

WebSphere Business Monitor V6.1

End-to-end security with a federated repository (LDAP)

What this exercise is about	2
Lab requirements	2
What you should be able to do	2
Introduction	2
LDAP information (reference)	3
User names used to complete the end-to-end security configuration	3
Part 1: Installing and configuring Tivoli Directory Server V6.0.....	4
→ Creating a new Tivoli Directory Server Instance	10
→ Configuring IBM Tivoli Directory Server	17
Part 2: Securing the Portal Server with Tivoli Directory Server V6.0.....	20
→ Disable WebSphere Application Server and Portal security:	20
→ Enable WebSphere Portal Security with LDAP:	25
Part 3: Enable security for Monitor Server profile (WebSphere Application Server V6.1).....	37
→Update J2C authentication data entries for messaging buses.....	58
Part 4: Enable security for WebSphere Process Server V6.1	61
→Update security role mappings for BPE container and task container.....	76
→Update J2C authentication data entries for messaging buses.....	80
Part 5: Configure Remote CEI server to use WebSphere Business Monitor in a secured environment.....	83
Part 6: Security configuration - After model deployment	93
Troubleshooting:	95

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	ldslldap.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
```

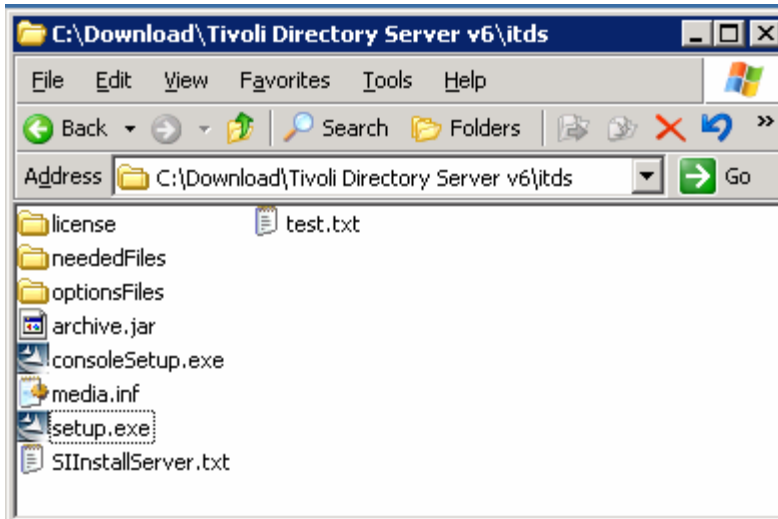
Reference: 2

```
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**



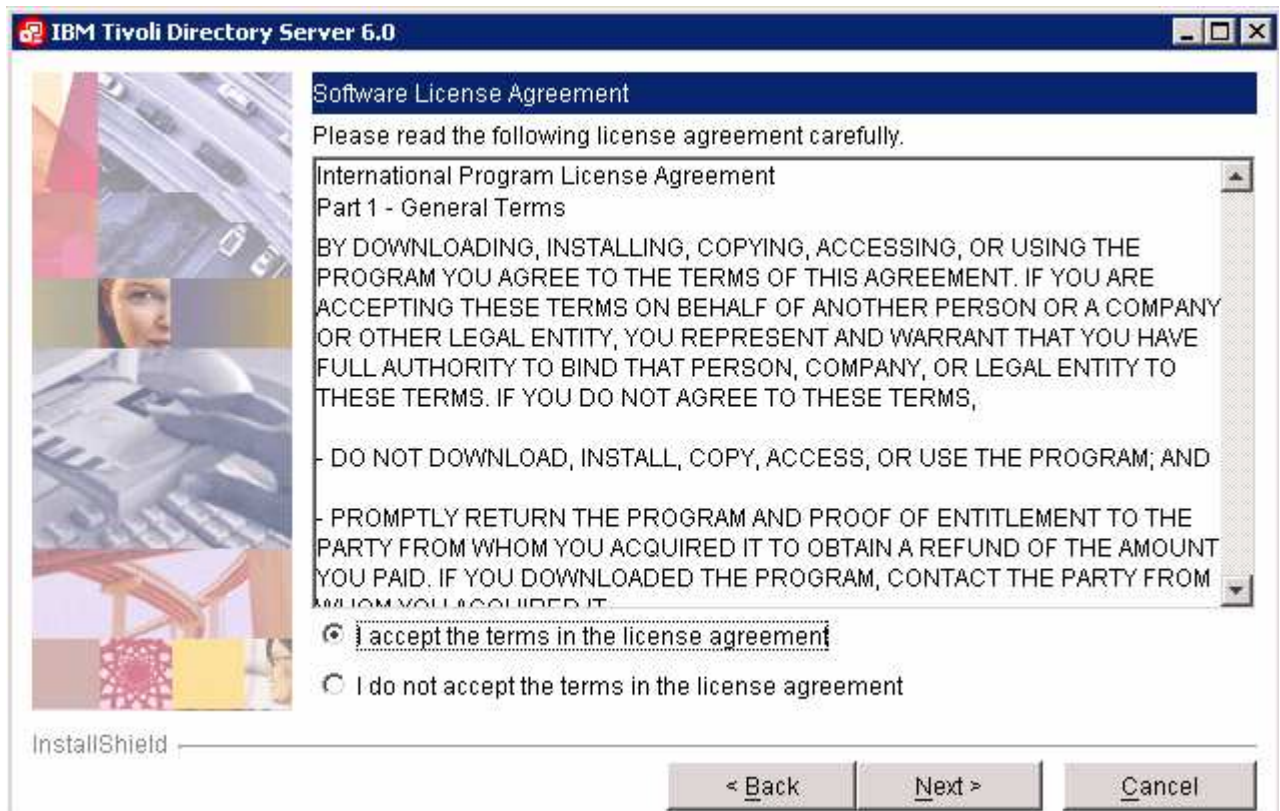
2. Select **English** as the language to be used for this wizard



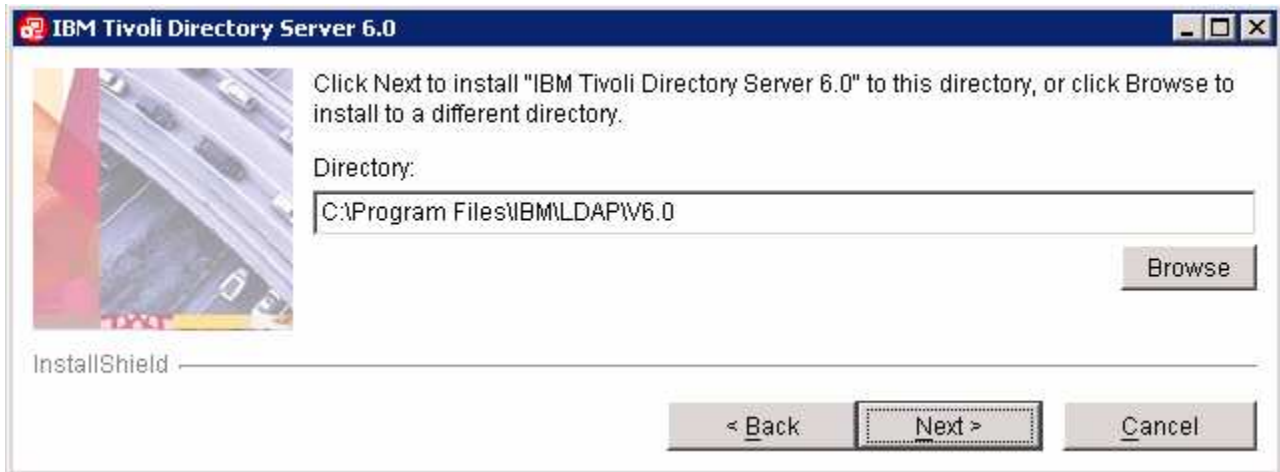
3. Click **OK**
4. Read the instructions on the Tivoli Directory Server V6.0 Welcome panel



