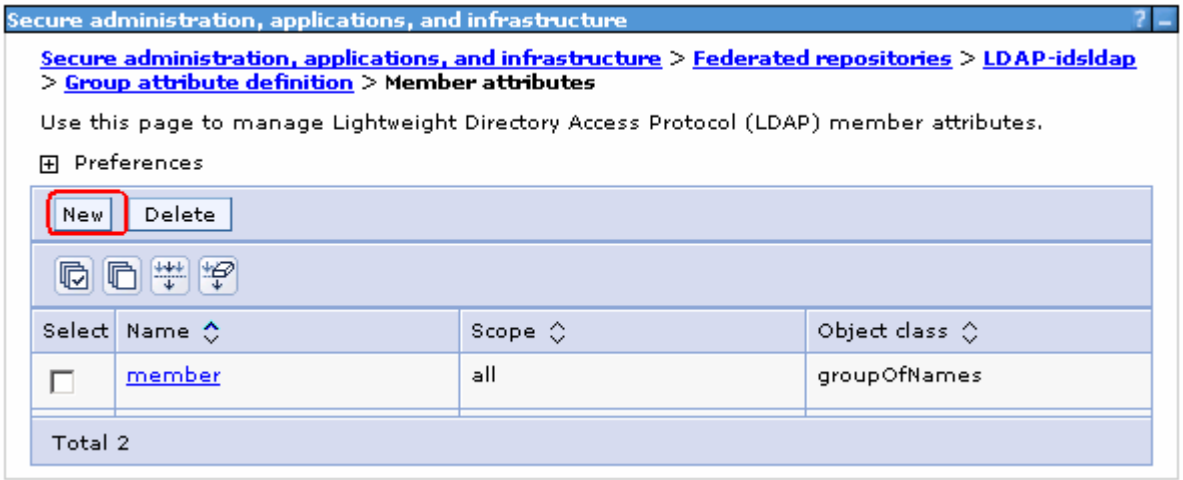
__ c. In the following '**Group attribute definition**' panel, enter the following information:

- Name of group membership attribute : **LDAP-AllGroups**
- For the scope, select the check box for '**All- Contains all direct, nested and dynamic members**'



- Click **Apply**

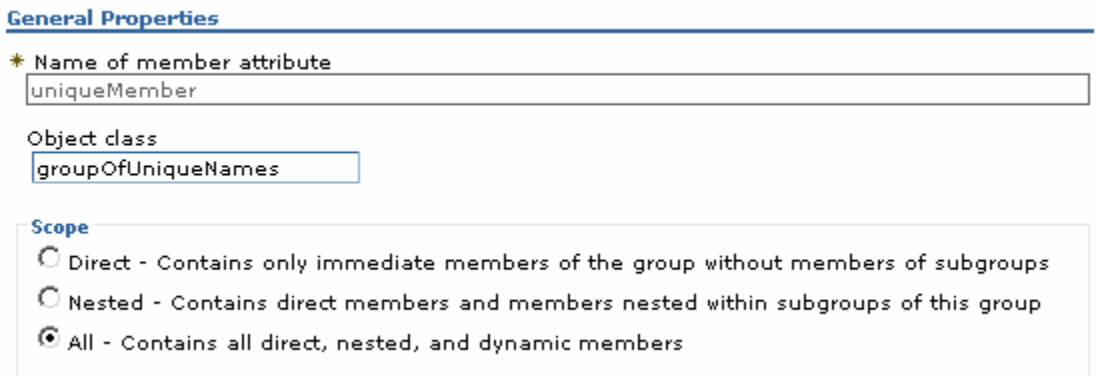
__ d. While you are in the '**Group attribute definition**' panel, click the '**Member attributes**' link under '**Additional properties**' section



__ e. In the following panel, click the **New** button to create a new member attribute

__ f. In the following panel, enter the following information:

- Name of member attribute : **uniqueMember**
- Object class : **groupOfUniqueNames**
- For the scope, select the check box for '**All- Contains all direct, nested and dynamic members**'

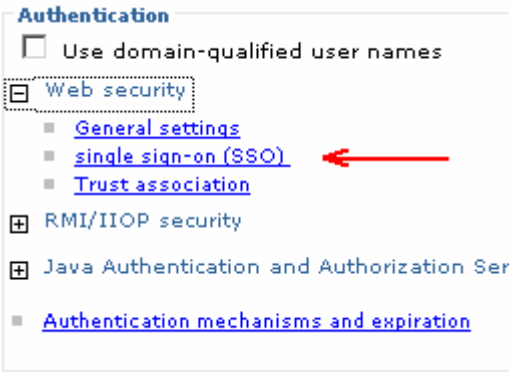


- Click **OK**

__ g. Save to the master configuration

____ 26. Configure 'Single Sign-on'

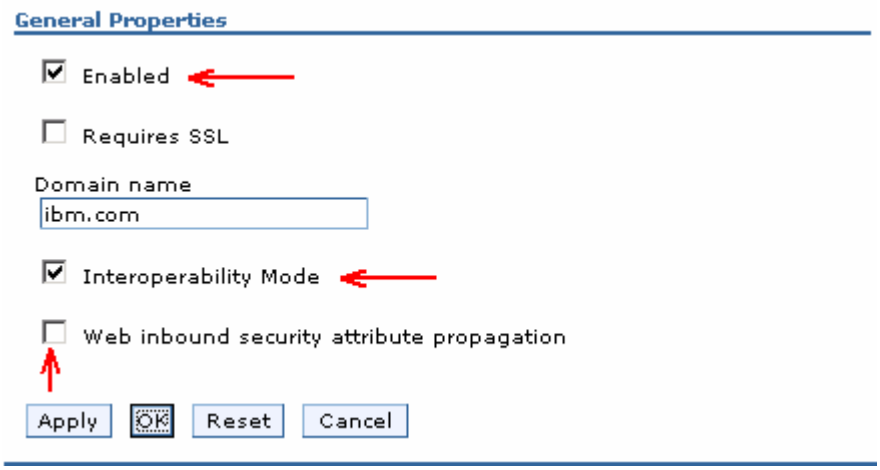
__ a. Navigate to the '**Secure administration, applications and infrastructure**' panel, expand '**Web Security**' under the '**Authentication**' category



__ b. Click the '**single sign-on (SSO)**' link

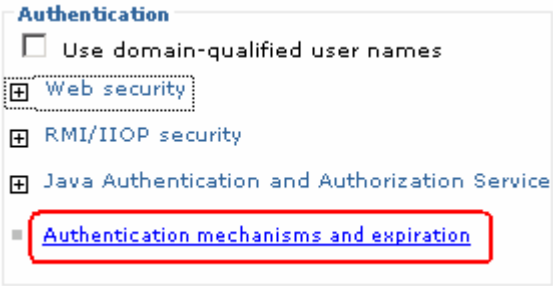
__ c. In the following '**single sign-on (SSO)**' panel, do the following:

- Select the check box for '**Enabled**'
- Ensure the check box for '**Required SSL**' is **not** selected
- Domain name : **ibm.com**
- Select the check box for '**Interoperability Mode**'
- **Unselect** the check box for '**Web bound security attribute propagation**'



____ 27. Click **OK**. You will be directed to the '**Secure administration, applications and infrastructure**' panel again

____ 28. While you are in the '**Secure administration, applications and infrastructure**' panel, click the '**Authentication mechanisms and expiration**' link



____ 29. In the following '**Authentication mechanisms and expiration**' panel, enter the following under the '**Cross-cell single sign-on**' category to import the key file that you had exported on the portal (dashboard) server machine

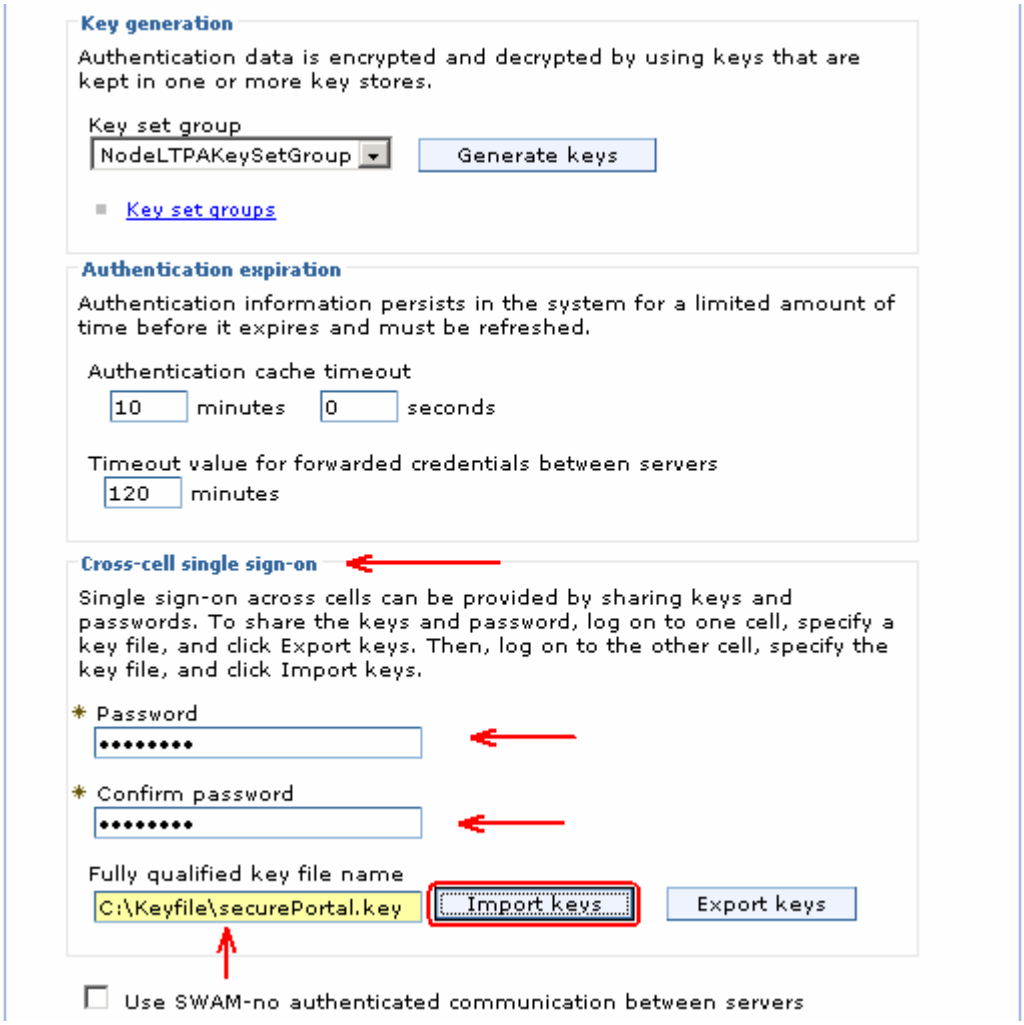
---

Note: Enter the LTPA password that you specified when you Enabled LDAP Security for Portal, and enter the LTPA key file name that you specified near the end of the "LDAP Security for Portal" configuration.

__ a. Password : **password**

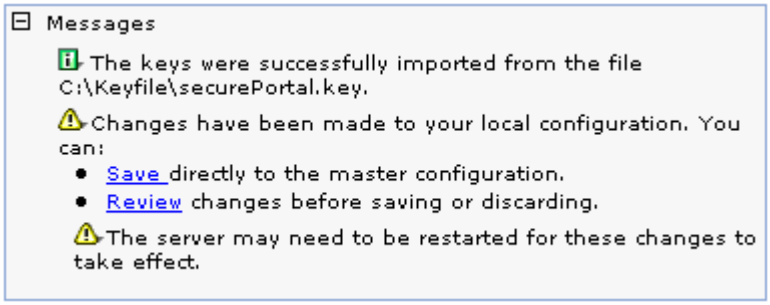
__ b. Confirm password : **password**

__ c. Fully Qualified Key file name : Example:- **C:\KeyFile\securePortal.key**



____ 30. Click the '**Import Keys**' button

____ 31. Click the **Save** link, to save the configuration

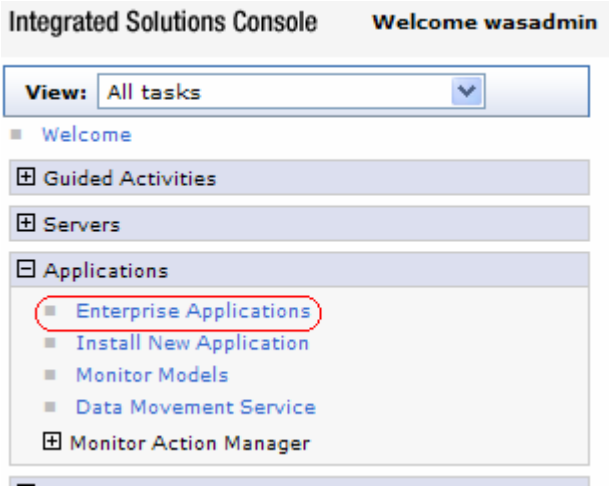


____ 32. Restart the server, launch the administrative console and log in using the user name and password

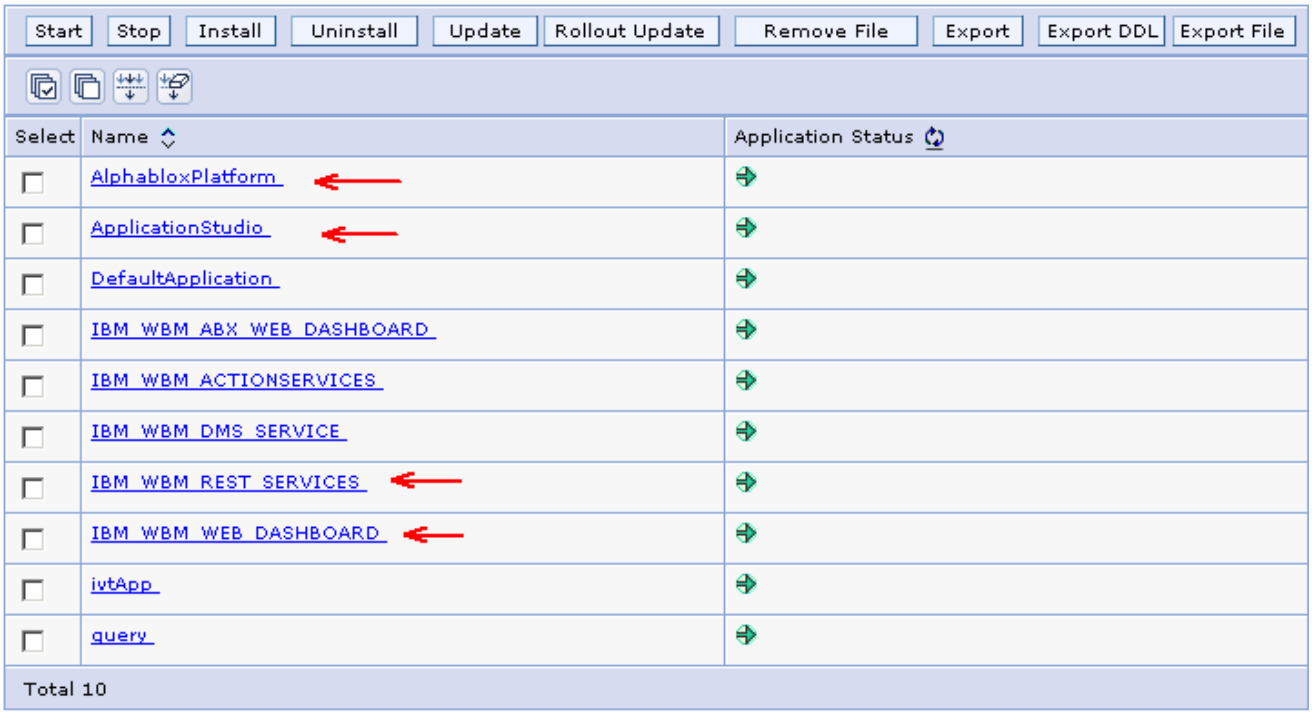
---

Note: To restart the server at this time, you should enter the old user name and password configured during the WebSphere Business Monitor server installation.

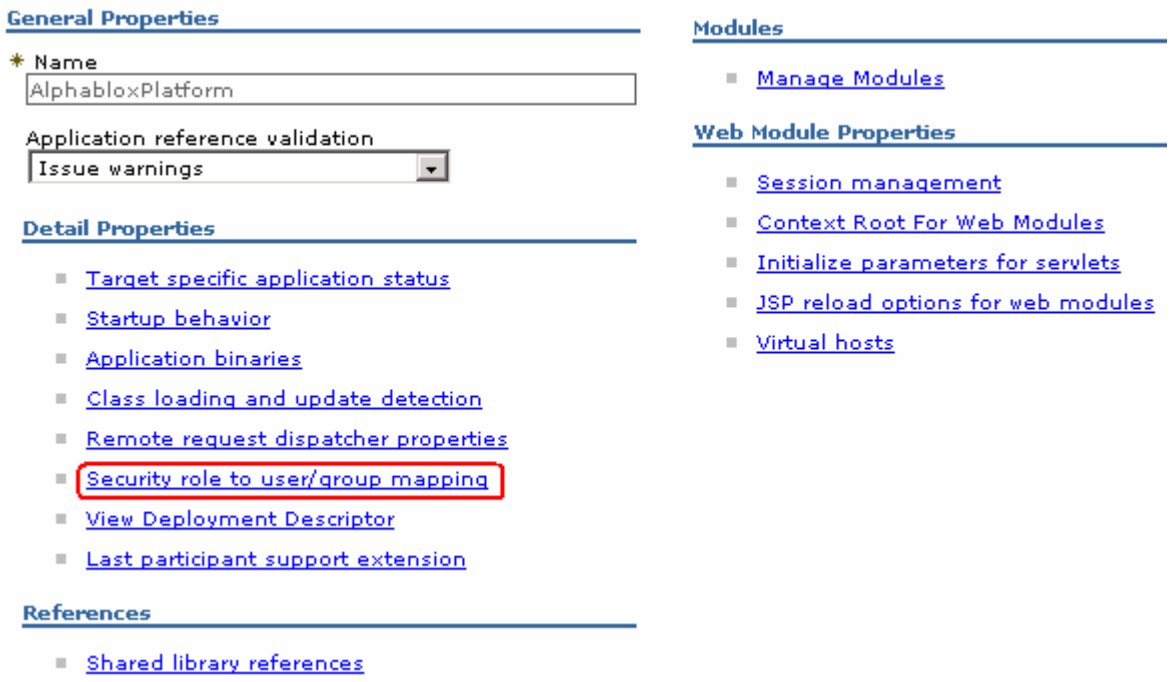
____ 33. In the left navigation pane of the administrative console, expand '**Applications**' and click the '**Enterprise Applications**' link.