- ___ 5. Click **Next**
- ___ 6. Read the License agreement and accept it

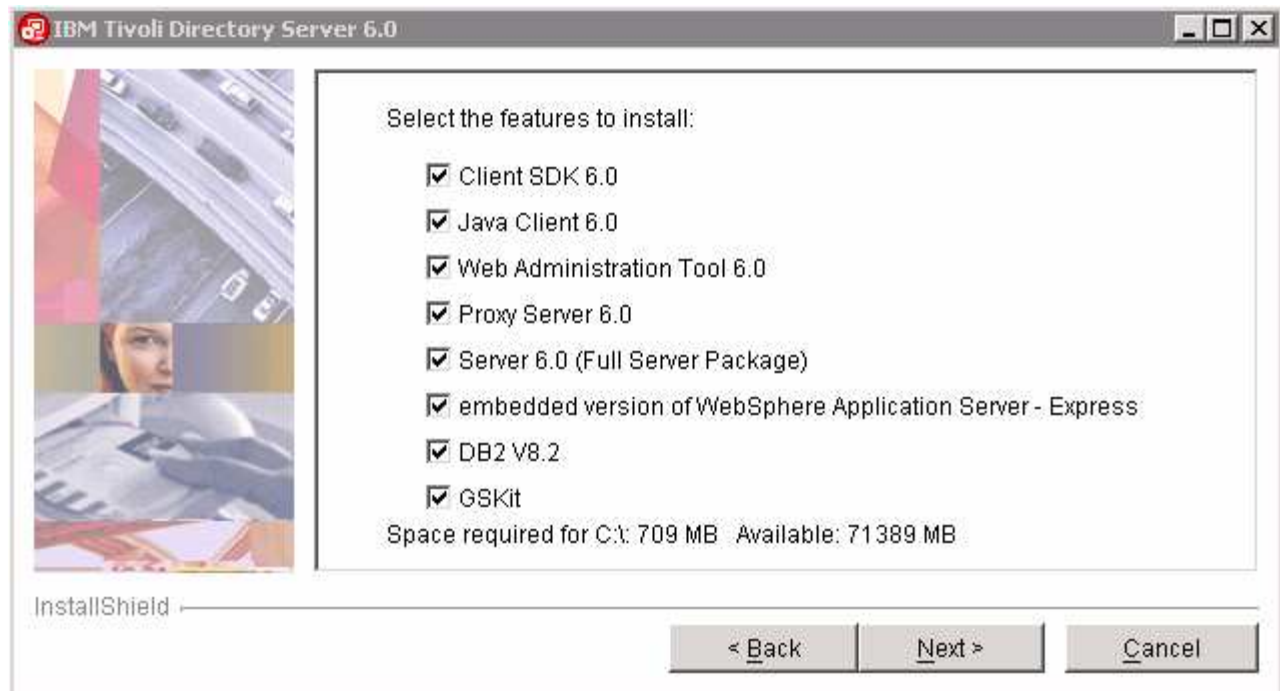


- ___ 7. Click **Next**
- ___ 8. In the following panel, accept the default **Directory Name** for the target install directory



___ 9. Click **Next**

___ 10. In the following “**Select the features to install**” panel, accept the defaults (all features)



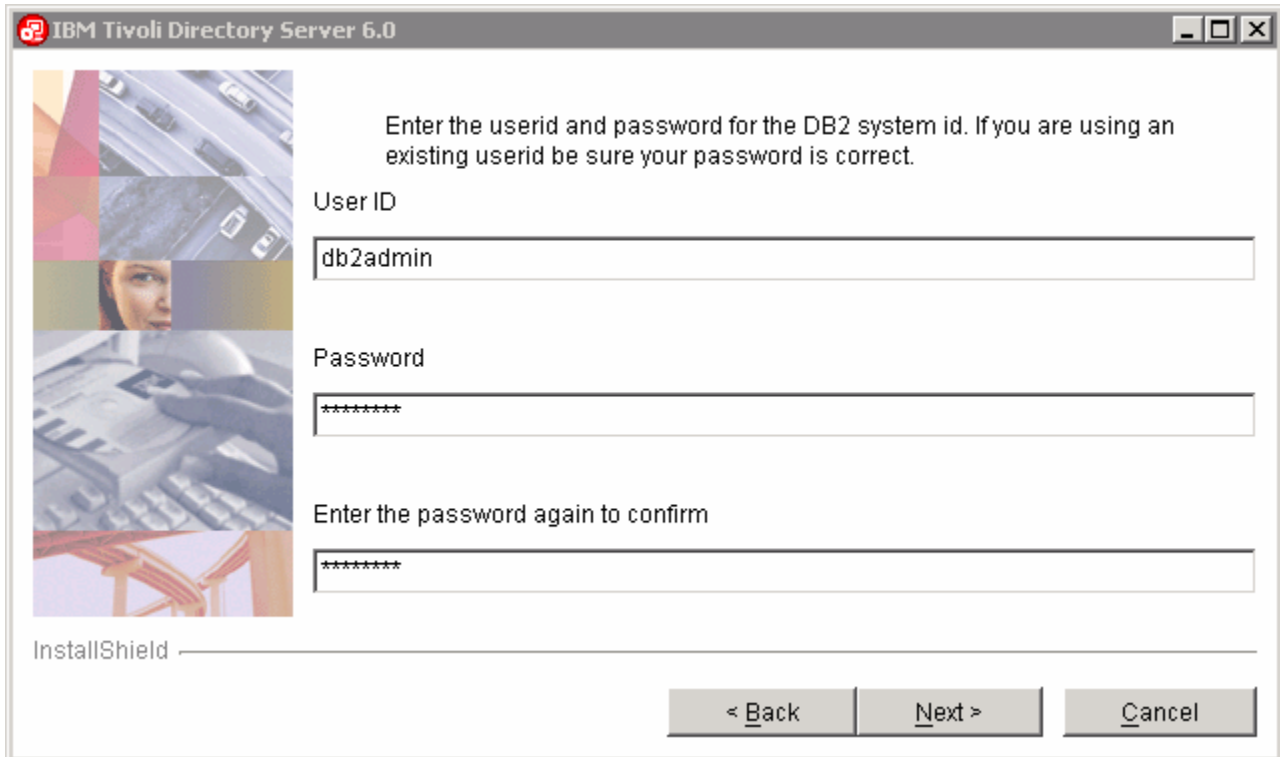
___ 11. Click **Next**

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

___ a. **User ID** : db2admin

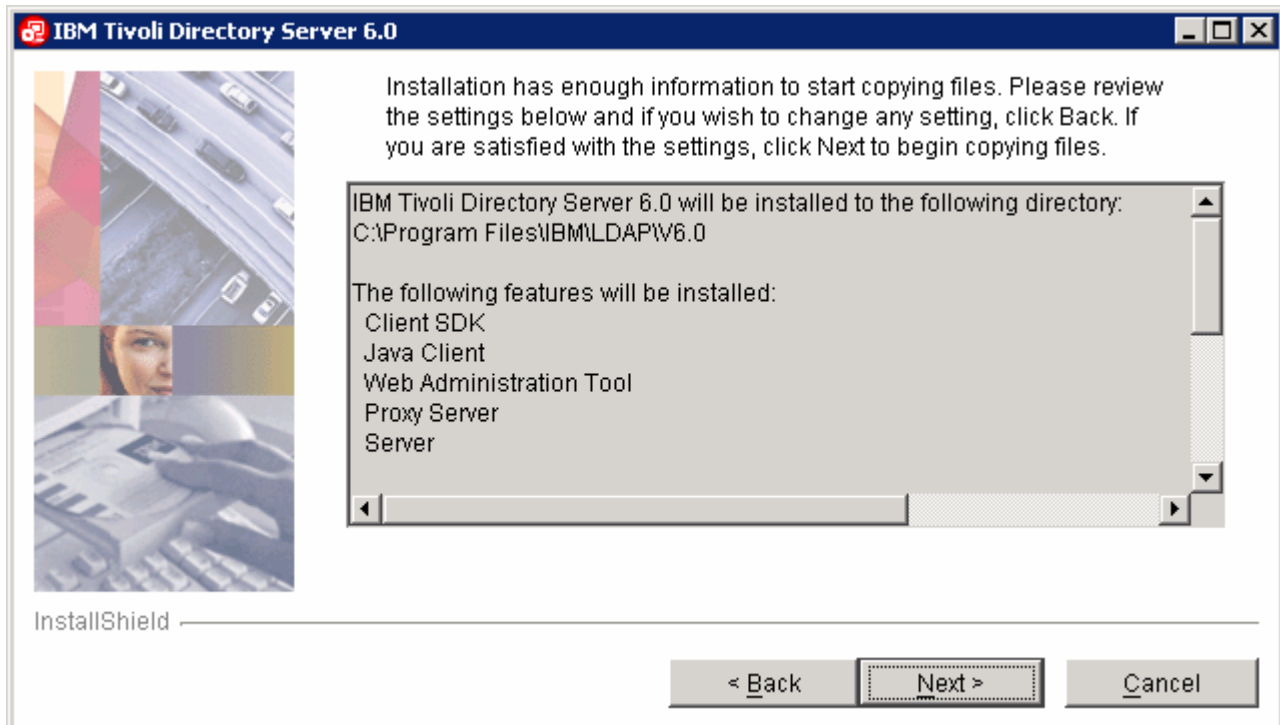
___ b. **Password** : db2admin

___ c. **Confirm Password** : db2admin



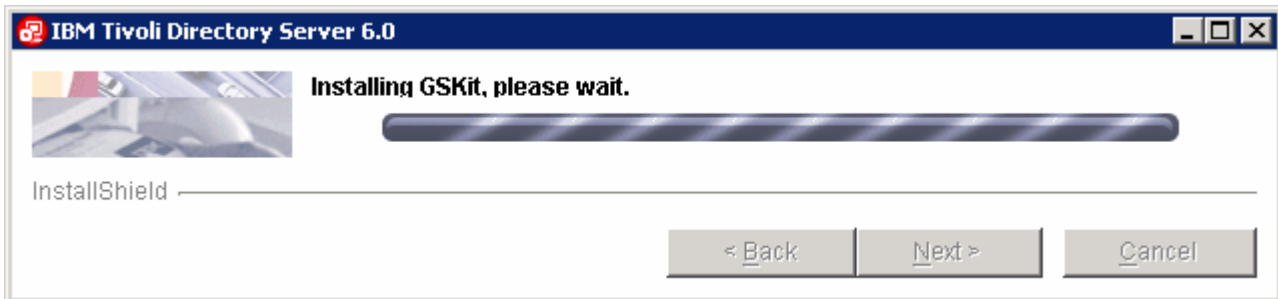
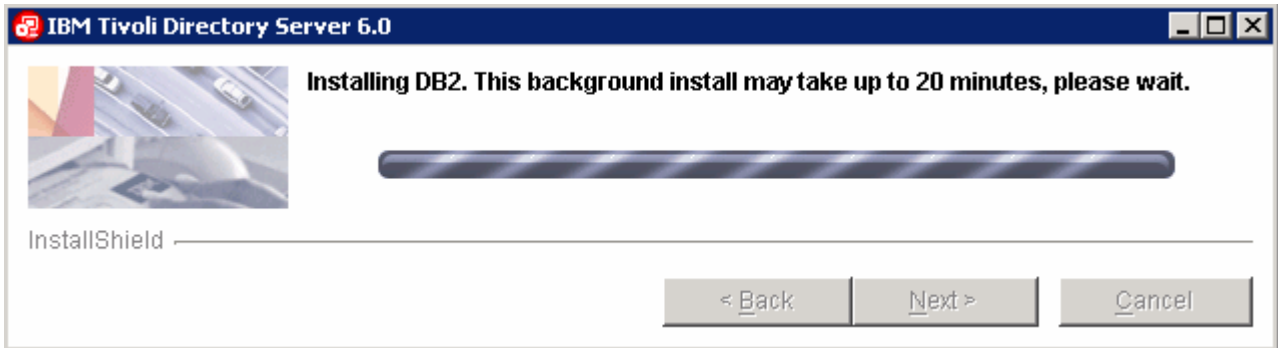
___ 13. Click **Next**

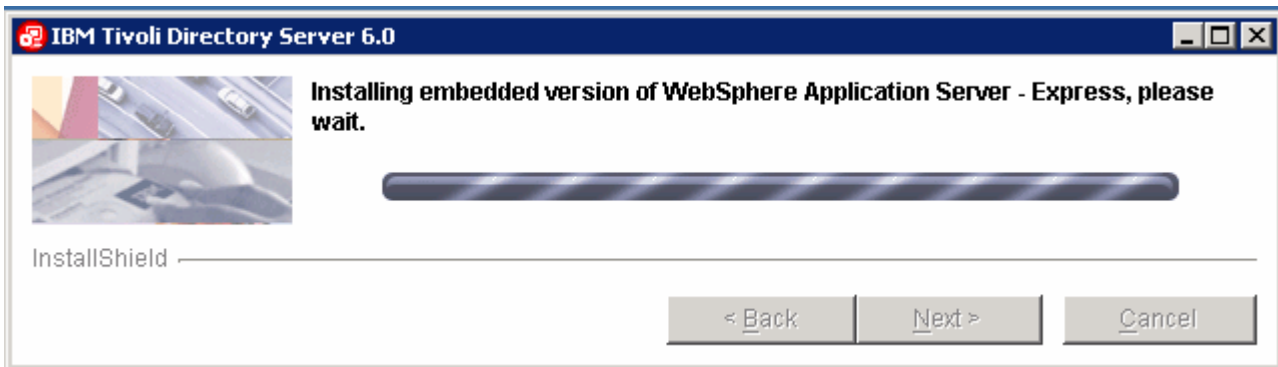
___ 14. Review the installation **Summary**



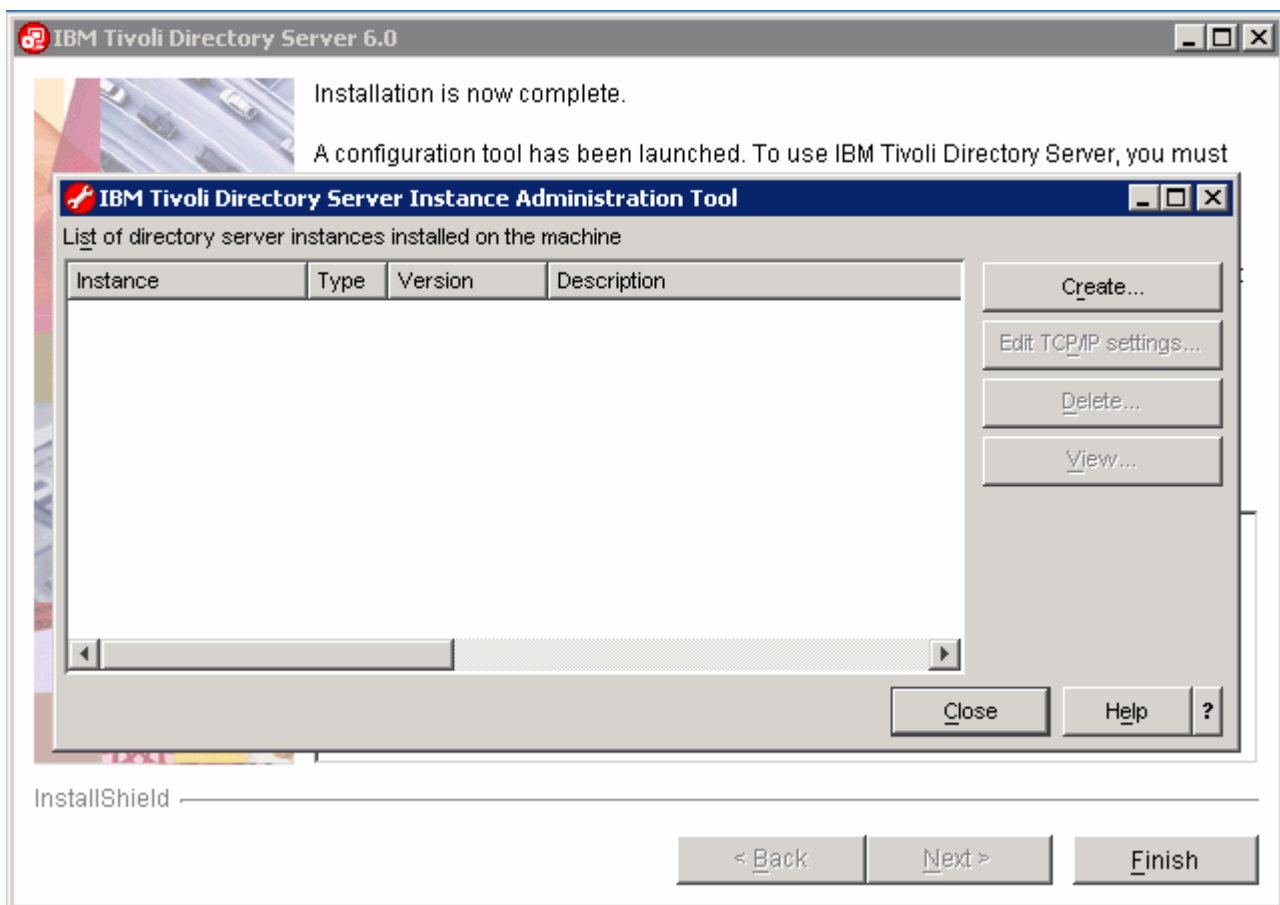
___ 15. Click **Next**

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.