____ 34. In the following '**Enterprise Applications**' panel, click the '**AlphabloxPlatform**' link

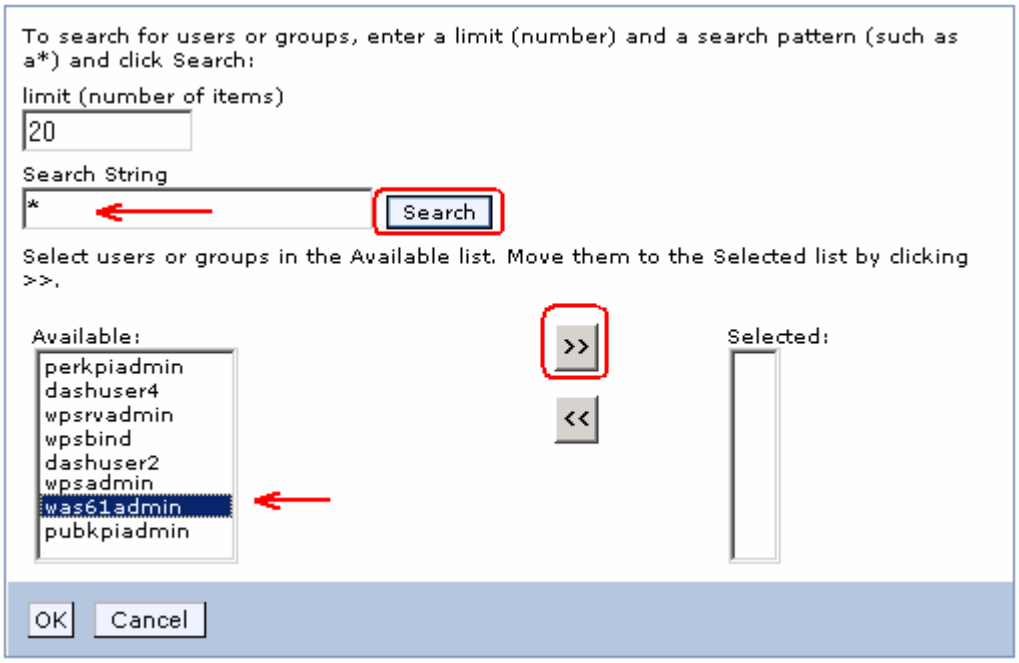


____ 35. In the following panel, click the '**security role to user/group mapping**' link



____ 36. In the following panel, select the check box for '**AlphabloxAdministrator**' role and click the '**Look up users**' button

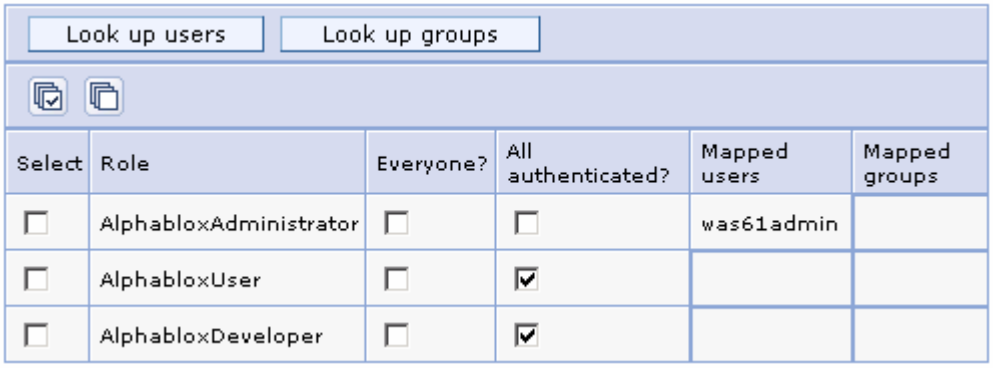
____ 37. In the following panel, enter a wild character (*****) as the search string and click the **Search** button. Select **was61admin** from the available users listed, and then click the right directional arrow button, to move the user ID to the selected text area



____ 38. Click **OK**

____ 39. Ensure that the check boxes for '**All authenticated?**' are selected for the '**AlphabloxUser**' and '**AlphabloxDeveloper**' roles

____ 40. The **security role to user/group mapping** panel for the **AlphabloxPlatform** application will look like the picture below:



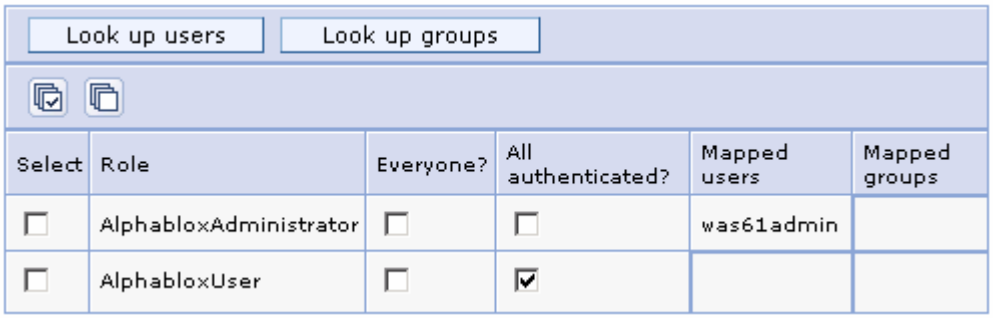
____ 41. Click **OK** and save to the master configuration

____ 42. Back to the '**Enterprise Applications**' panel, click the '**ApplicationStudio**' link

____ 43. In the following panel, click the '**security role to user/group mapping**' link

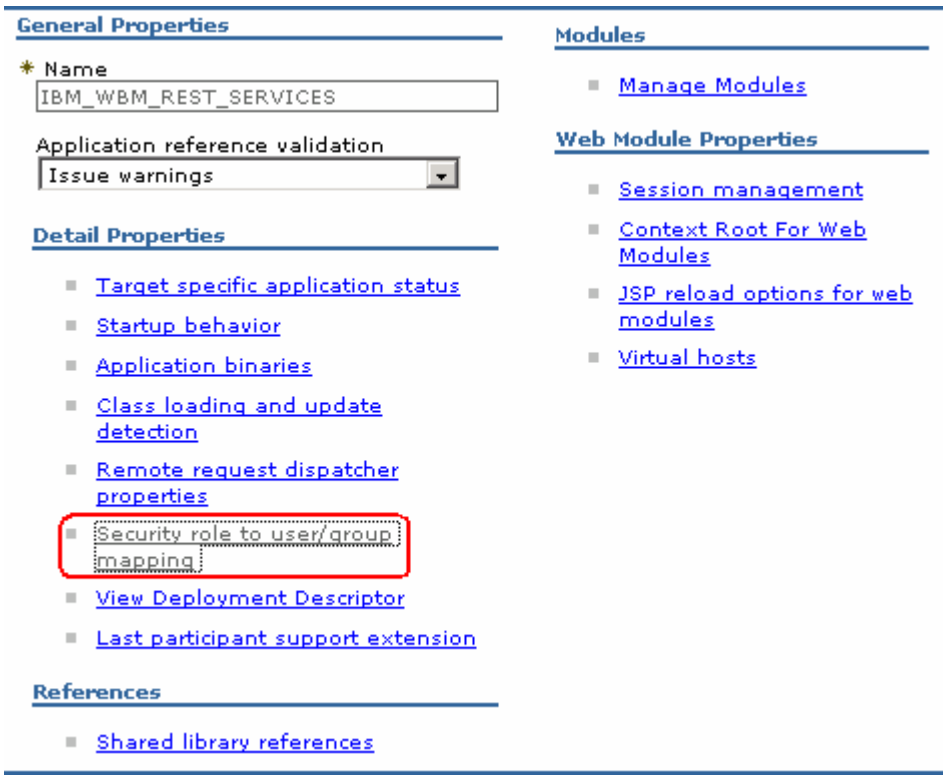
____ 44. In the following panel, map the **was61admin** user for '**AlphabloxAdministrator**' role and ensure the check box for '**All authenticated?**' is selected for '**AlphabloxUser**' role. Click **OK** and save to the master configuration

____ 45. The **security role to user/group mapping** panel for the **ApplicationStudio** application will look like the picture below:

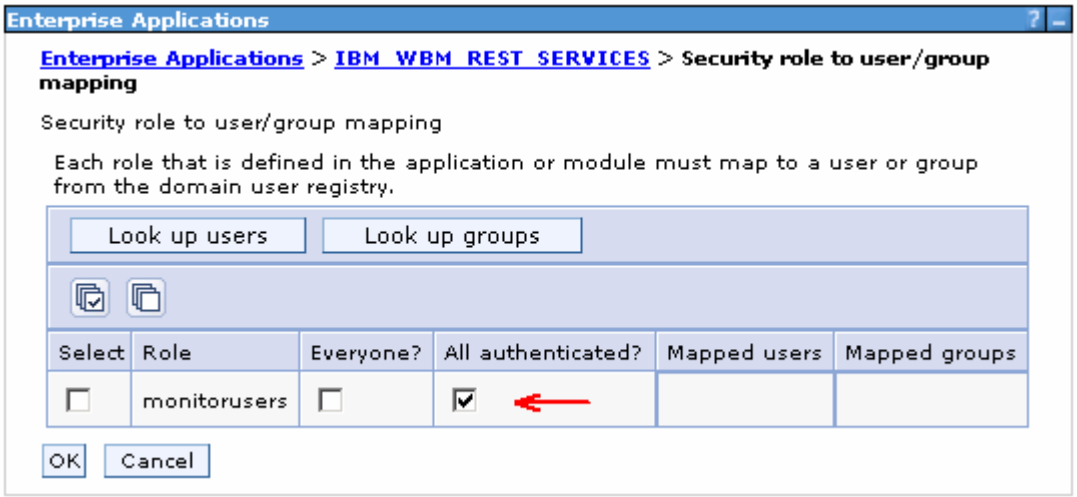


____ 46. Back to the '**Enterprise Applications**' panel, click the '**IBM_WBM_REST_SERVICES**' link

____ 47. In the following panel, click the '**security role to user/group mapping**' link



____ 48. In the following panel, ensure the check box for '**All authenticated?**' for the '**monitorusers**' role is selected

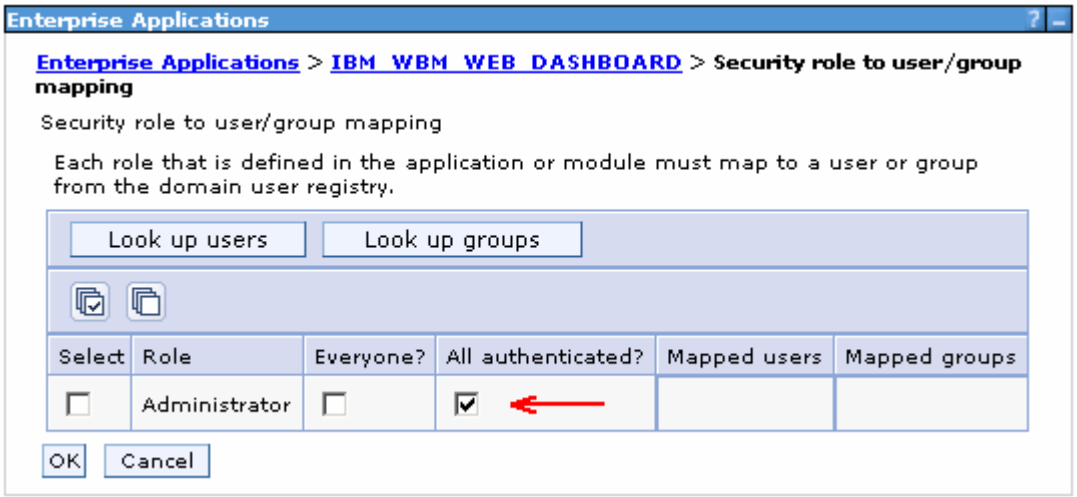


____ 49. Click **OK** and save the changes to the master configuration

____ 50. Back to the '**Enterprise Applications**' panel, click the '**IBM_WBM_WEB_DASHBOARD**' link

____ 51. In the following panel, click the '**security role to user/group mapping**' link

____ 52. In the following panel, select the check box for '**All authenticated?**' for the '**Administrator**' role



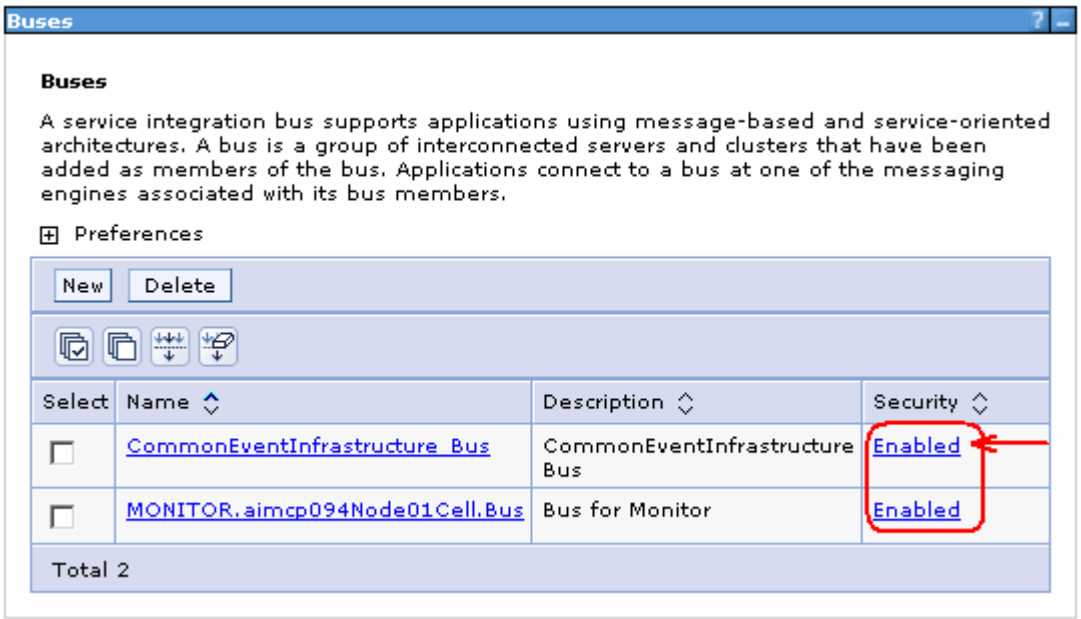
____ 53. Click **OK** and save to the master configuration

→Update J2C authentication data entries for messaging buses

This part of the lab updates the J2C authentication data entries for the messaging buses on the Monitor Server. There are two messaging buses, a Common Event Infrastructure (CEI) messaging bus and a Monitor messaging bus and you will be updating them with the user.

____ 1. In the left navigation pane of the administrative console, expand '**Security**' and then click '**Bus Security**' link

____ 2. In the following '**Buses**' panel, click the '**Enabled**' link for '**CommonEventInfrastructure_Bus**'



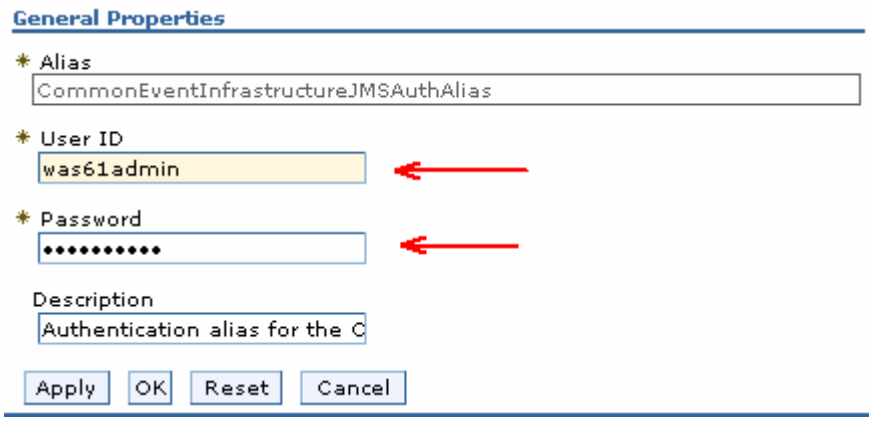
____ 3. In the following panel, click the '**J2C-authentication data**' under the '**Related Items**' section

____ 4. In the following panel, click the '**CommonEventInfrastructureJMSAuthAlias**' link

____ 5. In the following panel, update the User ID and Password

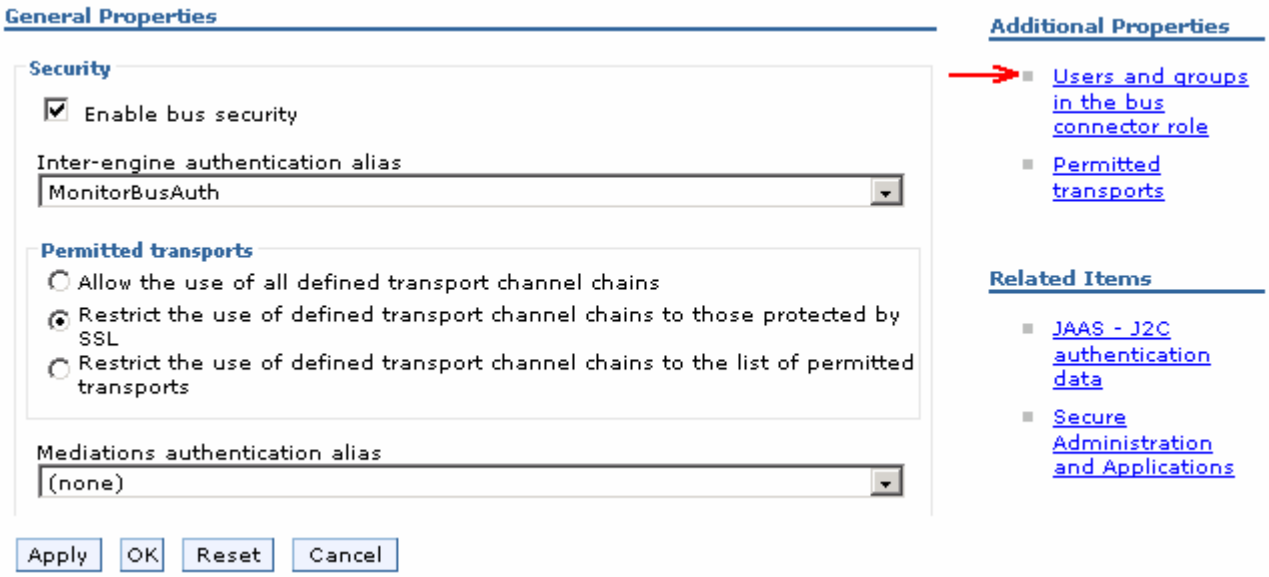
__ a. User ID : **was61admin**

__ b. Password : **was61admin**

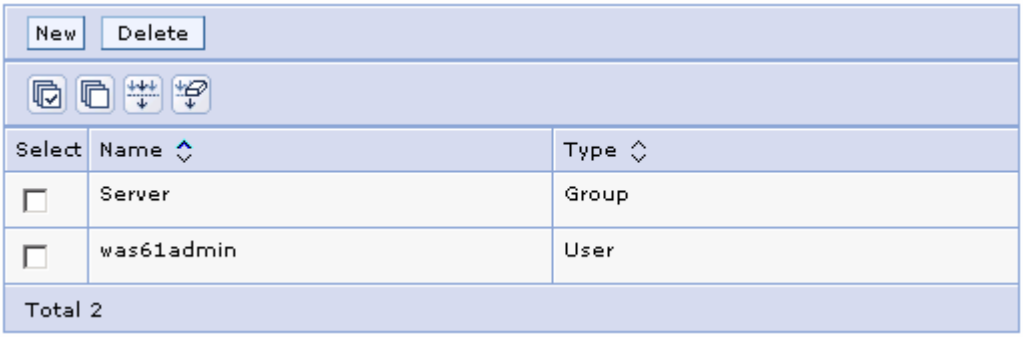


____ 6. Click **OK** and save to the master configuration

____ 7. Navigate to the '**Security → Bus Security → CommonEventInfrastructure_Bus → Enabled**' again and click the '**Users and groups in the bus connector role**' link under the '**Additional Properties**' section to the right