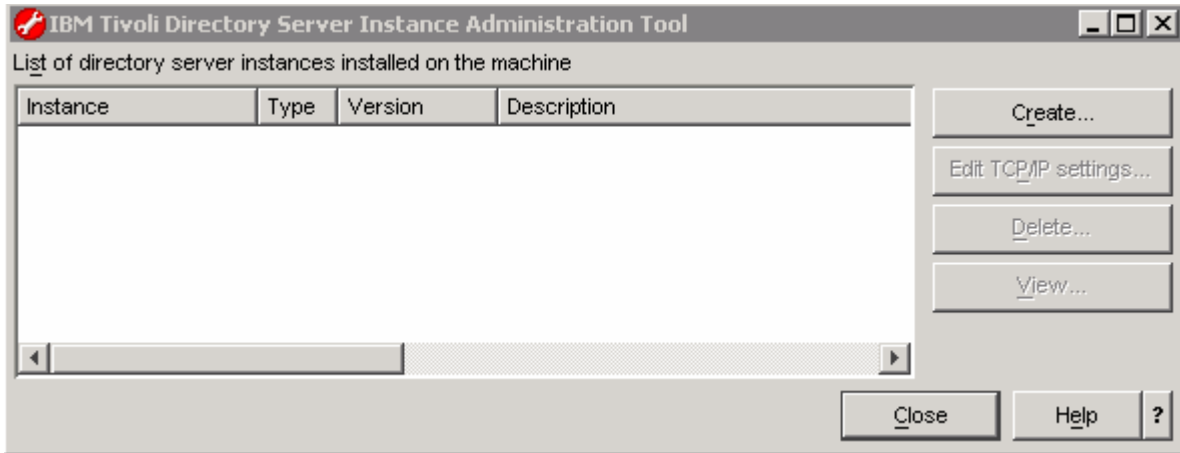
____ 18. Click the **Close** button to quit the IBM Tivoli Directory Server Instance Administration Tool. Click the **Yes** button to confirm

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

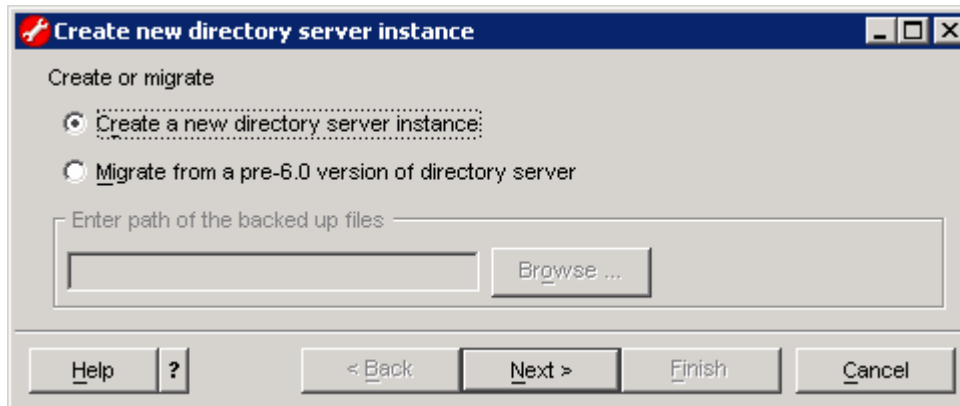
→ Creating a new Tivoli Directory Server Instance

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

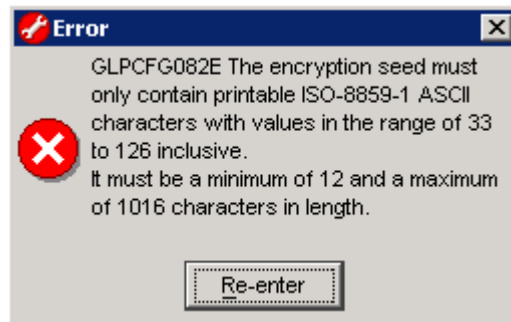
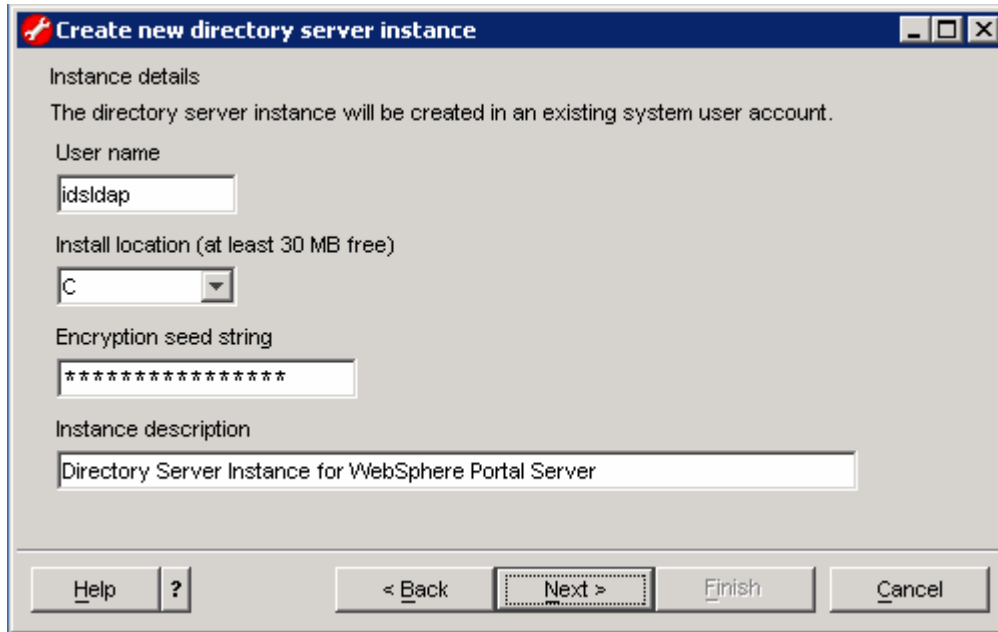
- ___ 1. Launch the IBM Tivoli Directory Server Instance Administration Tool, from Start → Programs → IBM Tivoli Directory Server 6.0 → Instance Administration tool ( Instance Administration Tool)



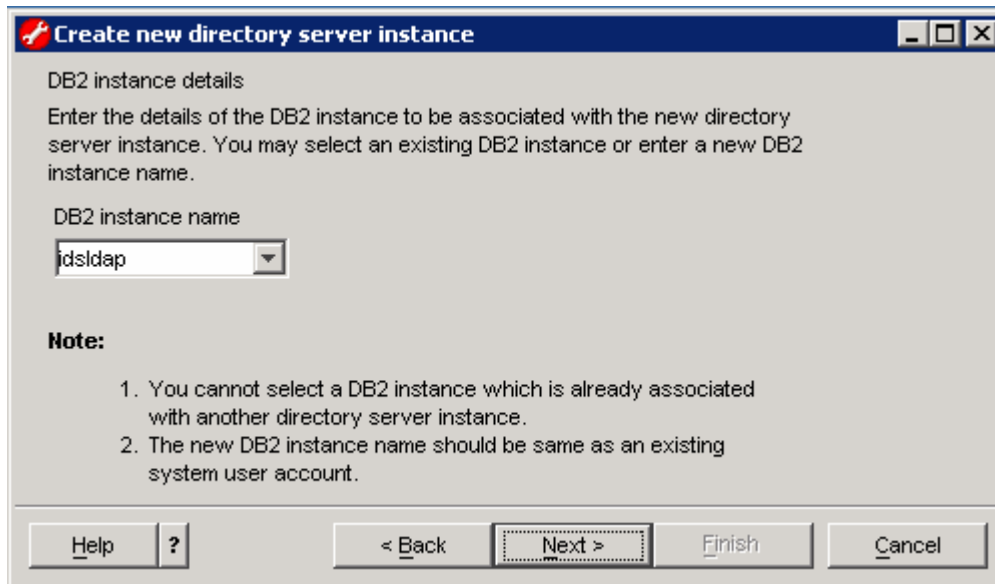
- ___ 2. Click the **Create** button
- ___ 3. The **Create new directory server instance** wizard is launched. Select the radio button next to **Create a new directory server instance**



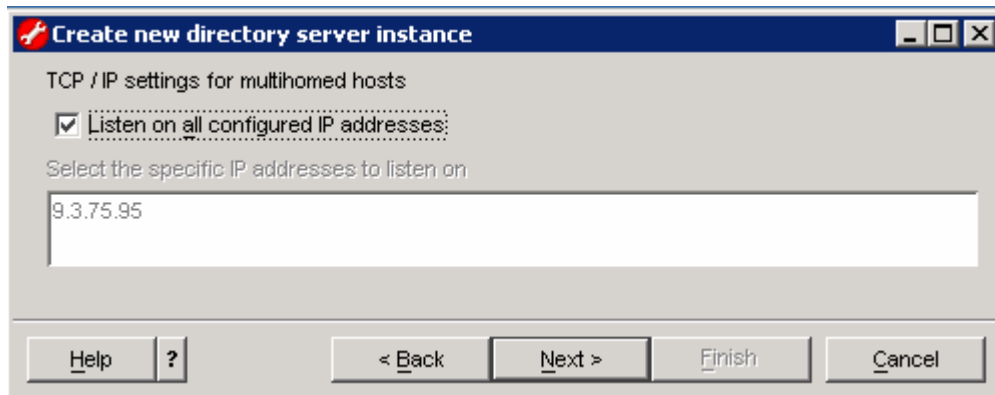
- ___ 4. Click **Next**
- ___ 5. In the following **instance details** panel, enter the following information:
 - ___ a. User name : **idsldap**
 - ___ b. Install location : **C** (default)
 - ___ c. Encryption seed string : **monitorserversecurity** (Note : 13 chars or more)
 - ___ d. Instance Description : **Directory Server Instance for WebSphere Portal Server**