____ 8. In the following panel, add the group and user as shown below:



____ 9. Save to the master configuration

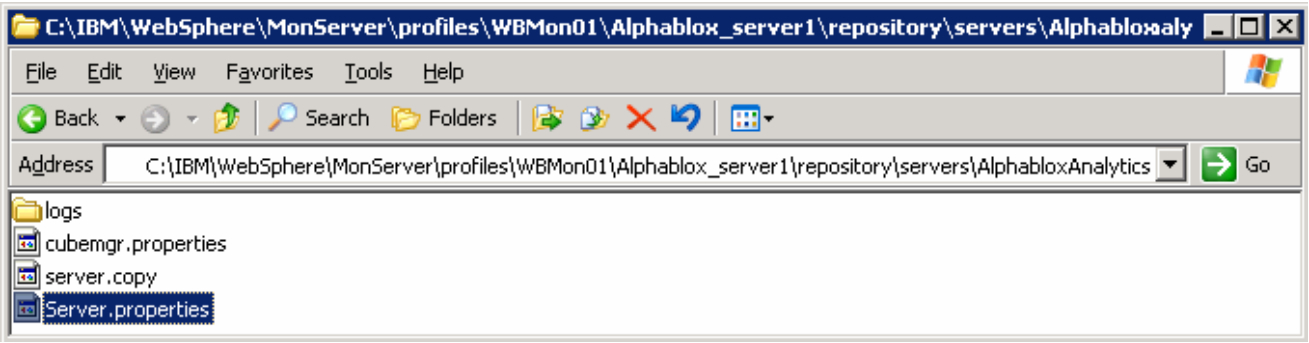
____ 10. Repeat the above instructions to update the J2C authentication alias data for the monitor bus named '**Monitor.<CELL_NAME>.Bus**'. The J2C authentication named you should update is **MonitorBusAuth**

____ 11. Now update the Alphablox '**Server.properties**' file wit the new user name and password

__ a. Navigate to the following location:

<WBM_PROFILE_HOME>\Alphablox_server1\repository\servers\AlphabloxAnalytics

Example: - **<WBM_PROFILE_HOME>** →C:\IBM\WebSphere\Monitor\profiles\WBMon01\



__ b. Edit the '**Server.properties**' file and scroll to the very end of this file

__ c. Add the following lines at the end of the properties file

- **ws.admin.username = <USERNAME>** (was61admin)
- **ws.admin.password = <PASSWORD>** (was61admin)

__ d. Save the changes and close the properties file

Restart the Monitor Server profile

- stopServer.bat server1 –username was61admin –password was61admin
- startServer.bat server1
- Ensure the server is started successfully. Review the '**SystemOut.log**' file for any security related errors

Part 4: Enable security for WebSphere Process Server V6.1

In this part of the lab, you will enable the LDAP security for WebSphere Process Server V6.1. This is not the Monitor Server, but the server where you are running your BPEL processes.

Prerequisite:-

Copy the **securePortal.key** file that you have exported to a temporary location on to the Process Server machine

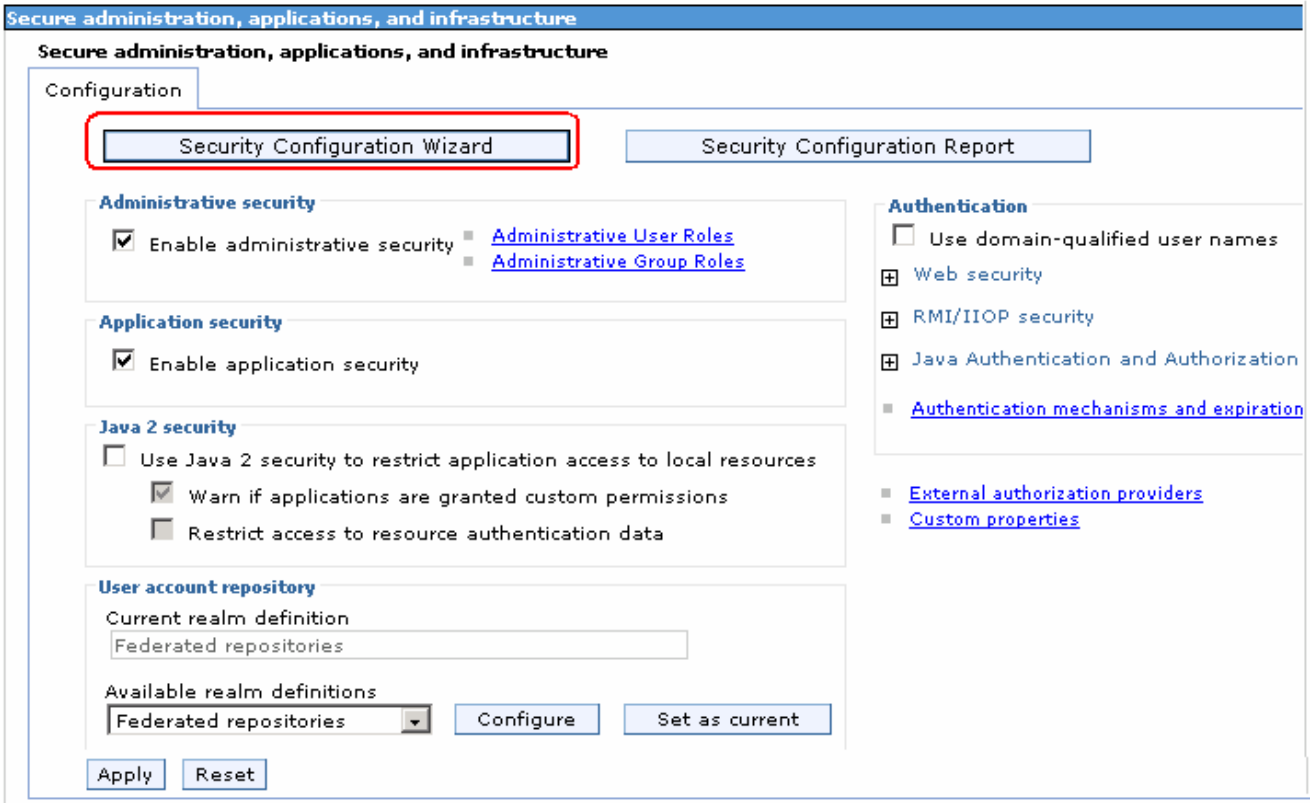
Complete the following instructions to enable LDAP security for the WebSphere Application Server, which is the Process Server profile

____ 1. Start the process server profile and launch the administrative console

____ 2. Login to the administrative console using the user name and password if the default security is enabled at this time

____ 3. In the administrative console's left navigation pane, expand '**Security**' and click the '**Secure administration, applications and infrastructure**' link

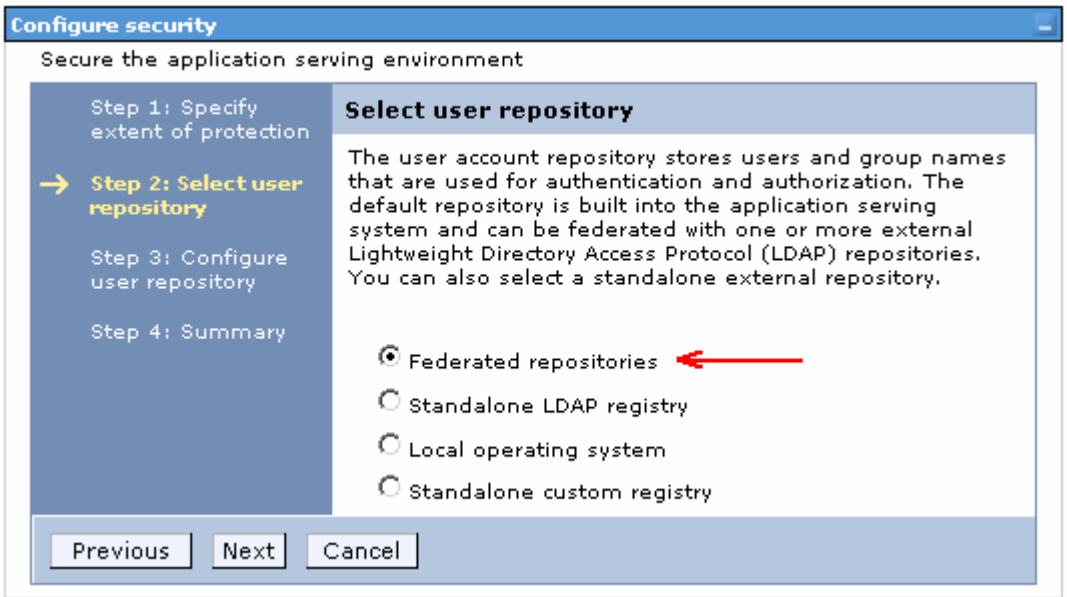
____ 4. In the following '**Secure administration, applications and infrastructure**' panel to the left, click the '**Security Configuration Wizard**' button



____ 5. In the following '**Step1: Specify extent of protection**' panel, ensure the check box for '**Enable application security**' is selected

____ 6. Click **Next**

____ 7. In the following '**Step2: Select user repository**' panel, ensure the radio button for '**Federated repositories**' is selected



____ 8. Click **Next**

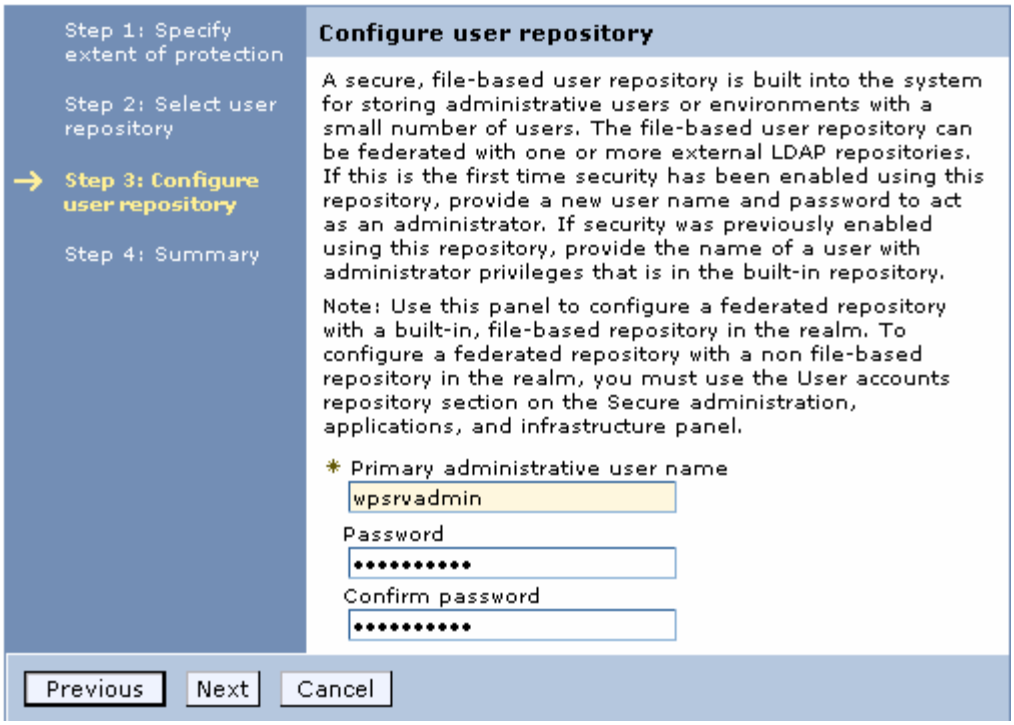
____ 9. In the following '**Step 3: Configure user repository**' panel, enter the primary administrative user name and password

__ a. Primary administrative user name : **wpsrvadmin**

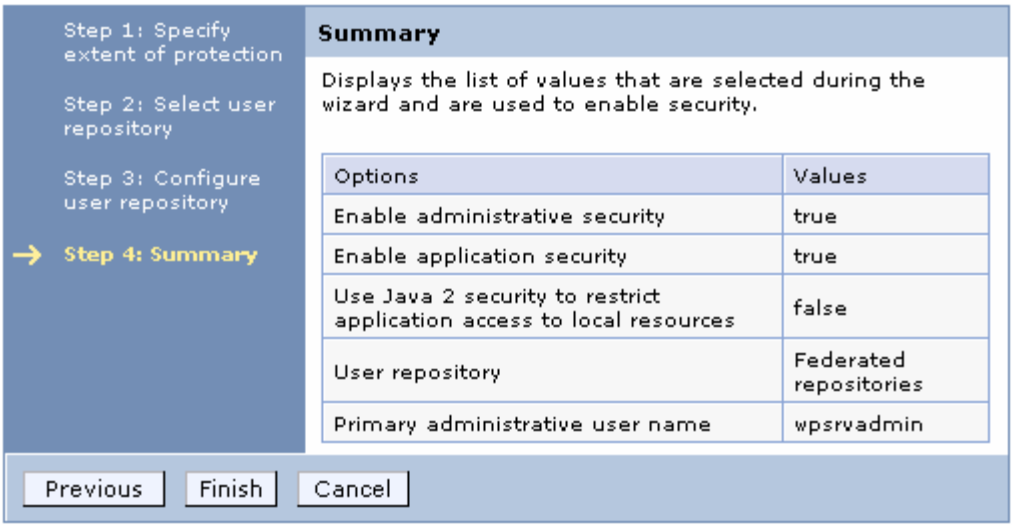
__ b. Password : **wpsrvadmin**

__ c. Conform password : **wpsrvadmin**

Note: The primary administrative user you enter here must exist in the LDAP user repository.

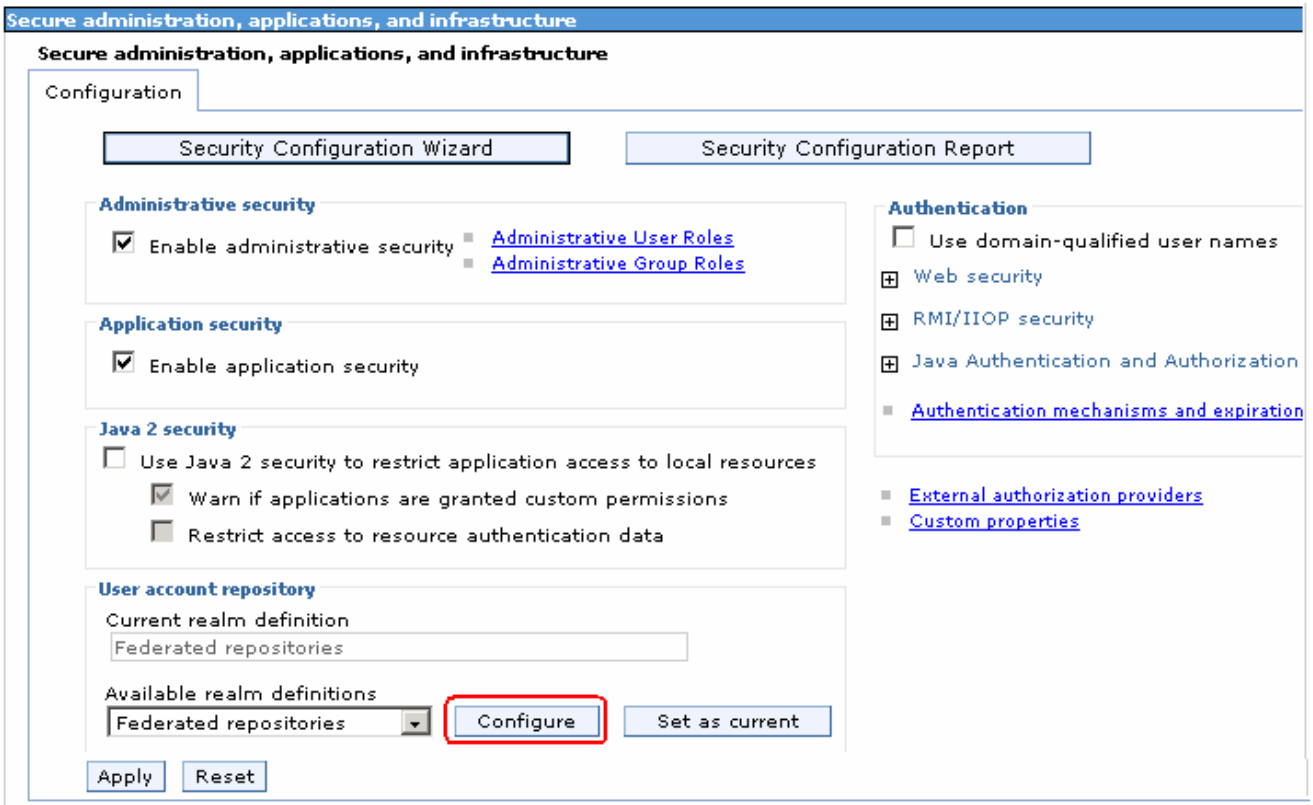


____ 10. In the following '**Step 4: Summary**' panel, review the summary information



____ 11. Click **Finish.** You should see the following '**Secure administration, applications and infrastructure**' panel

__ a. Select '**Federated repositories**' from the drop down list for the '**Available realm definitions**'



____ 12. Click the **Configure** button

____ 13. In the following '**Configuration**' panel for '**Federated repositories**', enter the following under the '**General Properties**' category

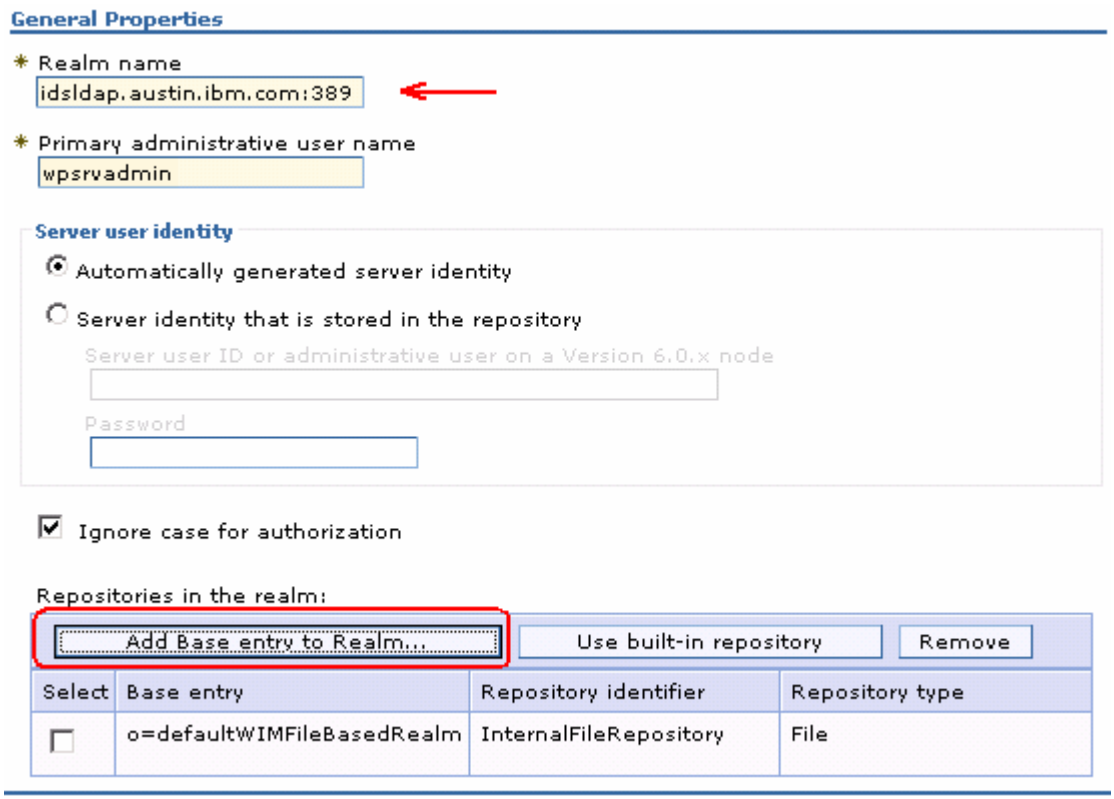
__ a. Realm name : **<fully qualified LDAP server host name>: <LDAP Port>**

: Example: **idsldap.austin.ibm.com:389**

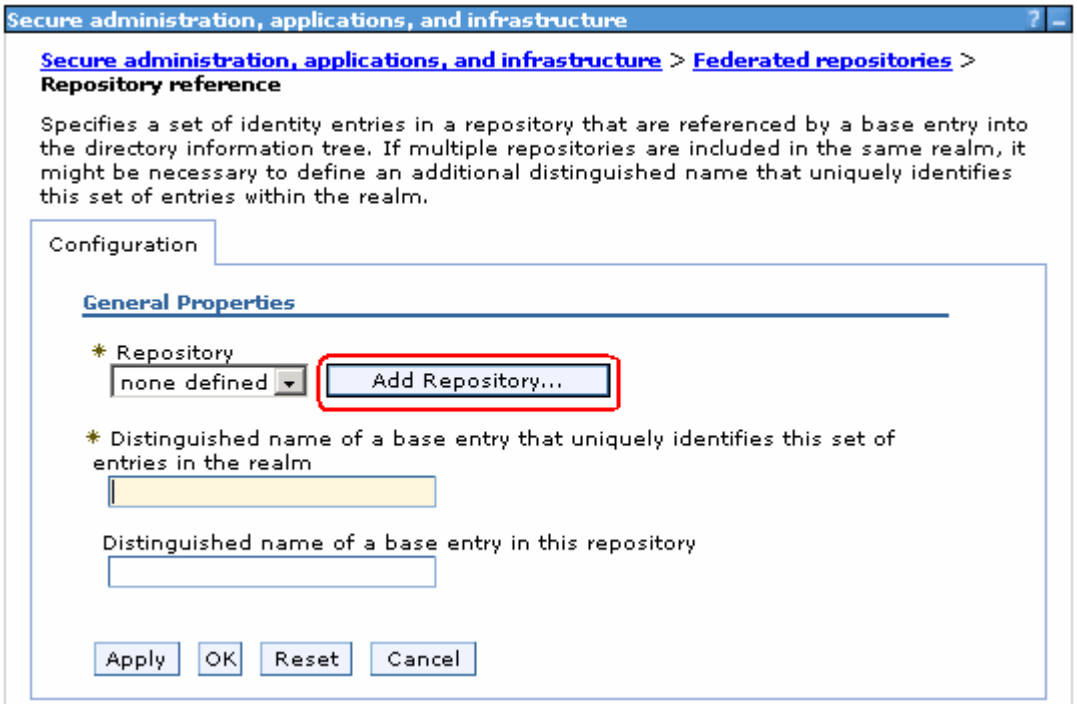
Note: The realm name for Portal is typically the fully qualified LDAP hostname:portNumber (example: "idsldap.austin.ibm.com:389") to verify this, you can open C:\ WebSphere\profiles\wp_profile\config\cells\<your-cell-name>\security.xml and look for <userRegistries xmi:type="security:LDAPUserRegistry" …. – there is a "realm=" entry on that line

---

__ b. Primary administrative user name : **wpsrvadmin**



____ 14. Scroll down and click the '**Add Base entry to Realm**' button. This action opens the '**Repository reference**' panel as shown below:



____ 15. Click the '**Add Repository**' button

____ 16. In the following new repository reference panel, enter the following:

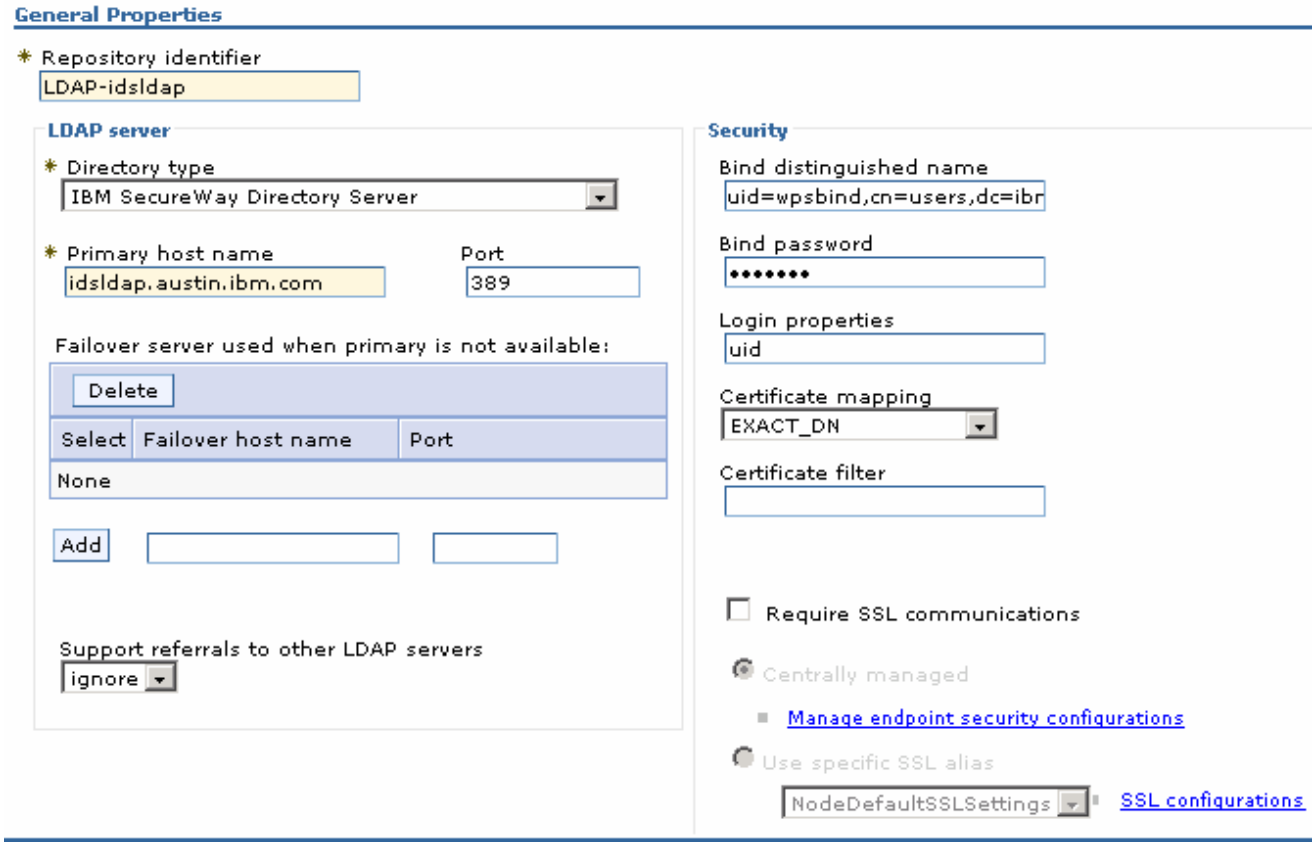
__ a. Repository identifier : **LDAP-idsldap** (Any meaningful identifier)

__ b. LDAP Server

- Directory Type : **IBM Tivoli Directory Server V6.0**
- Primary host name : **idsldap.austin.ibm.com**
- Port : **389**

__ c. Security

- Bind distinguished name : **uid=wpsbind,cn=users,dc=ibm,dc=com**
- Bind password : **wpsbind**
- Login properties : **uid**
- Certificate mapping : Select '**EXACT_DN**' from the drop down list



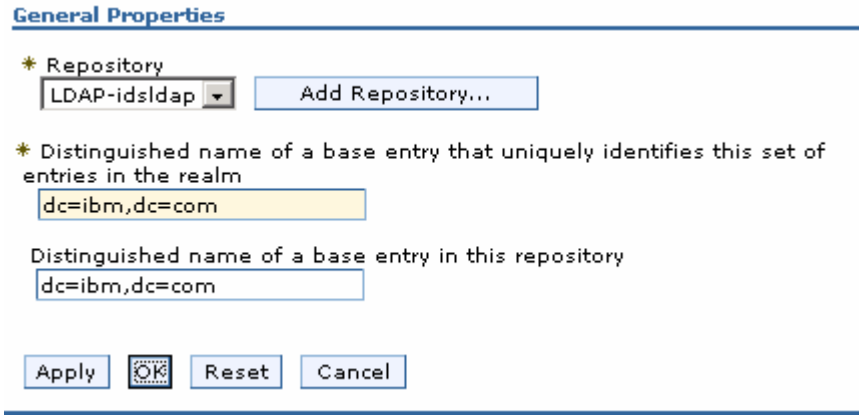
____ 17. Click **OK**. You will be back to the '**Repository reference**' panel again

____ 18. In the '**Repository Reference**' panel, enter the following:

__ a. Repository : Select '**LDAP-idsldap**' from the drop down list

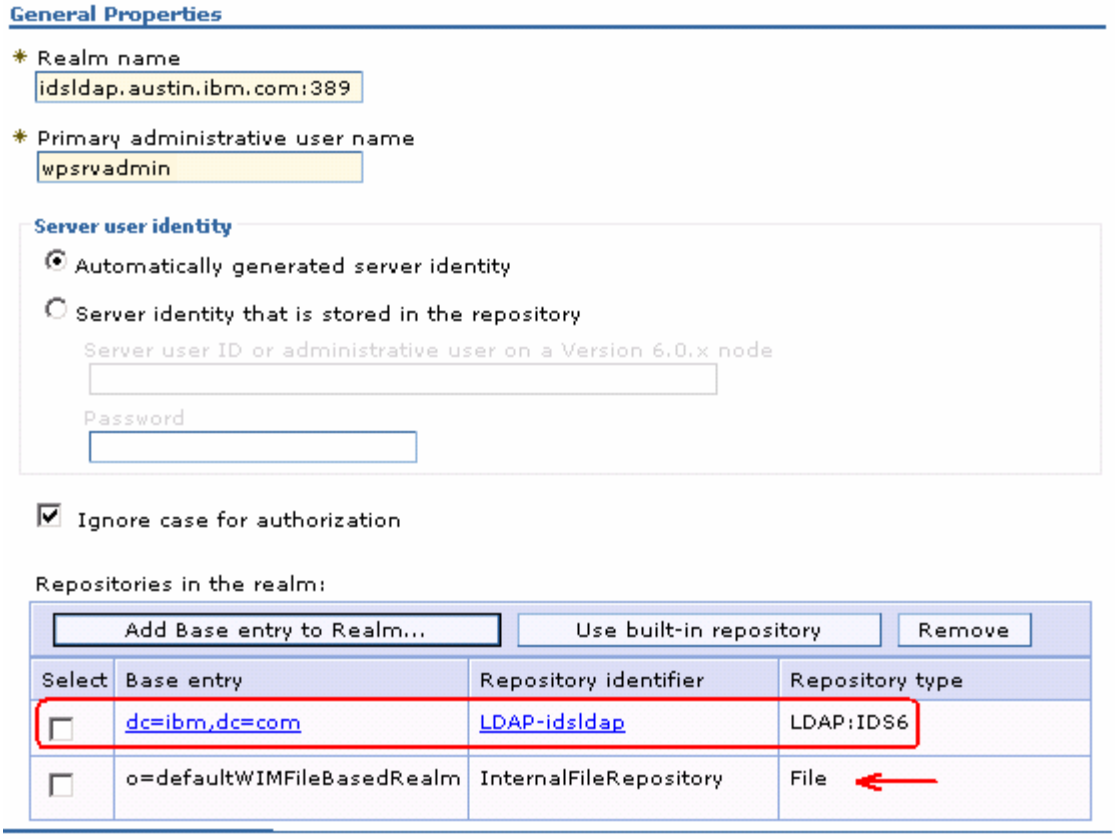
__ b. Distinguished names of a base entry that uniquely identifies this set of entries in the realm : **dc=ibm,dc=com**

__ c. Distinguished name of a base entry in this repository : **dc=ibm,dc=com**

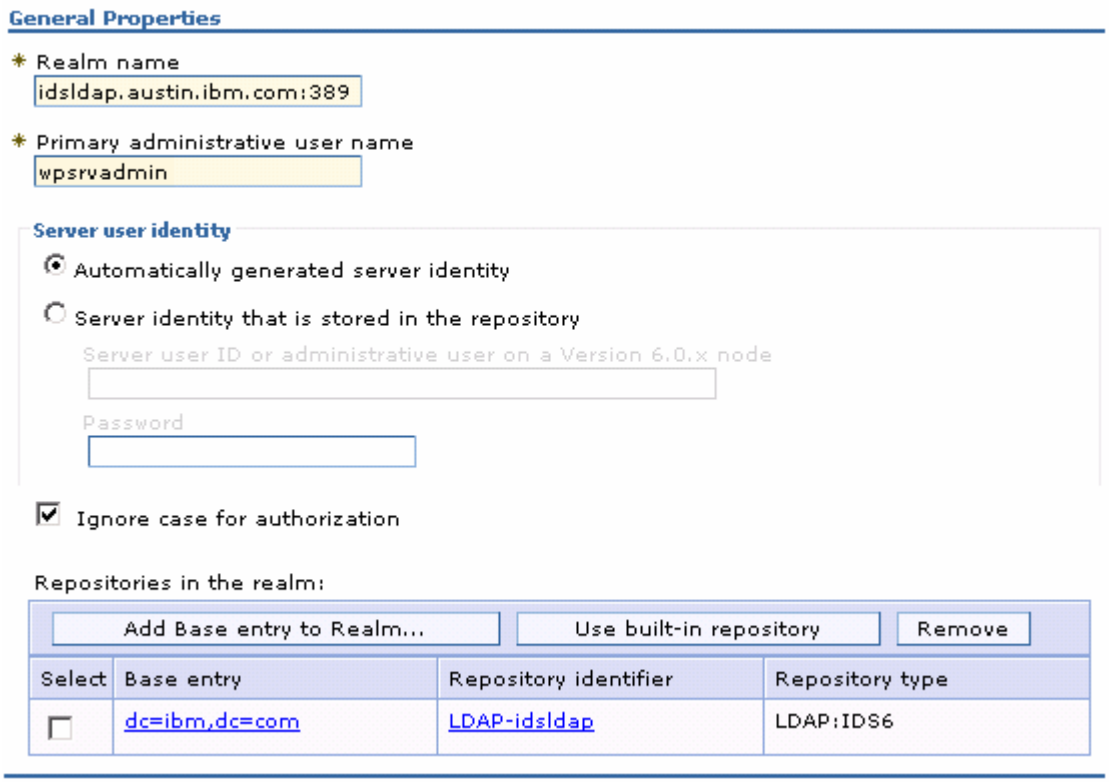


____ 19. Click **OK**

____ 20. The '**Federated repositories**' panel will look like the picture shown below:



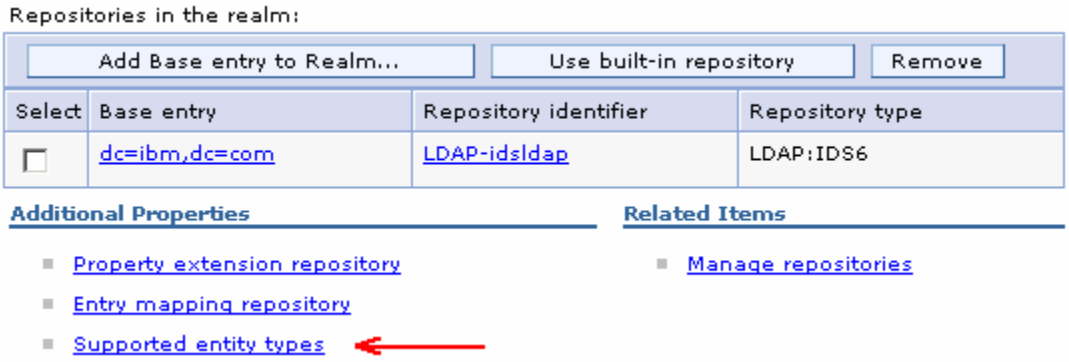
____ 21. Select the check box for '**o=defaultWIMFileBasedRealm**' if it is existing (it exists if the default security is enabled) and click the **Remove** button.