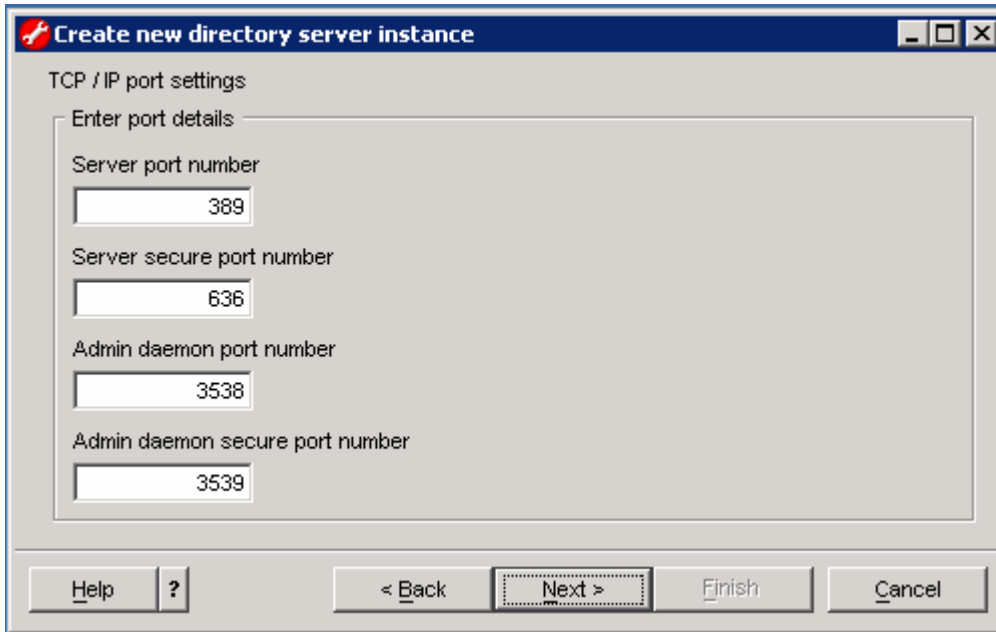
- ___ 6. Click **Next**
- ___ 7. In the following **DB2 instance details** panel, select **idsldap** as the **DB2 instance name** from the drop down list



- ___ 8. Click **Next**
- ___ 9. Accept the defaults in the following **TCP/IP settings for multihomed hosts** panel

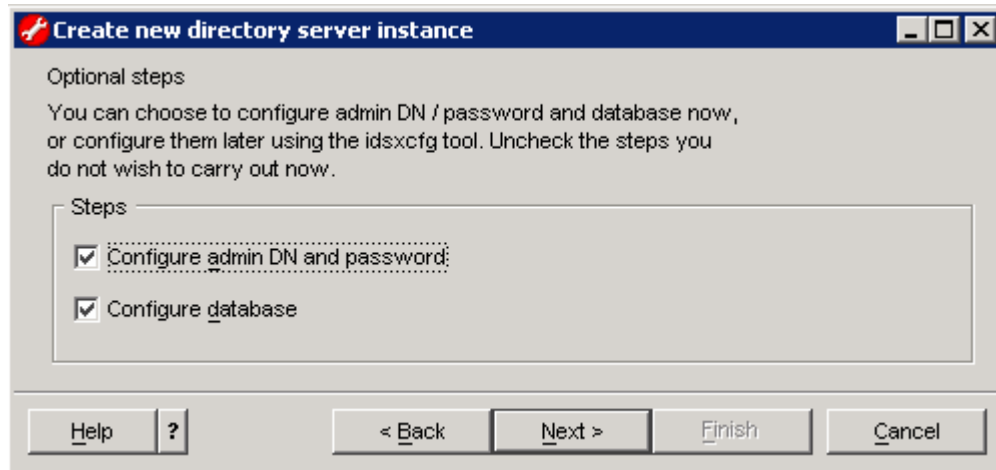


- ___ 10. Click **Next**
- ___ 11. In the following **TCP/IP ports settings** panel, accept the default port numbers



___ 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**

The screenshot shows a dialog box titled "Create new directory server instance" with a red arrow icon. The main heading is "Configure administrator DN and password". There are three text input fields: "Administrator DN" containing "cn=root", "Administrator password" containing "*****", and "Confirm password" containing "*****". At the bottom, there are five buttons: "Help", "?", "< Back", "Next >" (which is highlighted with a dashed border), "Finish", and "Cancel".

___ 16. Click **Next**

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

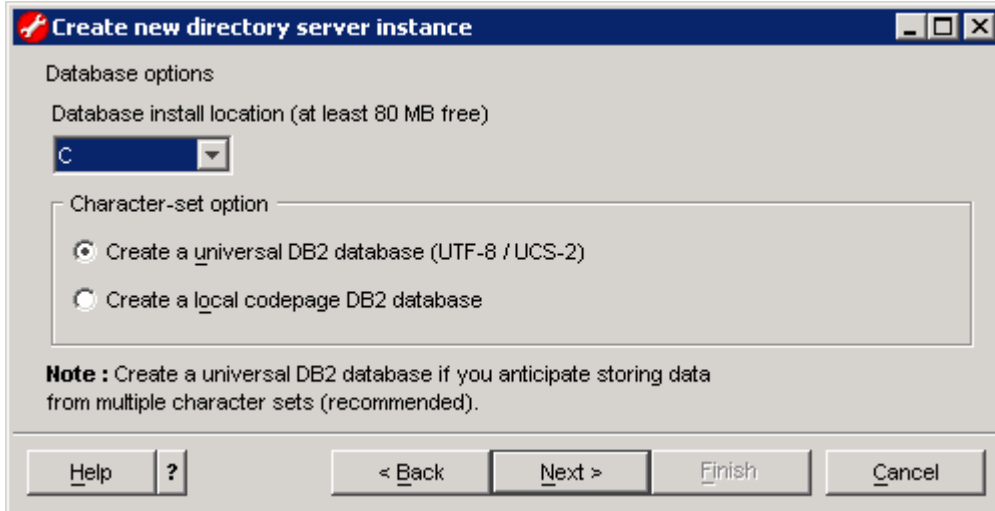
- ___ a. Database user name : **db2admin**
- ___ b. Password : **db2admin**
- ___ c. Database name : **LDAPDB**

The screenshot shows the same dialog box, now at the "Configure database" step. There are three text input fields: "Database user name" containing "db2admin", "Password" containing "*****", and "Database name" containing "LDAPDB". The "Next >" button is still highlighted with a dashed border.

___ 18. Click **Next**

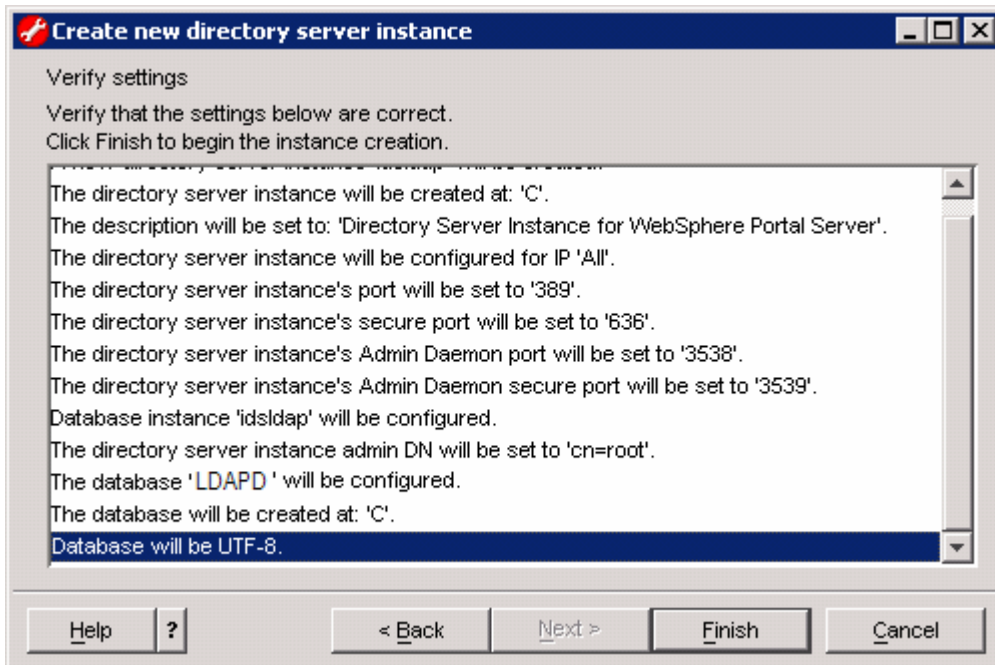
___ 19. In the following **Database options** panel, complete the following instructions:

- ___ 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



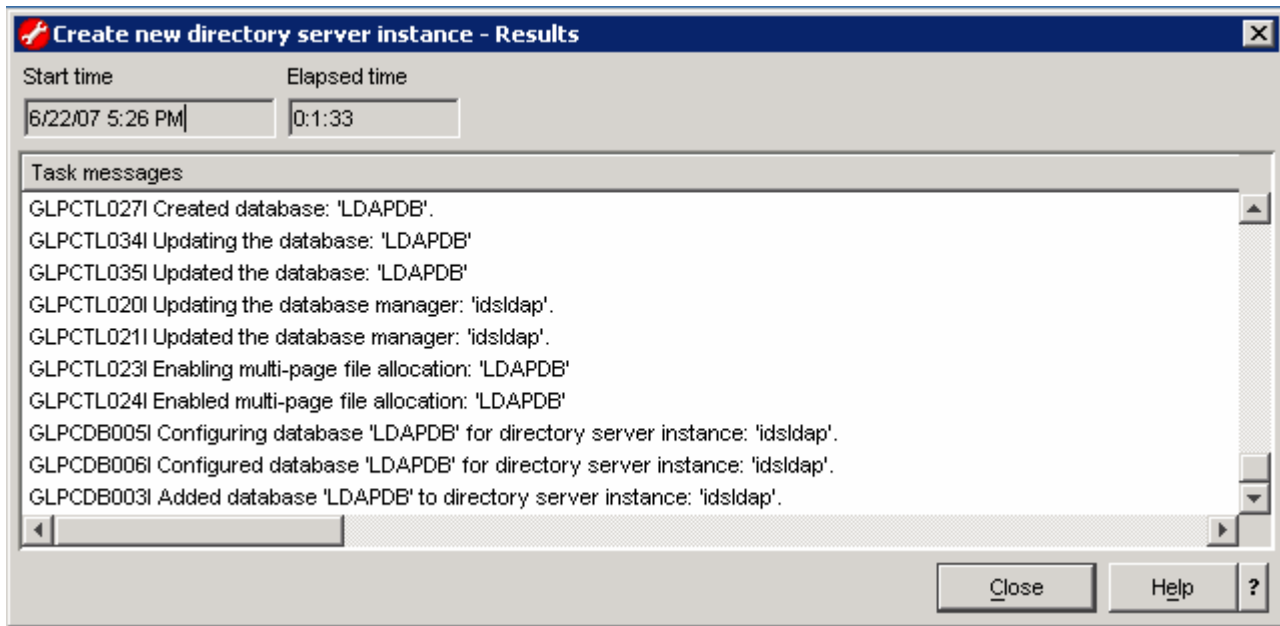
___ 20. Click **Next**

___ 21. Verify the settings in the following panel

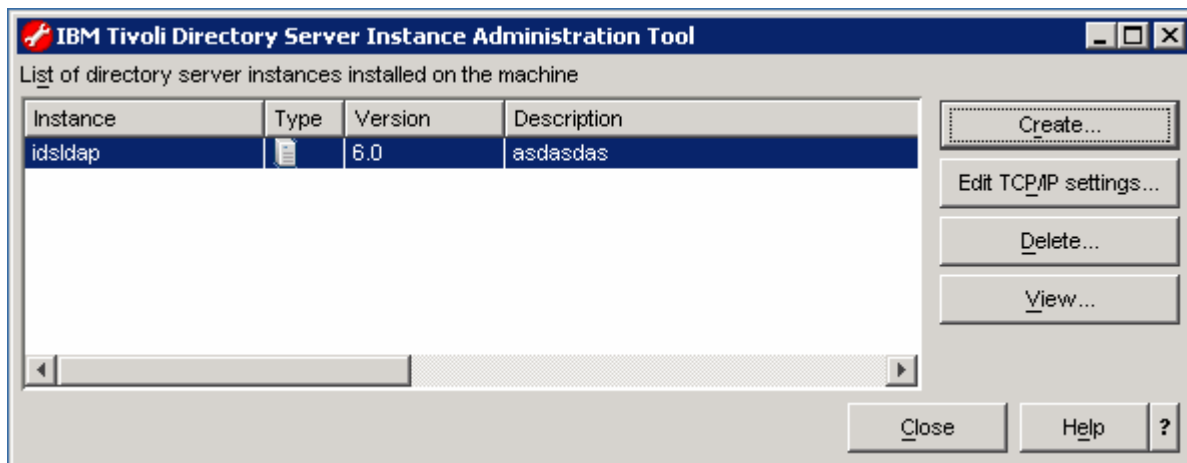


___ 22. Click the **Finish** button

___ 23. Ensure the Directory Server Instance is successfully created



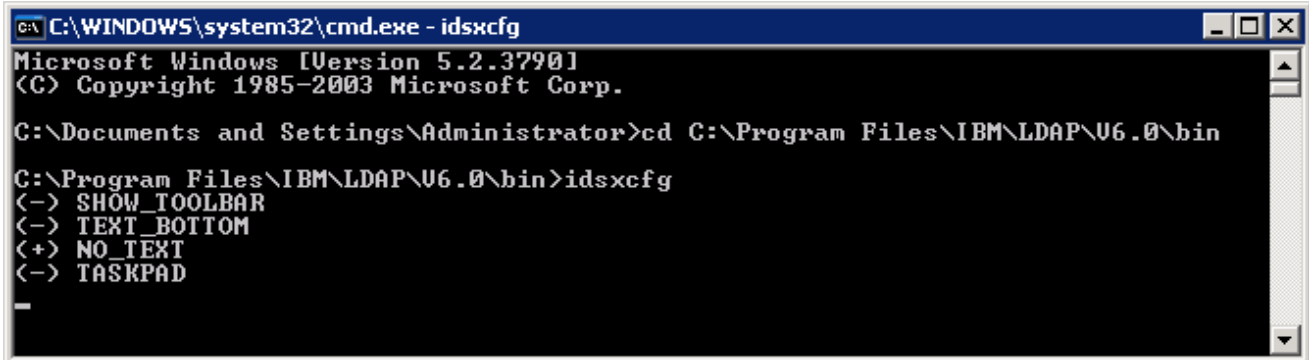
24. Click the **Close** button



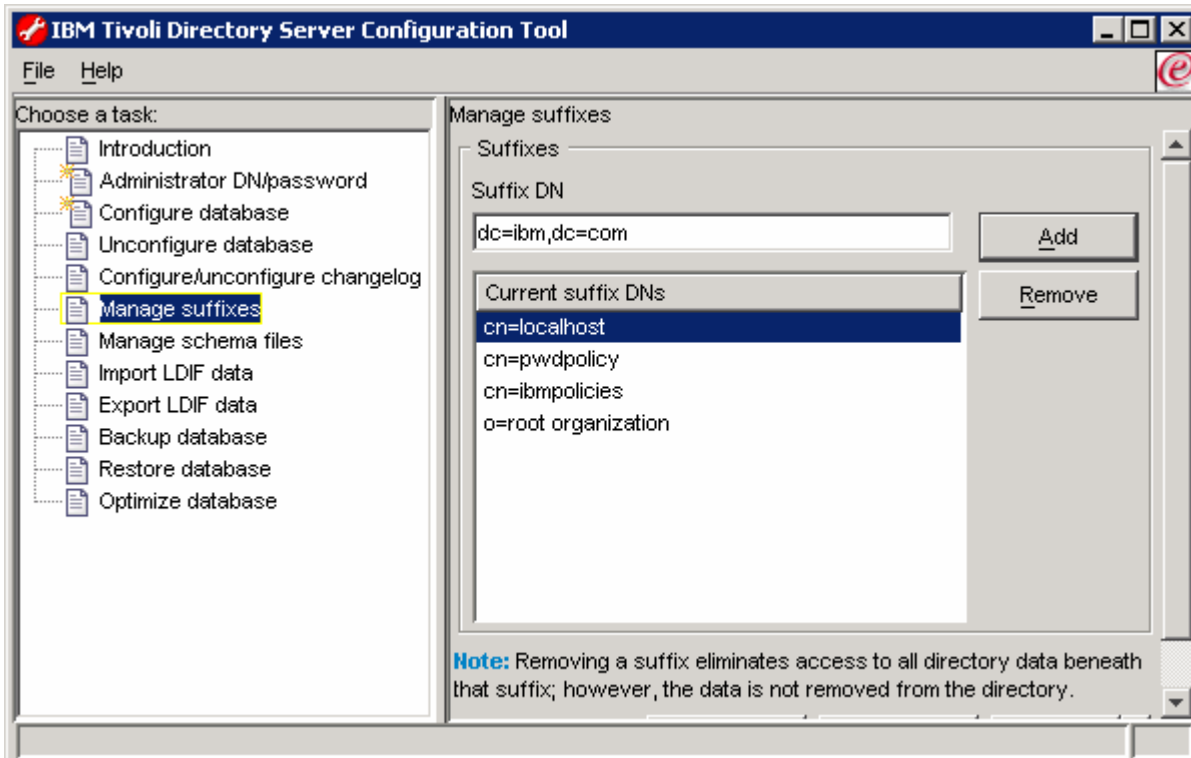
25. Close the IBM Tivoli Directory Server instance Administration Tool