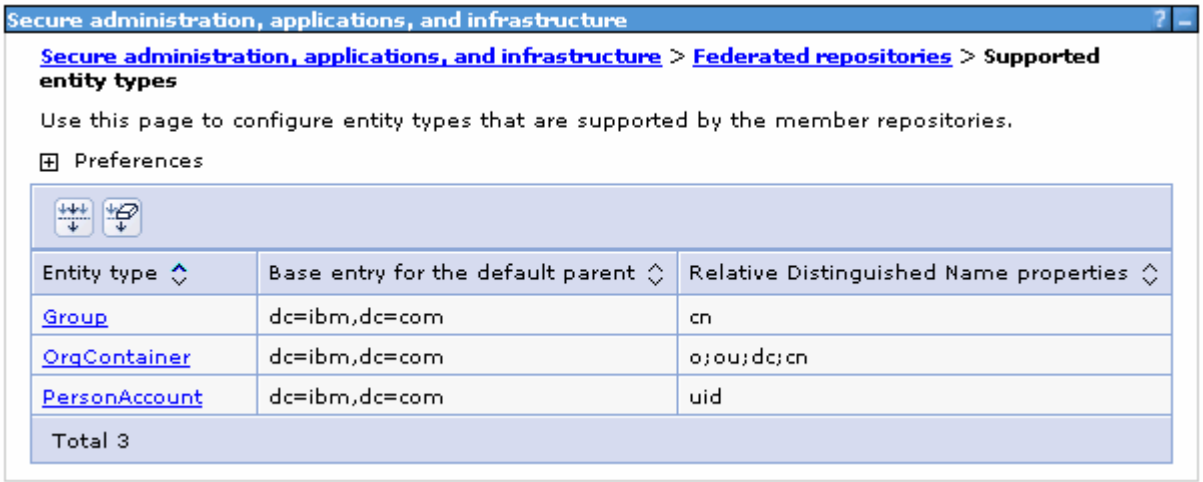
____ 22. Click **OK**.

____ 23. Configuring supported entity types in a federated repository configuration

__ a. In the **Federated Repositories** panel, click the '**Supported entity types**' under the '**Additional Properties**' section



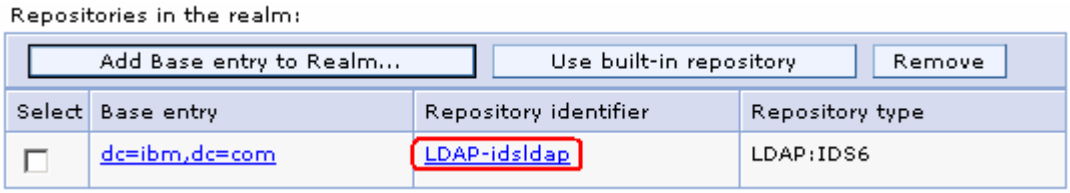
__ b. In the '**Supported entity types**' panel, update the '**Base entry for default parent**' values for **Group**, **OrgContainer** and **PersonAccount** with '**dc=ibm,dc=com**' and accept the defaults for the '**Relative Distinguished Name properties**'. The '**Supported entity types**' panel will look like the picture below:



__ c. Save to the master configuration

____ 24. Configure the LDAP entity types

__ a. While you are in the '**Federated repositories**' panel (**Secure administration, applications and infrastructure → Federated repositories**), click the '**Repository identifier**' link, (Example:- **LDAP-idsldap**)



__ b. In the following panel, scroll to the bottom and click the '**LDAP entity types**' link under the '**Additional Properties**' section

__ c. In the following '**LDAP entity types**' panel, update the following for the **Group**, **OrgContainer** and **PersonAccount** entity types:

1) Group

- Object classes : **groupOfUniqueNames**
- Search bases : **dc=ibm,dc=com**
- Search filter : **(objectclass=groupOfUniqueNames)**

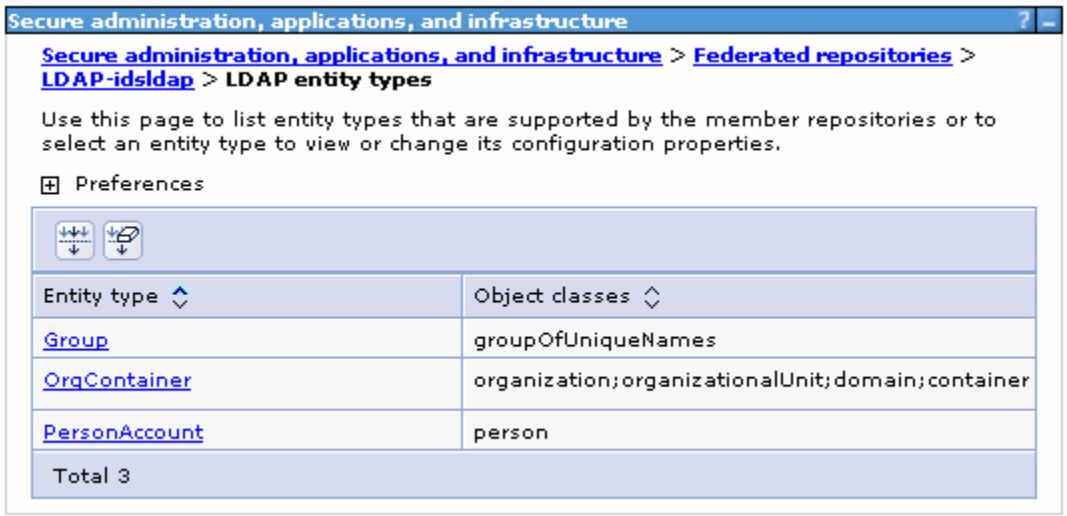
2) **OrgContainer**

- <Accept the defaults>

3) **PersonAccount**

- Object classes : **person**
- Search bases : **dc=ibm,dc=com**
- Search filter : **(objectclass=person)**

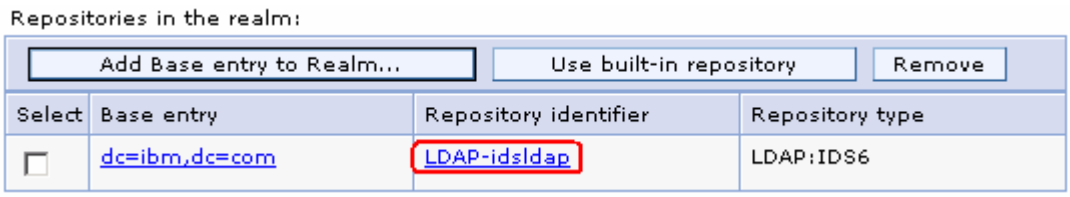
4) The '**LDAP entity**' panel will look like the picture below:



__ d. Save to the master configuration

____ 25. Configure group attribute definition

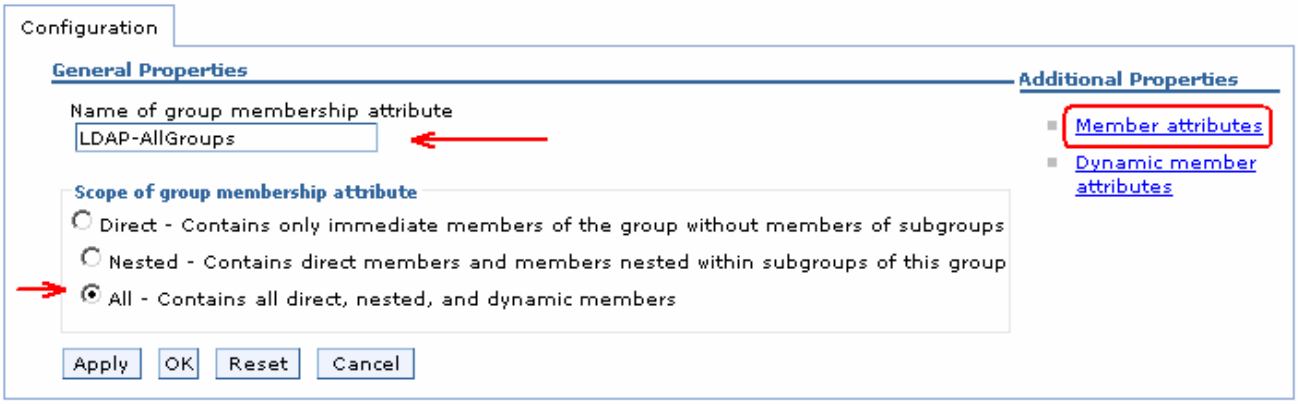
__ a. While you are in the '**Federated repositories**' panel (**Secure administration, applications and infrastructure → Federated repositories**), click the '**Repository identifier**' link, (Example:- **LDAP-idsldap**)



__ b. In the following panel, scroll to the bottom and click the '**Group attribute definition**' link under the '**Additional Properties**' section

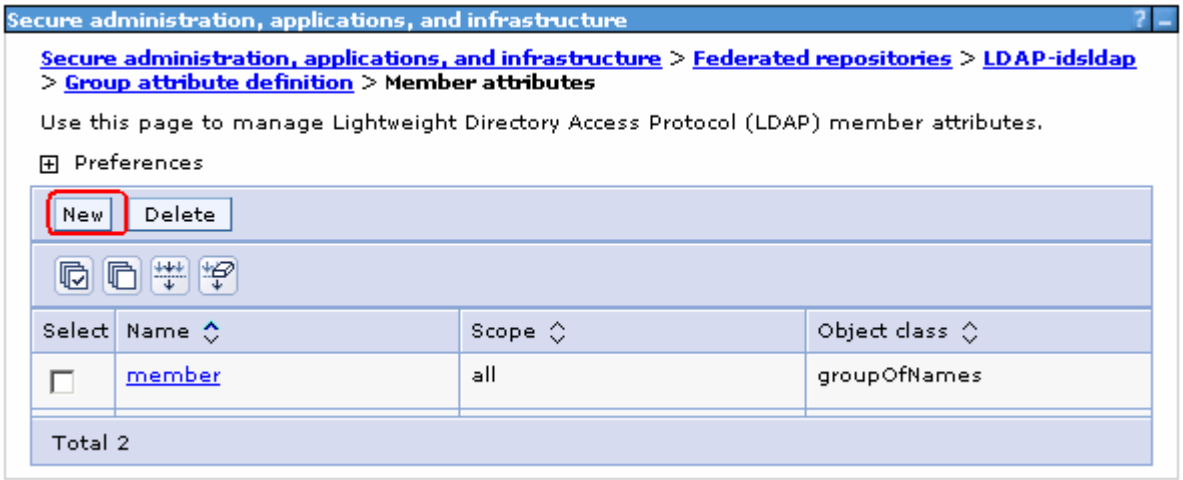
__ c. In the following '**Group attribute definition**' panel, enter the following information:

- Name of group membership attribute : **LDAP-AllGroups**
- For the scope, select the check box for '**All- Contains all direct, nested and dynamic members**'



- Click **Apply**

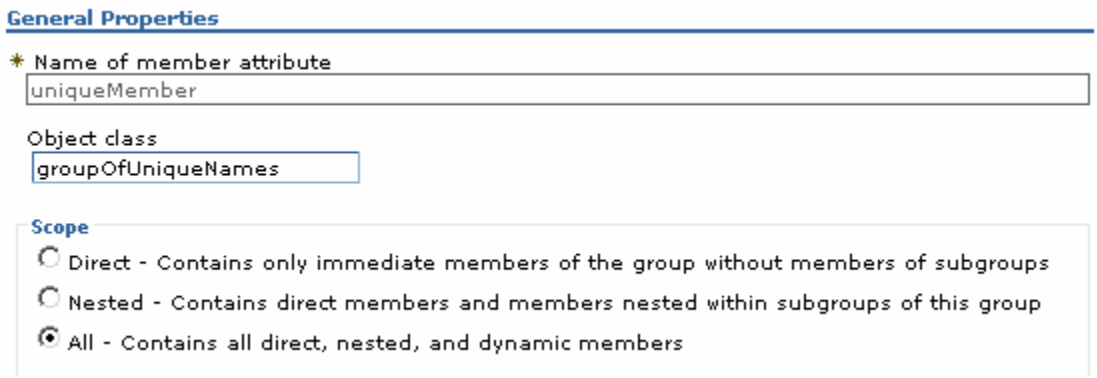
__ d. While you are in the '**Group attribute definition**' panel, click the '**Member attributes**' link under '**Additional properties**' sections



__ e. In the following panel, click the **New** button to create a new member attribute

__ f. In the following panel, enter the following information:

- Name of member attribute : **uniqueMember**
- Object class : **groupOfUniqueNames**
- For the scope, select the check box for '**All- Contains all direct, nested and dynamic members**'

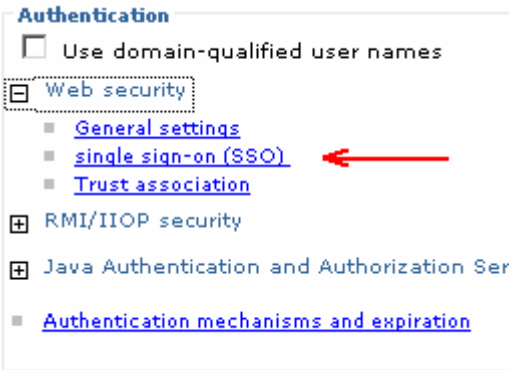


- Click **OK**

__ g. Save to the master configuration

____ 26. Configure 'Cross Cell Single Sign-on'

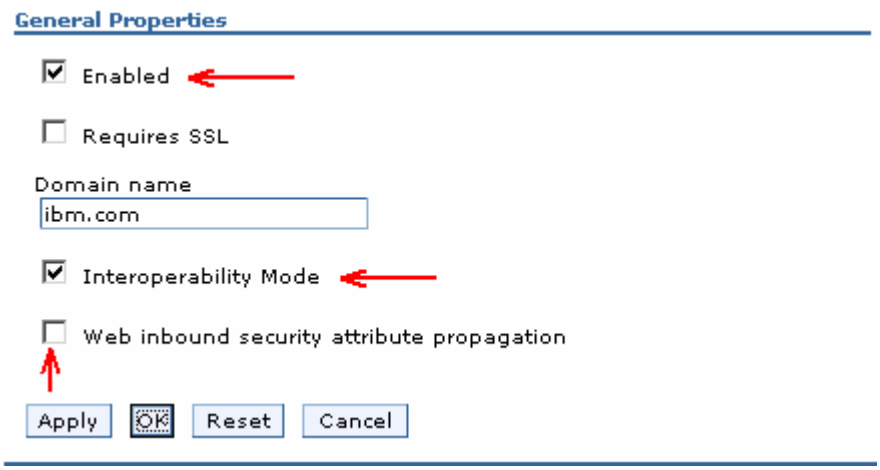
__ a. While you are in the '**Secure administration, applications and infrastructure**' panel, expand '**Web Security**' under the '**Authentication**' category



__ b. Click the '**single sign-on (SSO)**' link

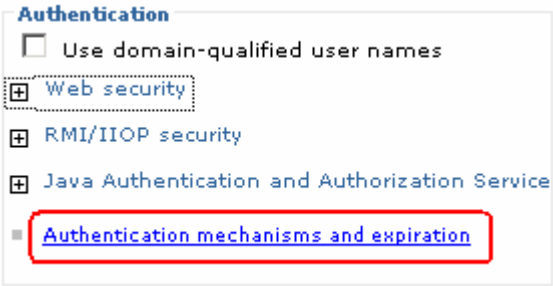
__ c. In the following '**single sign-on (SSO)**' panel, do the following:

- Select the check box for '**Enabled**'
- Ensure the check box for '**Required SSL**' is **not** selected
- Domain name : **ibm.com**
- Select the check box for '**Interoperability Mode**'
- **Unselect** the check box for '**Web bound security attribute propagation**'



____ 27. Click **OK**. You will be directed to the '**Secure administration, applications and infrastructure**' panel again

____ 28. While you are in the '**Secure administration, applications and infrastructure**' panel, click the '**Authentication mechanisms and expiration**' link



____ 29. In the following '**Authentication mechanisms and expiration**' panel, enter the following under the '**Cross-cell single sign-on**' category to import the key file that you had exported on the portal (dashboard) server machine

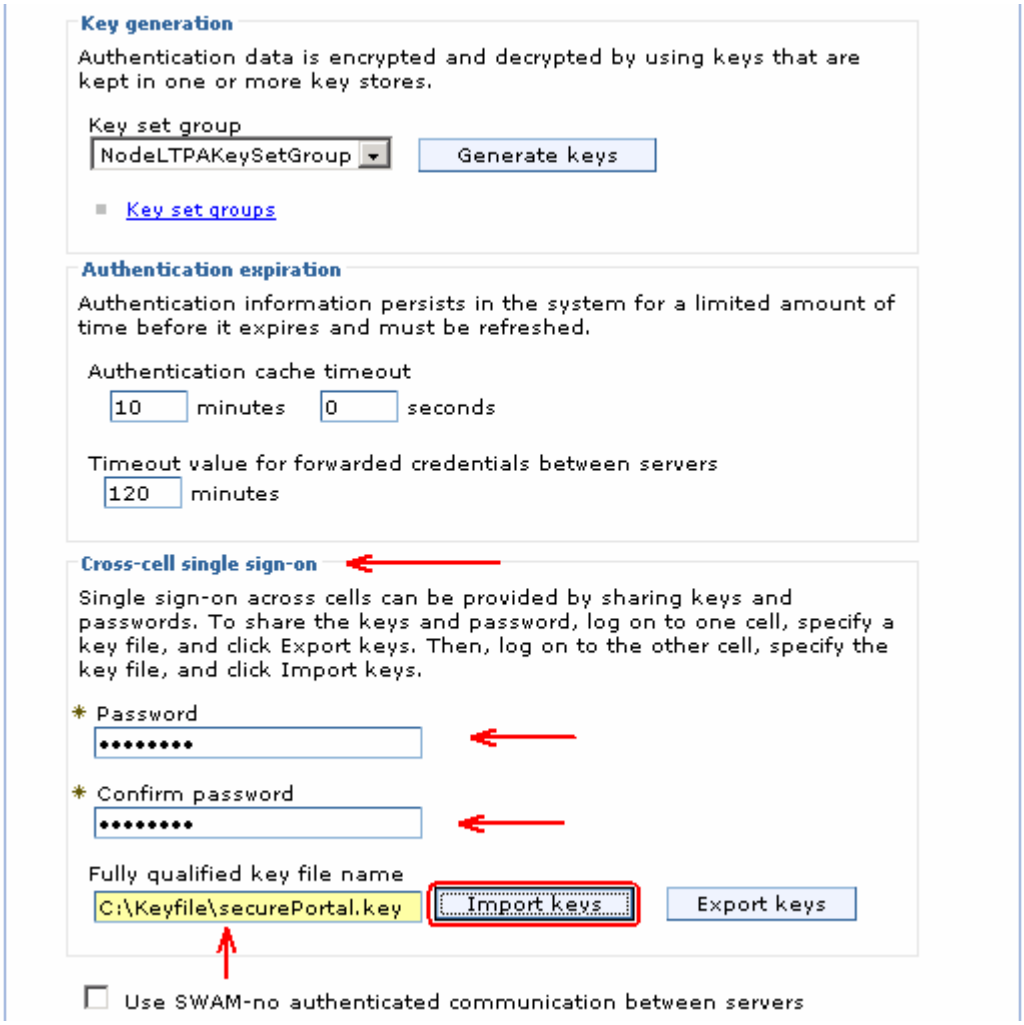
---

Note: Enter the LTPA password that you specified when you Enabled LDAP Security for Portal, and enter the LTPA key file name that you specified near the end of the "LDAP Security for Portal" configuration.