→ Configuring IBM Tivoli Directory Server

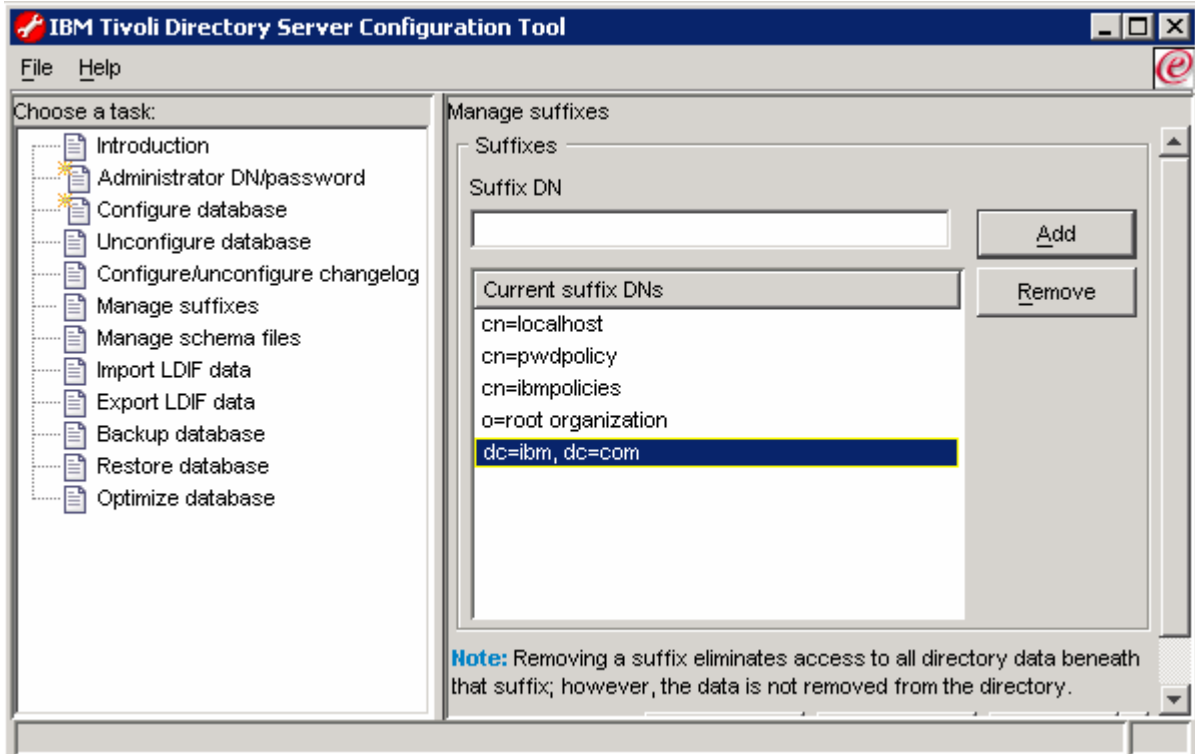
- ___ 1. To configure the directory server with Portal users, you will import the LDIF file.
 - ___ a. Open a command line window and change the directory to **C:\Program Files\IBM\LDAP\6.0\bin**
 - ___ b. Run the **idsxcfg** command to open the IBM Tivoli Directory Server Configuration Tool



- ___ 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**



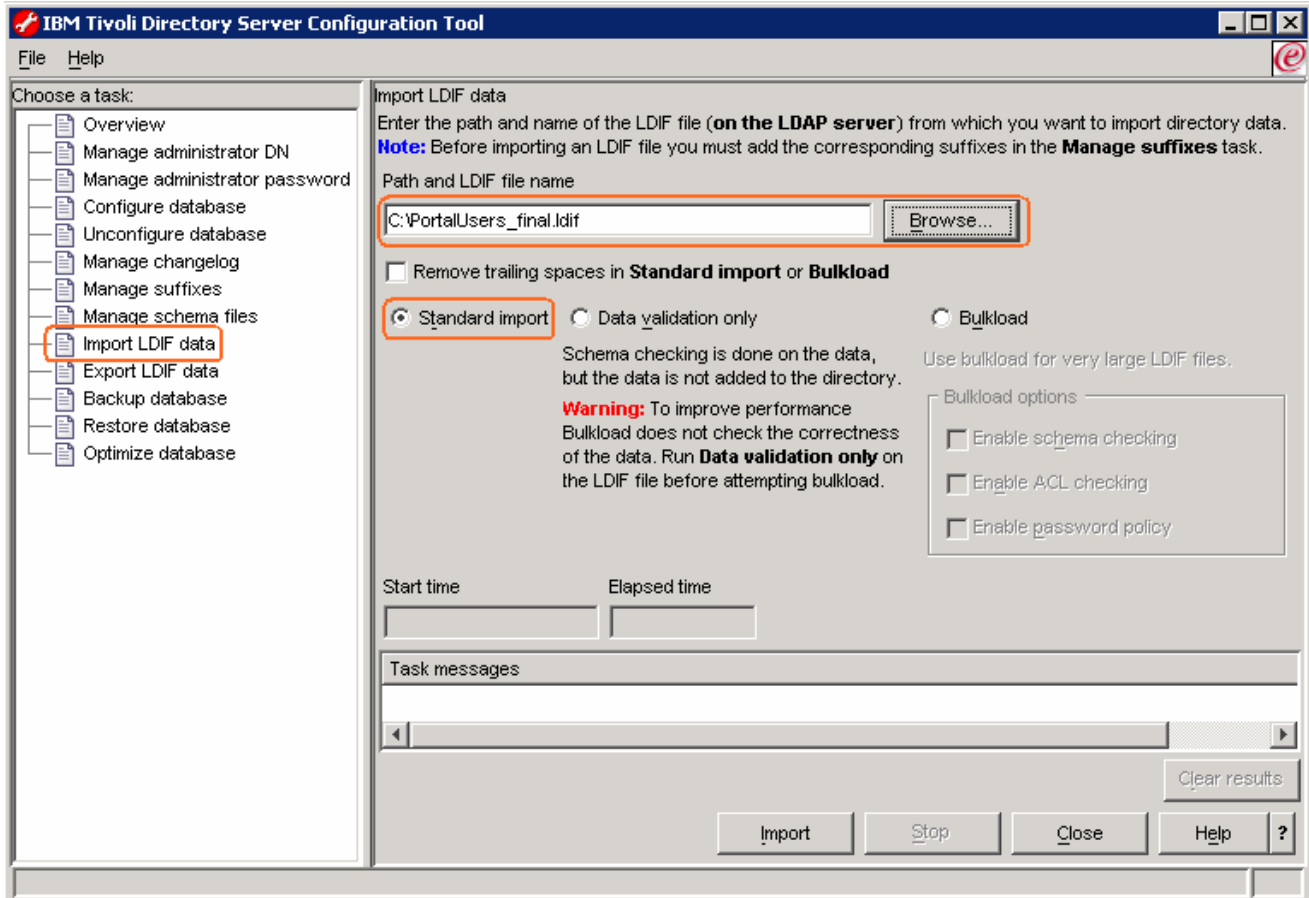
___ e. Click the **OK** button

___ 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

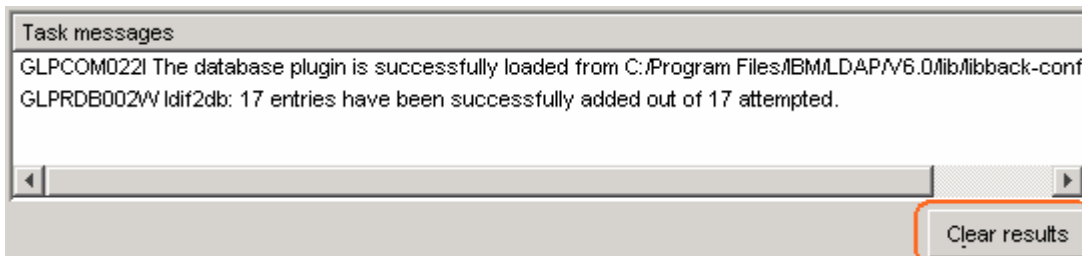
___ b. In the **Import LDIF data** window on the right, click the **Browse** button to locate the LDIF file that consists of the portal users