__ a. Password : **password**

__ b. Confirm password : **password**

__ c. Fully Qualified Key file name : Example:- **C:\KeyFile\securePortal.key**



____ 30. Click the '**Import Keys**' button

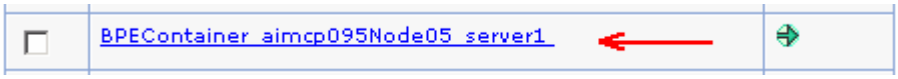
____ 31. Click the **Save** link, to save the configuration

Note: To restart the server at this time, you should enter the old user name and password configured during the WebSphere Process Server profile creation.

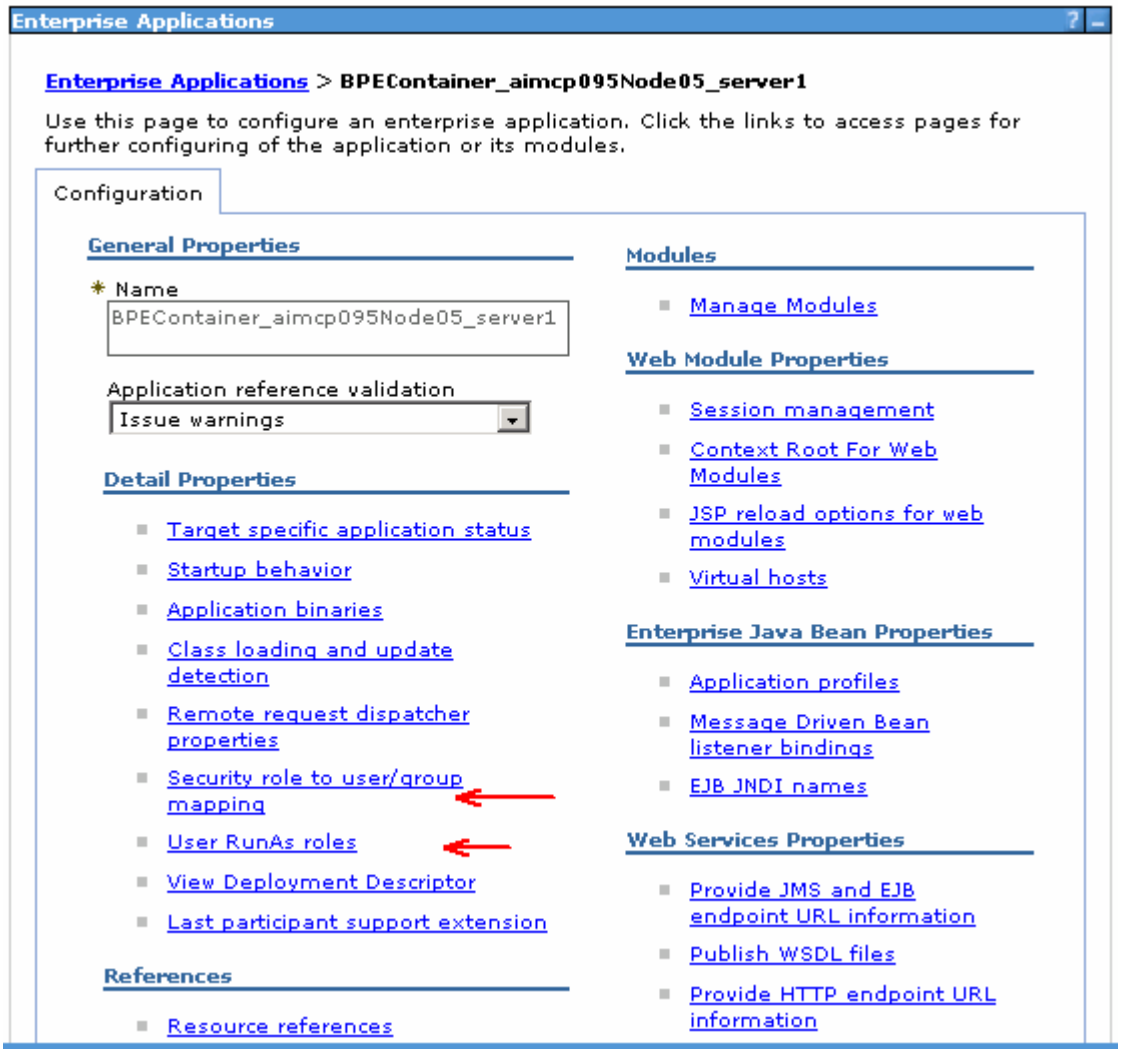
→Update security role mappings for BPE container and task container

____ 1. In the left navigation pane of the administrative console, expand '**Applications**' and click the '**Enterprise Applications**' link

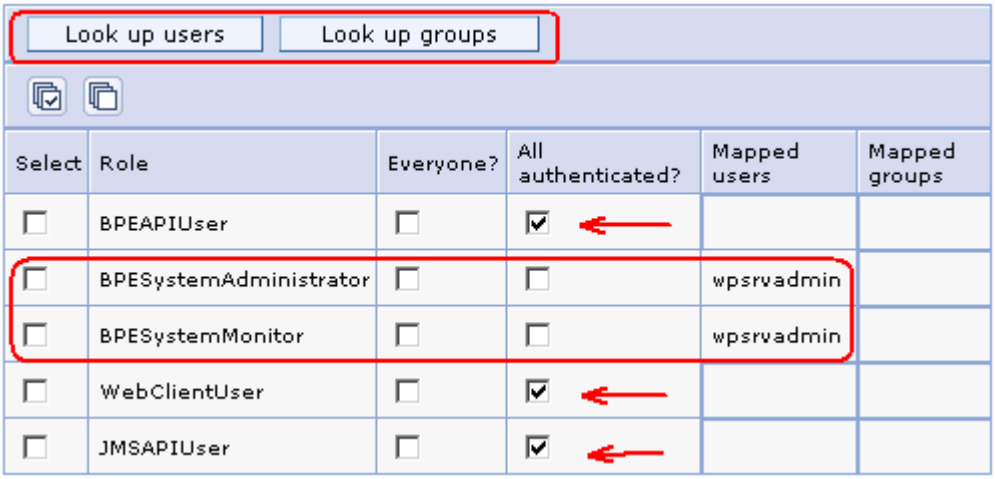
____ 2. In the following '**Enterprise Applications**' panel, click the '**BPEContainer_<NODE_NAME>_server1**' link



____ 3. In the following panel, click the '**Security role to user/group mapping**' link under the '**Detail Properties**' section

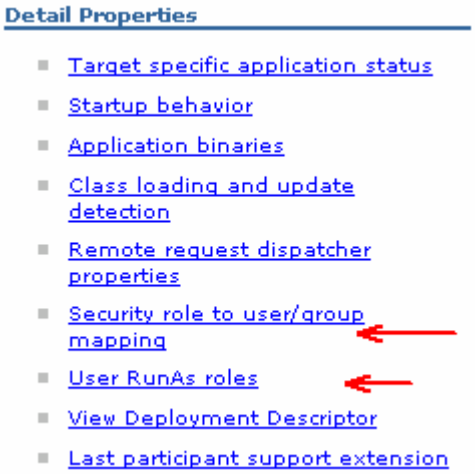


____ 4. In the flowing panel, select the check boxes for '**BPESystemAdministrator**' and '**BPESystemMonitor**' roles, click the '**Look up users**' button and map the user ID (Example: wpsrvadmin). Also select the check boxes in the '**All Authenticated**' column for '**BPEAPIUser**', '**WebClientUser**' and '**JMSAPIUser**' roles



____ 5. Click **OK** and save to the master configuration

____ 6. Back to the '**BPEContainer_<NODE_NAME>_server1**' configuration panel, click the '**User RunAs roles**' link under the '**Detail Properties**' section



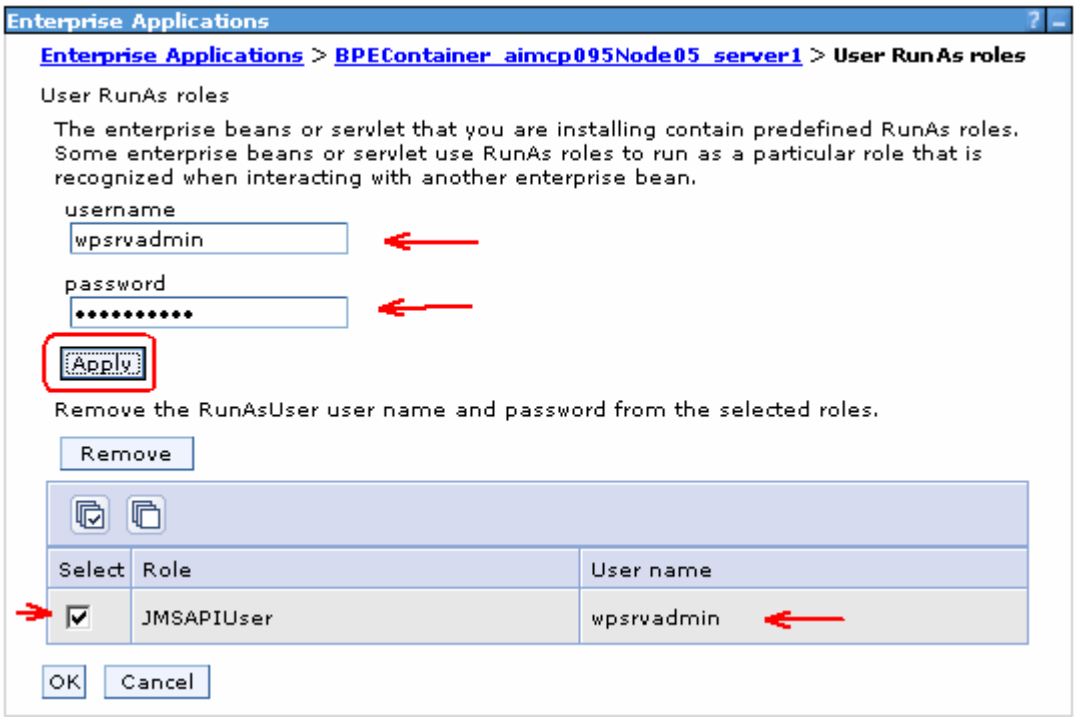
____ 7. In the following panel, update the '**JMSAPIUser**' role. Do the following:

__ a. Username : **wpsrvadmin**

__ b. Password : **wpsrvadmin**

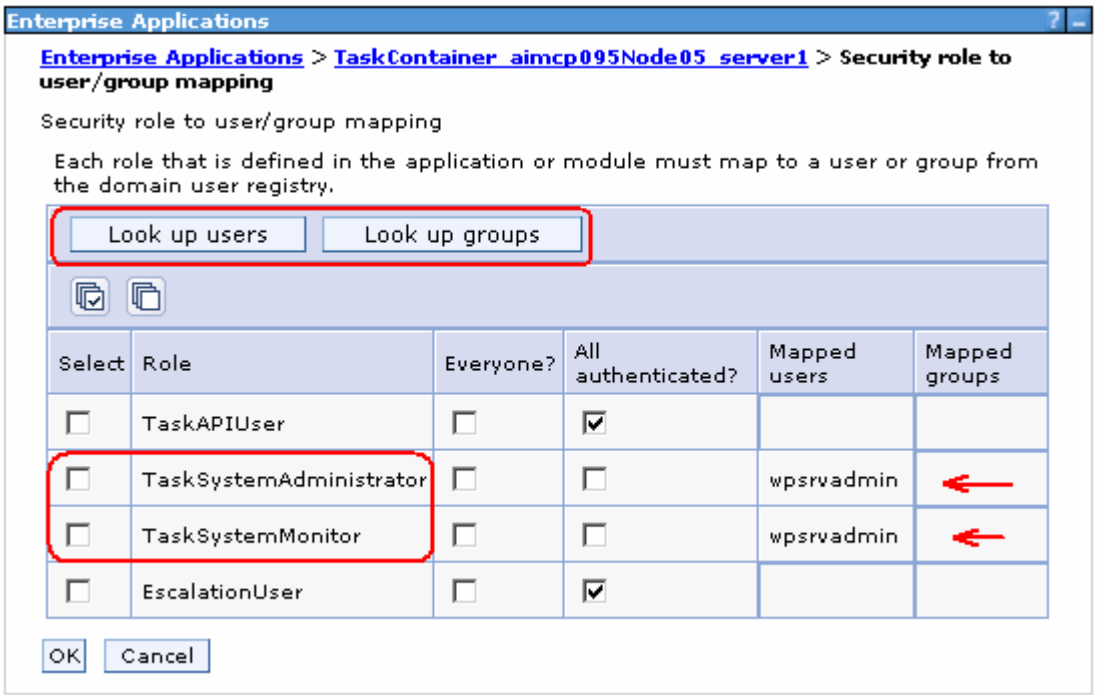
__ c. Select the check box for '**JMSAPIUser**' role

__ d. Click the **Apply** button. You should specify the JMSAPIUser



____ 8. Click **OK** and save to the master configuration

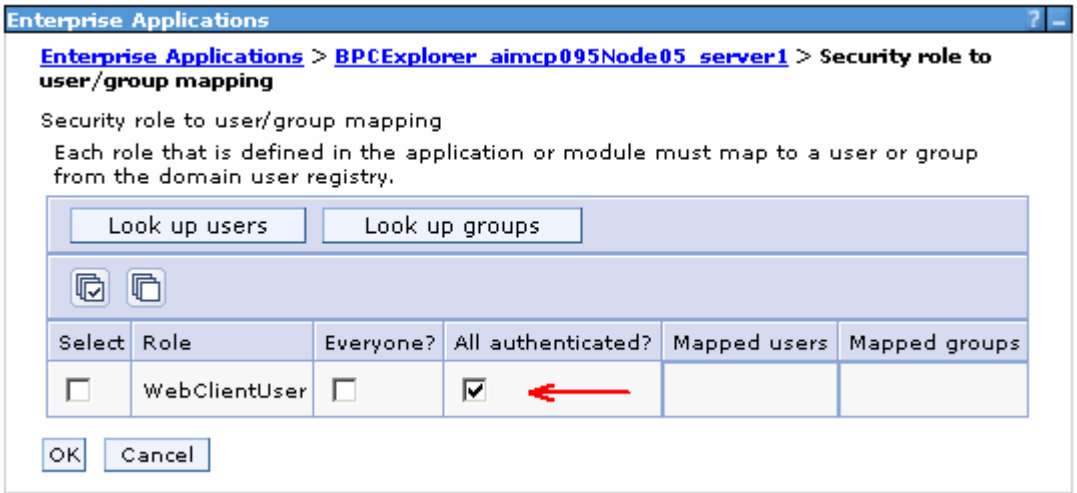
____ 9. Follow the above instructions and update the security role mappings for the '**Task Container**' named '**TaskContainer_<NODE_NAME>_server1**'. The security configuration is as show below:



____ 10. Click **OK** and save to the master configuration

____ 11. Update security role mappings for **BPC Explorer**

__ a. On the Enterprise Application page, click on **BPCExplorer_<NODE_NAME>_server1**



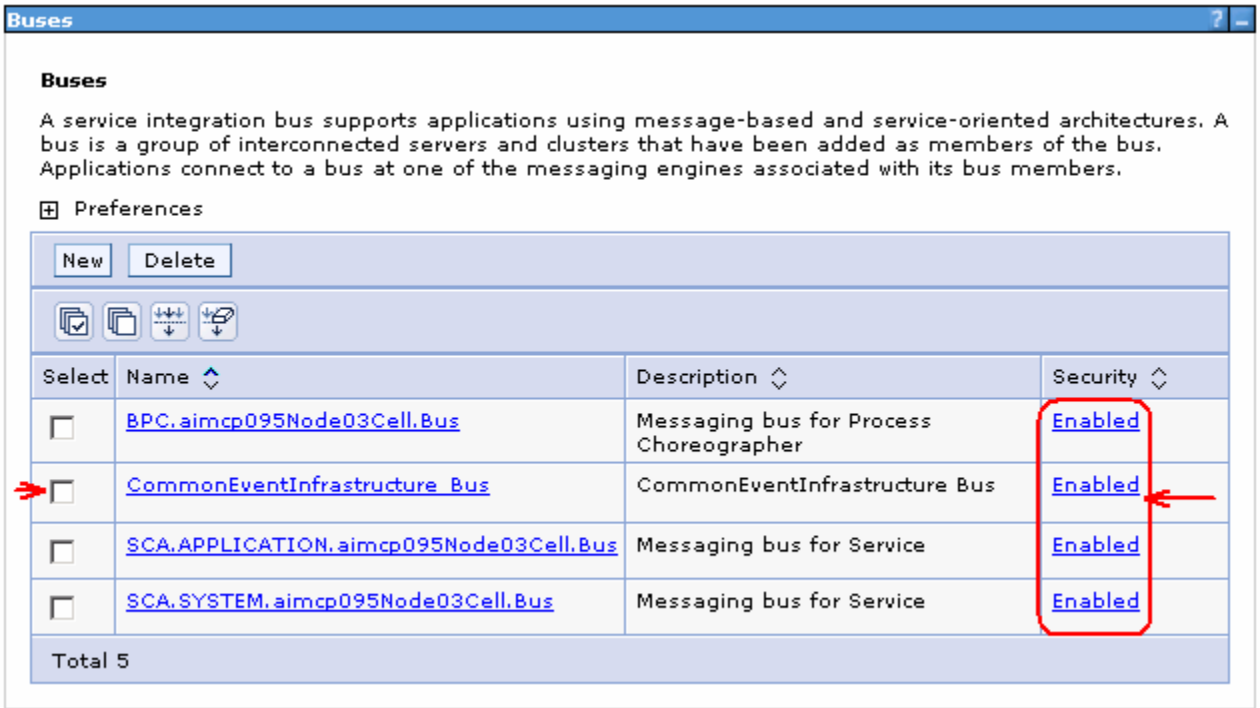
____ 12. Click **OK** and save to the master configuration

→Update J2C authentication data entries for messaging buses

This part of the lab updates the J2C authentication data entries for the messaging buses on the WebSphere Process Server.

____ 1. In the left navigation pane of the administrative console, expand '**Security**' and then click '**Bus Security**' link

____ 2. In the following '**Buses**' panel, click the '**Enabled**' link for '**CommonEventInfrastructure_Bus**'



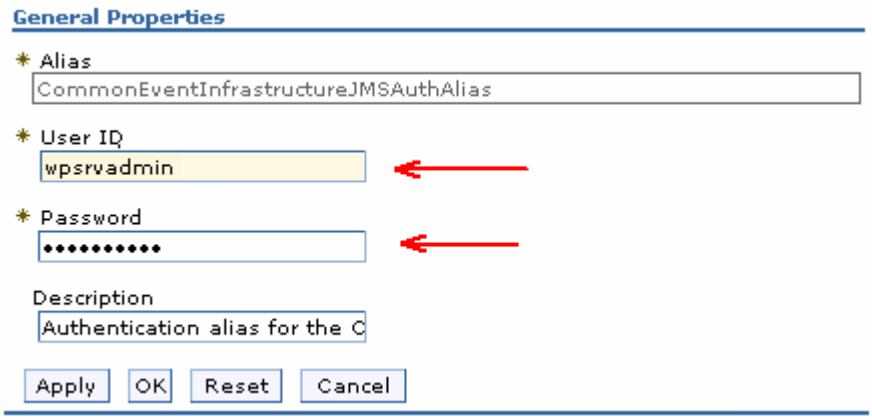
____ 3. In the following panel, click the '**J2C-authentication data**' under the '**Relation Items**' section

____ 4. In the following panel, click the '**CommonEventInfrastructureJMSAuthAlias**' link

____ 5. In the following panel, update the User ID and Password

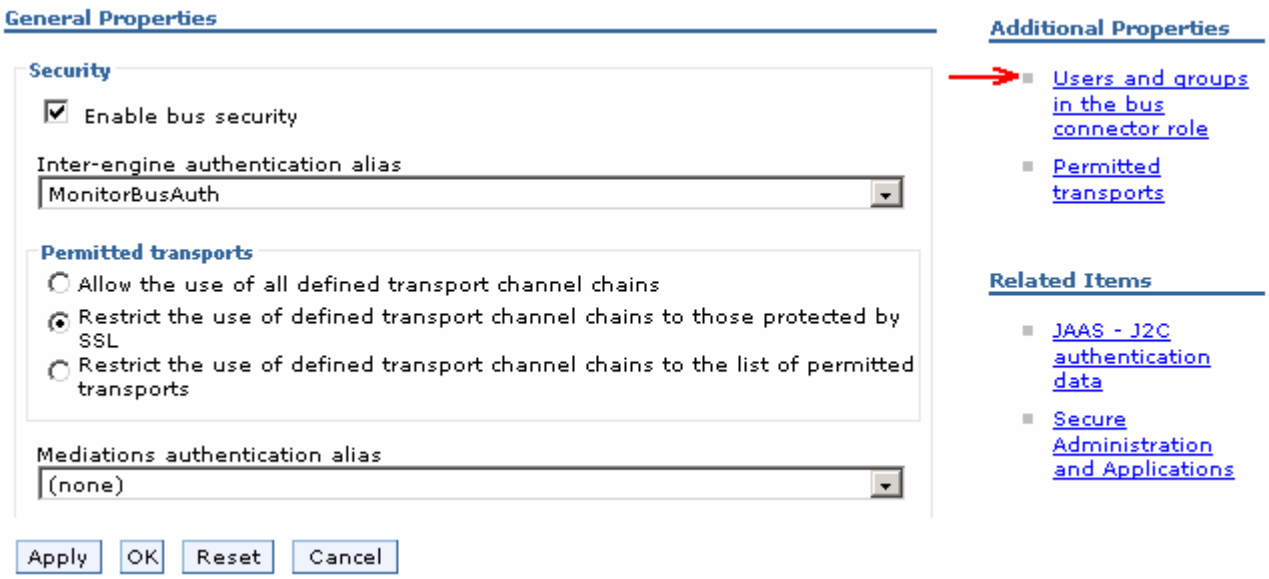
__ a. User ID : **wpsrvadmin**

__ b. Password : **wpsrvadmin**

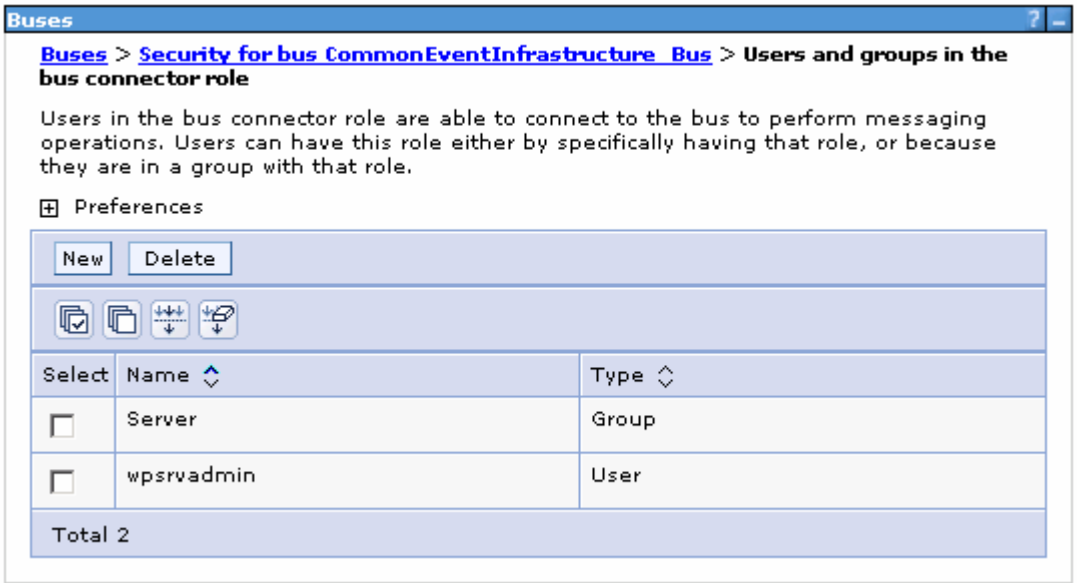


____ 6. Click **OK** and save to the master configuration

____ 7. Navigate to the '**Security → Bus Security → CommonEventInfrastructure_Bus → Enabled**' again and click the '**Users and groups in the bus connector role**' link under the '**Additional Properties**' section to the right



____ 8. In the following panel, add the group and user as shown below:



____ 9. Save to the master configuration

____ 10. Repeat the above instructions to update the J2C authentication alias data for the monitor bus named '**BPC.<CELL_NAME>.Bus**', '**SCA.APPLICATION.<CELL_NAME>.Bus**' and '**SCA.SYSTEM.<CELL_NAME>.Bus**'

Restart the Process Server profile

- stopServer.bat server1 –username was61admin –password was61admin
- startServer.bat server1
- Ensure the server is started successfully

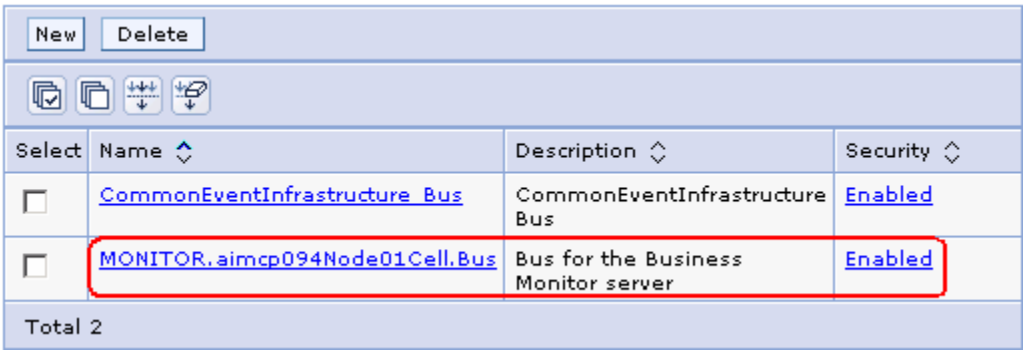
Part 5: Configure Remote CEI server to use WebSphere Business Monitor in a secured environment

In this part of the lab, you will use the cross cell files and run the cross cell script to create the remote service integration bus and create the link between the local and remote buses. This enables WebSphere Business Monitor server to receive Common Event Infrastructure (CEI) events from a remote CEI server. The instructions in this lab are good for the remote CEI server on either WebSphere Process Server V6.1 or WebSphere Process Server V6.0.2 with or with out WebSphere Business Monitor installed.

Prerequisites:-

→ The service integration bus for the local Business Monitor server has been created. By default the WebSphere Business Monitor installation wizard creates it for you. To see if the monitor service integration bus has been created, launch the WebSphere Business Monitor profile administrative console and login using the user name and password.

- In the left navigation pane, expand '**Service Integration**' and then click the '**Bus**' link
- You should see the monitor service integration bus named as '**Monitor.<CELL_NAME>Bus>**' with security '**Enabled**'



- If the monitor service integration bus does not exist on your local Monitor server installation, follow the instructions below to create one:
    - Open a command line window and change directories to WebSphere Business Monitor server profile. Example: <WBM_PROFILE_HOME>\bin (C:\IBMWebSphere\Monitor\profiles\WBMon01\bin)
    - Run the '**`monitorSIBConfig.py`**' script interactively as shown below:
        - **wsadmin –f <WBM_HOME>\scripts.wbm\sib\monitorSIBConfig.py**

        Where <WBM_HOME> is C:\IBM\WebSphere\Monitor
    - Follow the instructions and enter the required parameters when prompted

→ Ensure security is enabled on both the local WebSphere Business Monitor server and the remote WebSphere Process Server cells. Note that they both should use the one federated repository, for example LDAP.

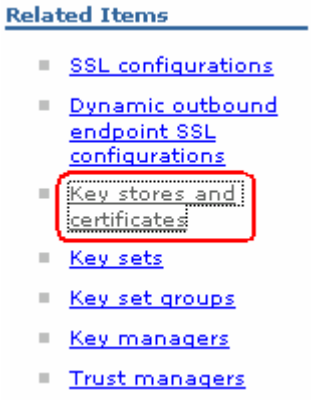
→ Ensure that LTPA authentication is configured across the WebSphere Business Monitor and WebSphere Process Server cells. For example export the LTPA key from the WebSphere Business Monitor cell and import it to WebSphere Process Server cell

→ Enable the server-to-server trust (SSL) between the servers hosting each side of the service integration bus. Follow the instructions below, to enable the server-to-server trust among the servers:

Local WebSphere Business Monitor Server:

- Login to the WebSphere Business Monitor server administrative console. In the left navigation pane, expand '**Security**' and then click the '**SSL certificate and key management**' link

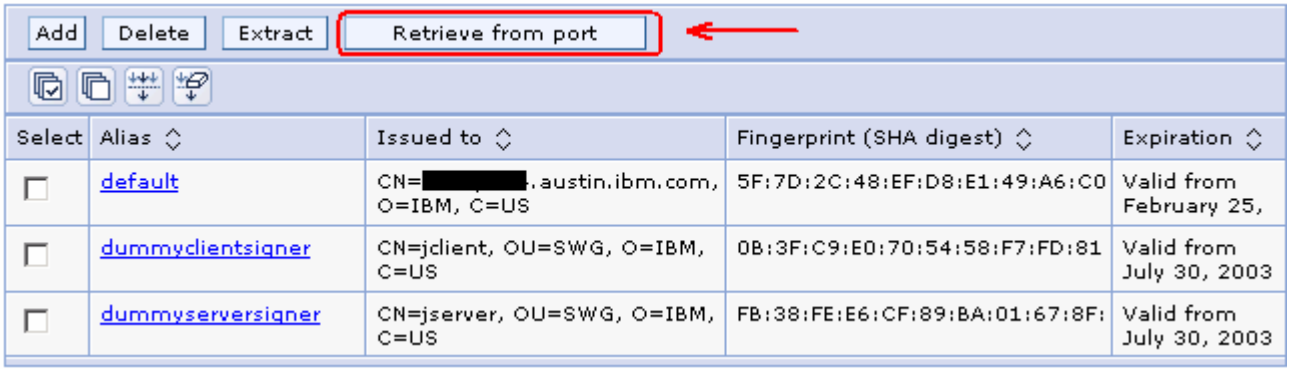
- In the following '**SSL certificate and key management**' to the right, click the '**Key stores and certificates**' link under the '**Related Items**' section



- In the following '**Key stores and certificates**' panel, click the '**NodeDefaultTrustStore**' link

- In the following '**NodeDefaultTrustStore**' panel, click the '**Signer Certificates**' link under the '**Additional Properties**' section

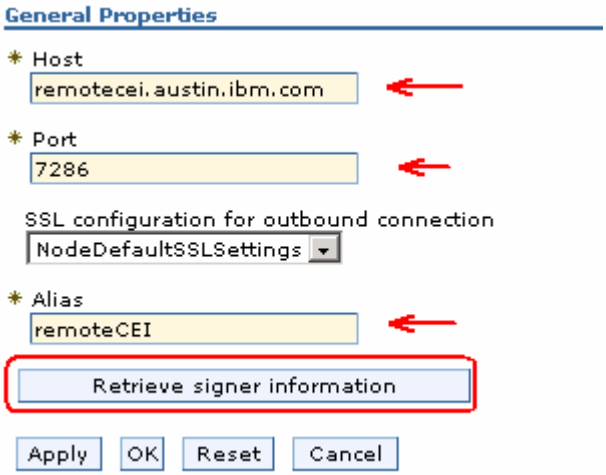
- In the following '**Signer Certificates**' panel, click the '**Retrieve from port**' button



- In the following '**Retrieve from port**' panel, enter the following information:
  - Host : **<fully qualified host name of the remote CEI Server>** (Example: remotecei.austin.ibm.com)
  - Port : **7286** (SSL port)

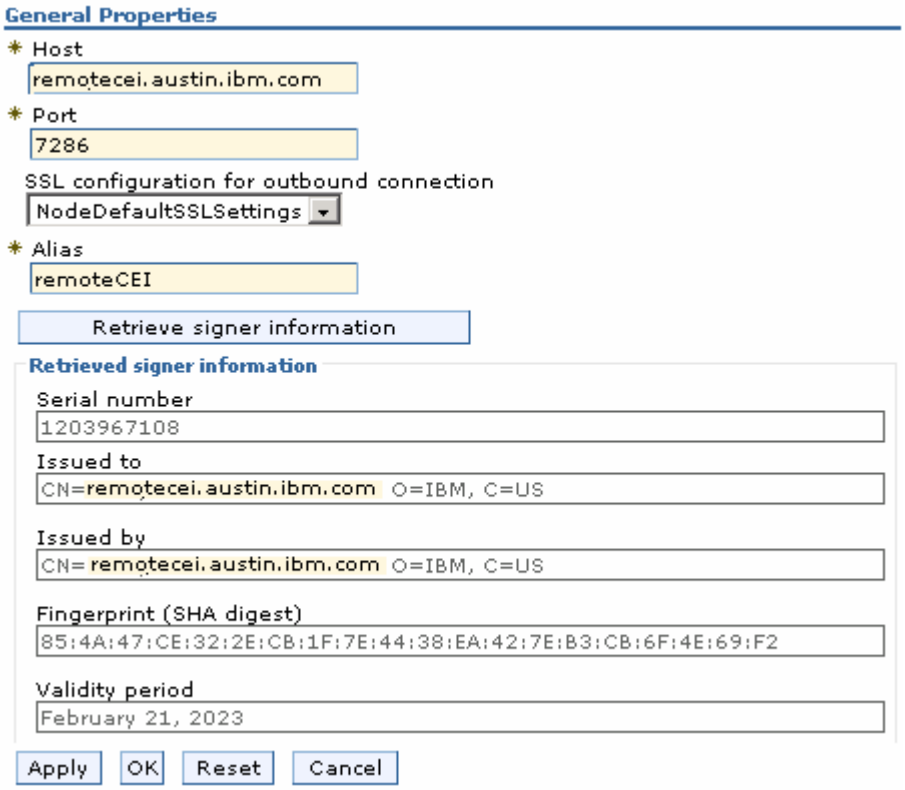
Note: To determine the correct SSL port number, log in to the WebSphere Business Monitor server administrative console; expand '**Servers**' in the left navigation pane and then click the '**Application Servers**' link. In the following application server panel to the right, click the '**server1**' link. In the following panel expand '**Ports**' under the '**Communications**' section and note down the port number corresponding to '**SIB_ENDPOINT_SECURE_ADDRESS**' port name.

  - Alias : **Example: remoteCEI**



- Click the '**Retrieve signer information**' button

- You should see the following signer information that is retrieved from the remote CEI server



- Click **OK** and save to the master configuration

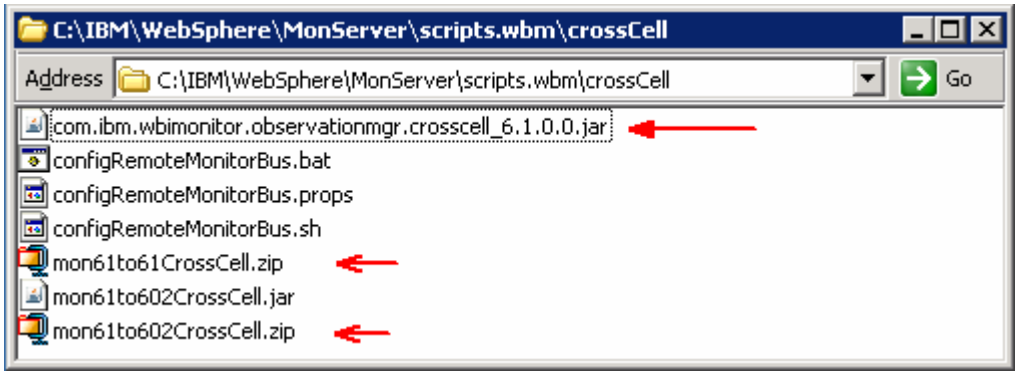
Remote CEI Server (WebSphere Process Server V6.1):

- Now you need to setup trust on the remote CEI server. So follow the above instructions but this time you will be logged on the remote CEI server in order to retrieve the signer information from the WebSphere Business Monitor Server cell

→ Create a user that is valid in both the WebSphere Business Monitor server and WebSphere Process Server for the Monitor Bus link authentication. The monitor bus link requires a user ID where the user name is valid in both the cells. However the password can be unique to each cell, but the user name must be the same.

Complete the following instructions to configure the cross cell communication between the WebSphere Business Monitor server and WebSphere Process Server cells:

____ 1. Navigate to the WebSphere Business Monitor, scripts (**scripts.wbm**) directory located at **<WBM_HOME>** (Example: C:\IBM\WebSphere\Monitor\scripts.wbm\crossCell)

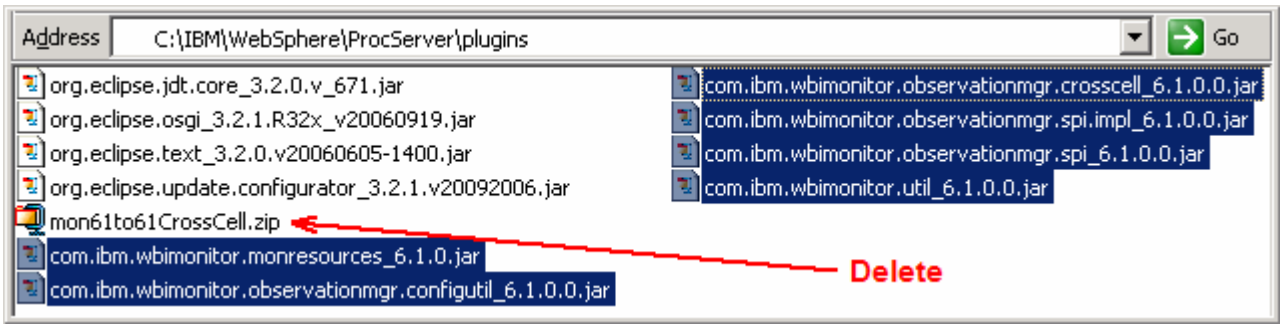


____ 2. Depending on the type of remote CEI server, take the appropriate action.

__ a. Remote CEI server on WebSphere Process Server V6.1

1) If WebSphere Business Monitor 6.1 is installed locally, but **not** on the remote CEI server:

From the **<WBM_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the **`mon61to61CrossCell.zip`** file to the **<WPS61_HOME>\plugins** directory of the remote CEI server, that is WebSphere Process Server V6.1 and extract the contents



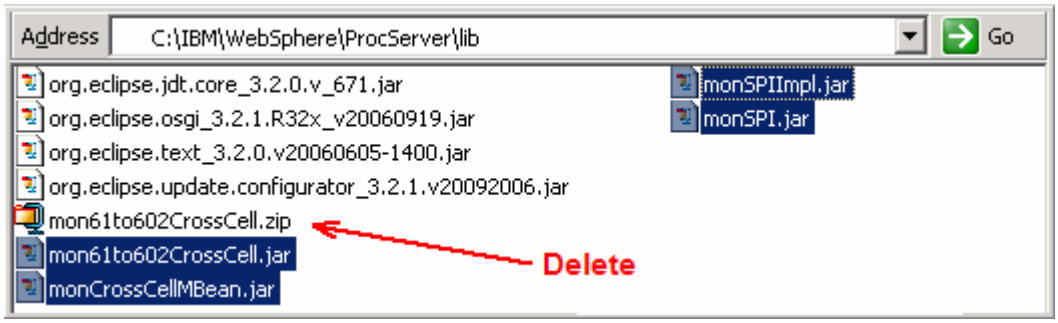
2) If WebSphere Business Monitor 6.1 is installed both locally and on the remote CEI server:

From the **<WBM_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the **`com.ibm.wbimonitor.observationmgr.crosscell_6.1.0.0.jar`** file to the **<WPS61_HOME>\plugins** of the remote CEI server, that is the WebSphere Process Server V6.1

3) From the remote CEI server's **<WPS61_HOME>/bin** directory, run the appropriate command to configure the application server to recognize the .jar files: **`osgiCfgInit.bat`** or **`osgiCfgInit.sh`**

__ b. Remote CEI Server on WebSphere Process Server V6.0.2

1) From the **<WBM_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the **`mon61to602CrossCell.zip`** file to the **<WPS602_HOME>/lib** folder of the remote CEI server, that is WebSphere Process Server V6.0.2 and extract the contents



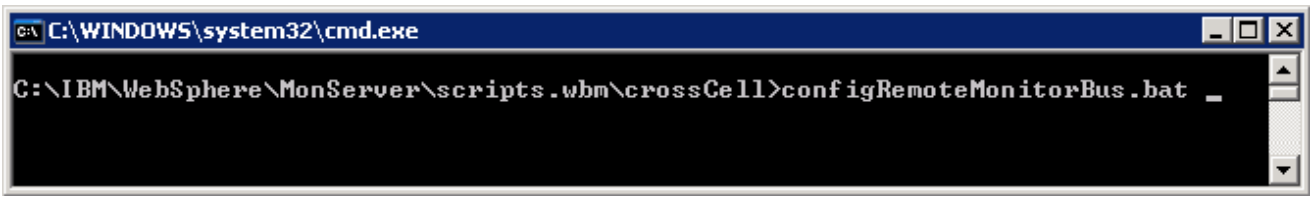
2) Restart the WebSphere Process Server

____ 3. Run the '**configRemoteMonitorBus.bat**' script on the local WebSphere Business Monitor server

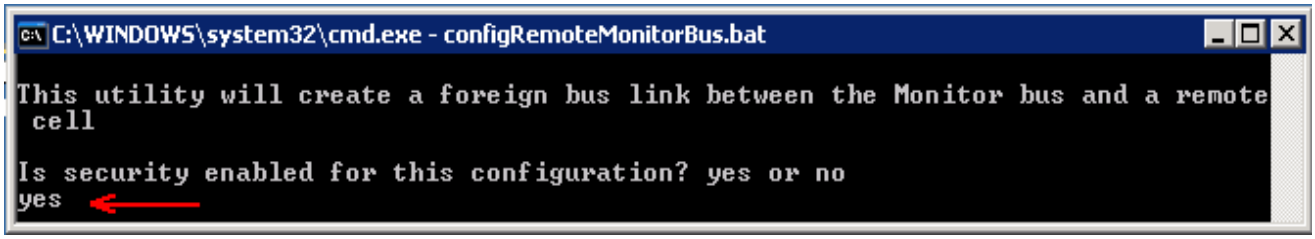
---

Note: Ensure both the WebSphere Business Monitor server and the WebSphere Process server are started at this time.

__ a. Open a command line window and change directories to **<WBM_HOME>\scripts.wbm\crossCell** and run the '**configRemoteMonitorBus.bat**' script



__ b. Type '**yes**' when prompted to answer the question '**Is security enabled for this configuration?**'



__ c. Hit the '**Enter**' key

__ d. Enter the fully qualified host name of the host machine hosting the WebSphere Business Monitor Server (Example: monitor61.austin.ibm.com)

__ e. Hit the '**Enter**' key

__ f. Enter the SOAP port of the WebSphere Business Monitor Server. (Example: **8880**)

Note: To determine the correct SOAP port number, log in to the WebSphere Business Monitor server administrative console; expand '**Servers**' in the left navigation pane and then click the '**Application Servers**' link. In the following application server panel to the right, click the '**server1**' link. In the following panel expand '**Ports**' under the '**Communications**' section and note down the port number corresponding to '**SOAP_CONNECTOR_ADDRESS**' port name.

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter the SOAP port of the server or deployment manager hosting Business Monitor
 :
Hit enter to accept the default (8880) :
8880
```

__ g. Hit the '**Enter**' key

__ h. Enter the administrative user ID for the WebSphere Business Monitor Server (Example: was61admin)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter an administrator userid for the server or deployment manager hosting Busin
ess Monitor :
was61admin
```

__ i. Hit the '**Enter**' key

__ j. Enter the password for the above user ID when prompted. (Example: was61admin). Hit the '**Enter**' key

__ k. Enter the fully qualified host name of the host machine hosting the remote CEI server, that is the WebSphere Process Server (Example: remotecei.austin.ibm.com)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter the hostname of the remote server or deployment manager hosting CEI
Hit enter to accept the default (localhost) :
remotecei.austin.ibm.com
```

__ l. Hit the '**Enter**' key

__ m. Enter the SOAP port of the remote CEI server (Example: **8880**)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter the SOAP port of the remote Server or deployment manager hosting CEI :
Hit enter to accept the default (8880) :
8880
```

__ n. Hit the '**Enter**' key

__ o. Enter the administrative user ID for the remote CEI server (Example: wpsrvadmin)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter an administrator userid for the remote server or deployment manager hostin
g CEI :
wpsrvadmin
```

__ p. Hit the '**Enter**' key

__ q. Enter the password for the above user ID when prompted. (Example: wpsrvadmin). Hit the '**Enter**' key

__ r. If prompted for a SSL Signer Certificate exchange, say '**y**' for yes

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
*** SSL SIGNER EXCHANGE PROMPT ***
SSL signer from target host [redacted] is not found in trust store C:/IBM/WebSphe
re/MonServer/profiles/WBMon01/etc/trust.p12.

Here is the signer information (verify the digest value matches what is displaye
d at the server):

Subject DN:    CN=[redacted].austin.ibm.com, O=IBM, C=US
Issuer DN:     CN=[redacted].austin.ibm.com, O=IBM, C=US
Serial number: 1203967108
Expires:       Tue Feb 21 13:18:28 CST 2023
SHA-1 Digest:  85:4A:47:CE:32:2E:CB:1F:7E:44:38:EA:42:7E:B3:CB:6F:4E:69:F2
MD5 Digest:    AE:59:BE:02:86:F2:CE:68:CA:9E:CD:4A:51:EA:0B:AE

Add signer to the trust store now? (y/n) y
```

__ s. Hit the '**Enter**' key

__ t. Say '**yes**' to use the defaults when configuring the messaging engine.

Note: Additional configuration is needed if you choose not to use the defaults when configuring the messaging engine. To make it simple, this lab covers only the default configuration.

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Do you want to use the defaults when configuring the messaging engine? yes or no

Hit enter to accept the default (yes) :
yes
```

__ u. Hit the '**Enter**' key

__ v. Enter the user ID for authentication with the Monitor bus in the remote cell (Example: wpsrvadmin)

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
Enter a userid for authentication with the Monitor bus in the remote cell :
wpsrvadmin
```

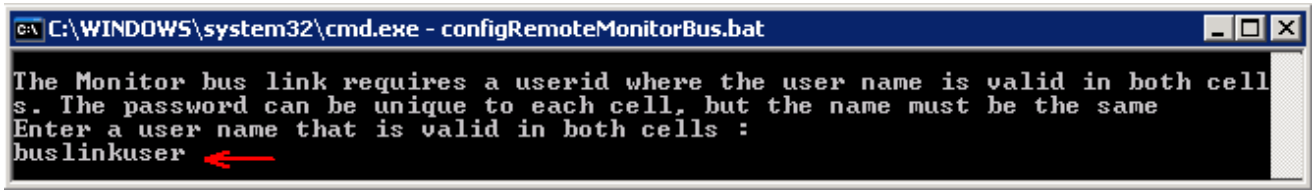
__ w. Hit the '**Enter**' key

__ x. Enter the password for the above user ID when prompted. (Example: wpsrvadmin). Hit the '**Enter**' key

__ y. Enter the user ID where the user name is valid in both the WebSphere Business Monitor and WebSphere Process Server cells

---

Note: The monitor bus link requires a user ID where the user name is valid in both the cells. However the password can be unique to each cell, but the user name must be the same.



__ z. Hit the '**Enter**' key

__ aa. Enter the password for the above user ID for the local cell, which is WebSphere Business Monitor cell when prompted. (Example: wpsrvadmin). Hit the '**Enter**' key

__ bb. Enter the password for the above user ID for the remote cell, which is WebSphere Process Server cell when prompted. (Example: wpsrvadmin). Hit the '**Enter**' key

__ cc. The remote CEI configuration progresses with the creation of remote bus named '**Monitor.<REMOTE_CELL_NAME.Bus>**' creates the foreign buses, foreign bus links and eventually saves the configuration.

__ dd. Restart both the WebSphere Business Monitor server and the WebSphere Process Server

---

Troubleshooting: If you see the following message on both the cells, it means that the server-to-server trust (SSL) across the WebSphere Business Monitor and the remote CEI server cells is not configured.

Local WebSphere Business Monitor cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=remotecei.austin.ibm.com, O=IBM, C=US" was sent from target host:port "remotecei.austin.ibm.com:7286". The signer may need to be added to local trust store "<WBM_PROFILE_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

Remote CEI Server (WebSphere Process Server) cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=monitor61.austin.ibm.com, O=IBM, C=US" was sent from target host:port "monitor61.austin.ibm.com:7286". The signer may need to be added to local trust store "<WPS_PROFILE_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

Follow the instructions from the prerequisite section of this document to configure the server-to-server trust (SSL) across the cells and then restart both the servers.

__ ee. You should see the following message in '**SystemOut.log**' of both the WebSphere Business Monitor and the remote WebSphere Process Server indicating that the monitor cross cell bus is consistent

Local WebSphere Business Monitor and **Remote CEI Server cells:**

SibMessage I [MONITOR.<CELL_NAME>.Bus:<NODE_NAME>.server1-MONITOR.<CELL_NAME>.Bus] CWSIP0382I: Messaging engine BE14D3AA1B50DA1B responded to subscription request, ***Publish Subscribe topology now consistent****.*

Part 6: Security configuration - After model deployment

After you deploy a model into a cross-cell configuration, it is necessary to perform additional security configuration for each model. The following instructions should be implemented on the remote CEI server:

→ Grant user or group Sender role access to the foreign bus:

- Open a command window and change directories to the WebSphere Process Server profile's **bin** directory

  cd <WPS_PROFILE_HOME>\bin

  Example: C:\IBM\WebSphere\ProcServer\profiles\ProcSrv01\bin

- Run the '**wsadmin**' script as shown below:

  > wsadmin –username wpsrvadmin –password wpsrvadmin

  wsadmin>

- Run the following wsadmin commands:

```
$AdminTask addUserToForeignBusRole {
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
-role Sender
-user <USER_NAME>
}

$AdminTask addGroupToForeignBusRole {
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
-role Sender
-group <GROUP_NAME>
}


$AdminConfig save
```

→ Grant user or group Sender role access to the foreign destination:

- Run the following wsadmin commands:

```
$AdminTask addUserToDestinationRole {
-type foreignDestination
-bus <BUS_NAME>
-foreignBus <FOREIGN_BUS_NAME>
-destination <DESTINATION_NAME>
-role Sender
-user <USER_NAME>
}

$AdminTask addGroupToDestinationRole {
-type foreignDestination
-bus <BUS_NAME>
```

-foreignBus <FOREIGN_BUS_NAME>
-destination <DESTINATION_NAME>
-role Sender
-group <GROUP_NAME>
}

$AdminConfig save

Example:

wsadmin> $AdminTask addUserToForeignBusRole { -bus Monitor.<REMOTECEI_CELL_NAME>.Bus –foreignBus Monitor.<WBM_CELL_NAME>.Bus -role Sender -user wpsrvadmin }

……..

……..

wsadmin> $AdminTask addUserToDestinationRole { -type foreignDestination -bus Monitor.<REMOTECEI_CELL_NAME>.Bus –foreignBus Monitor.<WBM_CELL_NAME>.Bus –destination wbm_clipsbpm_20071120175457_Q_Destination -role Sender –user wpsrvadmin }

……..

……..

wsadmin> $AdminConfig save

Troubleshooting:

→ Problem if the LTPA security configuration across the cells is missing

If you see the following exception during the monitor model deployment, which happens while retrieving the event group profile list name during the CEI configuration:

javax.naming.NoPermissionException: NO_PERMISSION exception caught [Root exception is org.omg.CORBA.NO_PERMISSION: JSAS0202E: [{0}] Credential token expired. {1} vmcid: 0x49424000 minor code: 306 completed: No]

Solution: Ensure the LTPA authentication is configured across the WebSphere Business Monitor and WebSphere Process Server cells. For example export the LTPA key from the WebSphere Business Monitor cell and import it to WebSphere Process Server cell

→ Send access to destination denied for user (CWSIA0069E: The user does not have authorization to carry out this operation). This error occurs on the remote CEI server.

The following error occurs if the user or group sender roles are not granted to the foreign bus and the foreign destination:

SibMessage W [:] CWSII0213W: The bus MONITOR.CELL_NAME.Bus denied the user <USER_NAME> access to send messages to the destination wbm_clipsbpm_20071120175457_Q_Destination.

EventDistribu E com.ibm.events.distribution.impl.EventDistribution publishEventNotifications CEIES0011E The event server failed to distribute an event notification.

Exception message: CEIES0004E No event notifications were sent because the event server could not connect to the JMS destination.

Event group name: wbm_clipsbpm_20071120175457_Group

JMS connection factory JNDI name: jms/wbm/clipsbpm/20071120175457/QF

JMS destination JNDI name: jms/wbm/clipsbpm/20071120175457/Q: CWSIA0069E: The user does not have authorization to carry out this operation. See the linked exception for details.

Solution: Grant user or group sender roles access to the foreign bus and the destination. Follow the instruction in the model deployment security configuration section of this lab.

→ SSL HANDSHAKE FAILURE

If you see the following message on both the cells, it means that the server-to-server trust (SSL) across the WebSphere Business Monitor and the remote CEI server cells is not configured.

Local WebSphere Business Monitor cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=remotecei.austin.ibm.com, O=IBM, C=US" was sent from target host:port "remotecei.austin.ibm.com:7286". The signer may need to be added to local trust store "<WBM_PROFILE_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

Remote CEI Server (WebSphere Process Server) cell:

CWPKI0022E: SSL HANDSHAKE FAILURE: A signer with SubjectDN "CN=monitor61.austin.ibm.com, O=IBM, C=US" was sent from target host:port "monitor61.austin.ibm.com:7286". The signer may need to be added to local trust store "<WPS_PROFILE_HOME>/config/cells/Node01Cell/nodes/Node01/trust.p12" located in SSL configuration alias "NodeDefaultSSLSettings" loaded from SSL configuration file "security.xml". The extended error message from the SSL handshake exception is: "No trusted certificate found".

Solution: Configure server-to-server trust (SSL) across the cells. Follow the instructions from the cross cell bus prerequisite section of this document to configure the server-to-server trust (SSL) across the cells and then restart both the servers.