___ 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

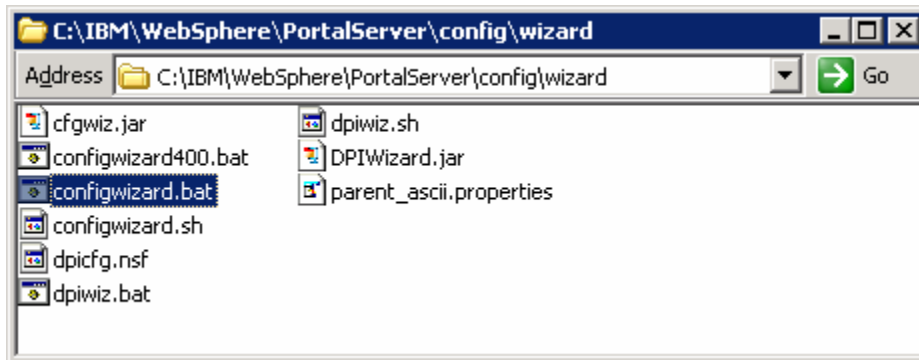
If WebSphere Application Server global security is enabled, you must disable it before modifying your security configuration. By default the WebSphere Application Server Global Security and Portal Server security is enabled internally during the installation for security reasons. So before trying to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

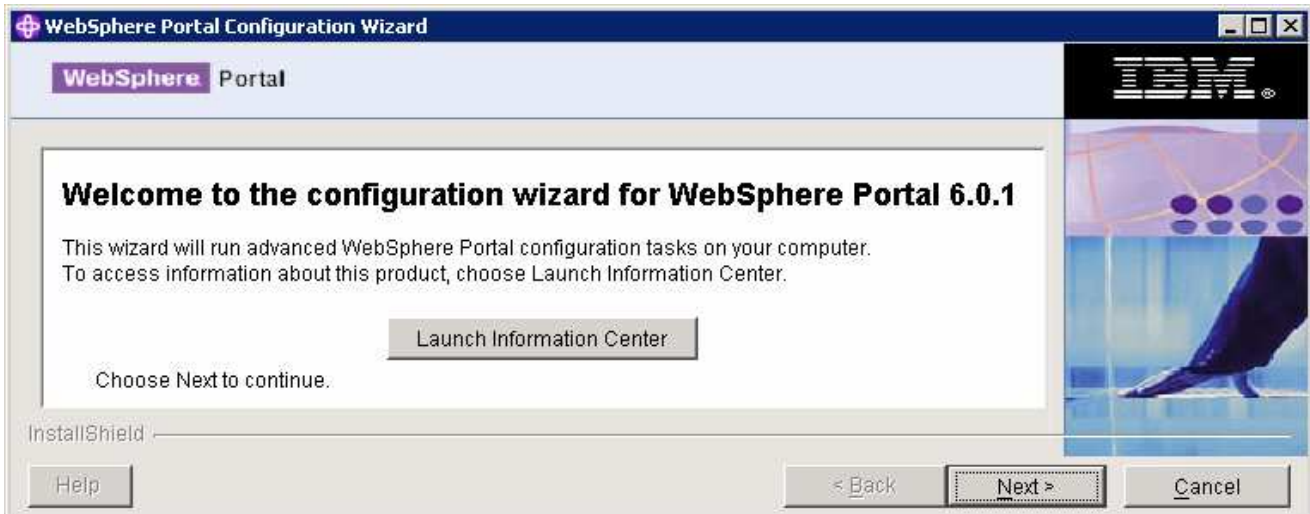
- ___ 1. Start the WebSphere Application Server (**server1**) and the WebSphere Portal Server (**WebSphere_Portal**)
 - ___ a. On the Portal Server machine, locate the **config/wizard** directory (**C:\IBM\WebSphere\PortalServer\config\wizard**)



- ___ b. Double click the **configwizard.bat** to launch the Portal Server Configuration Wizard
- ___ c. Select **English** as language

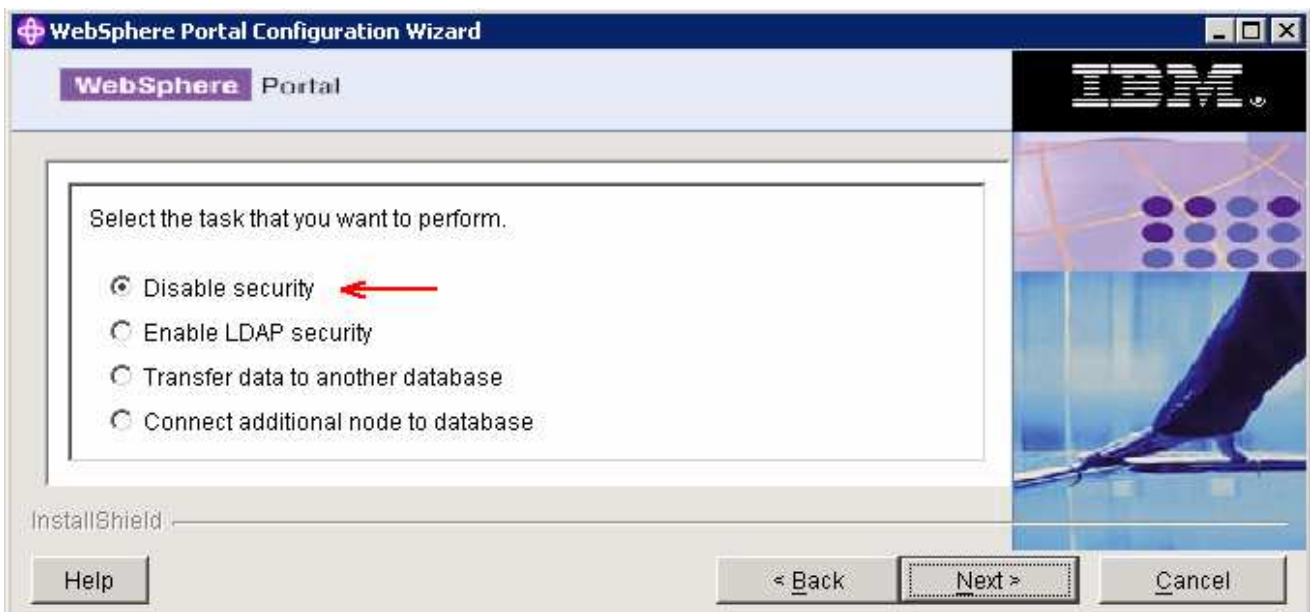


- ___ d. Click **OK**. The Configuration Wizard is launched



__ 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

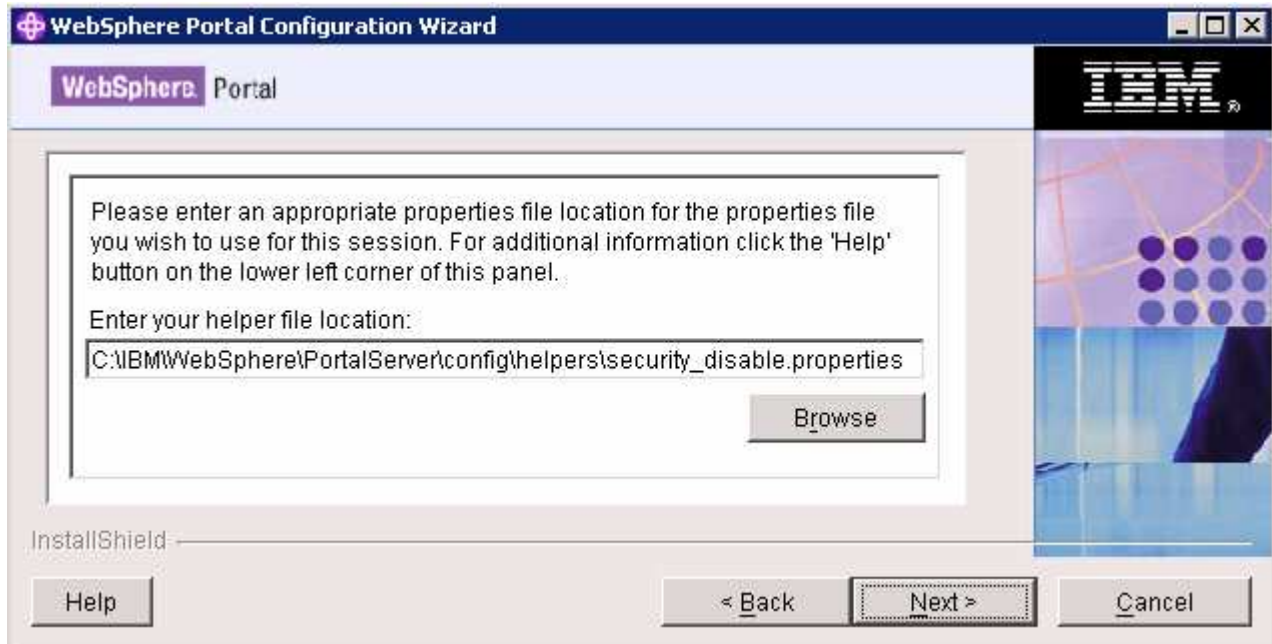
- **User ID** : was602admin
- **Password** : was602admin



__ 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**

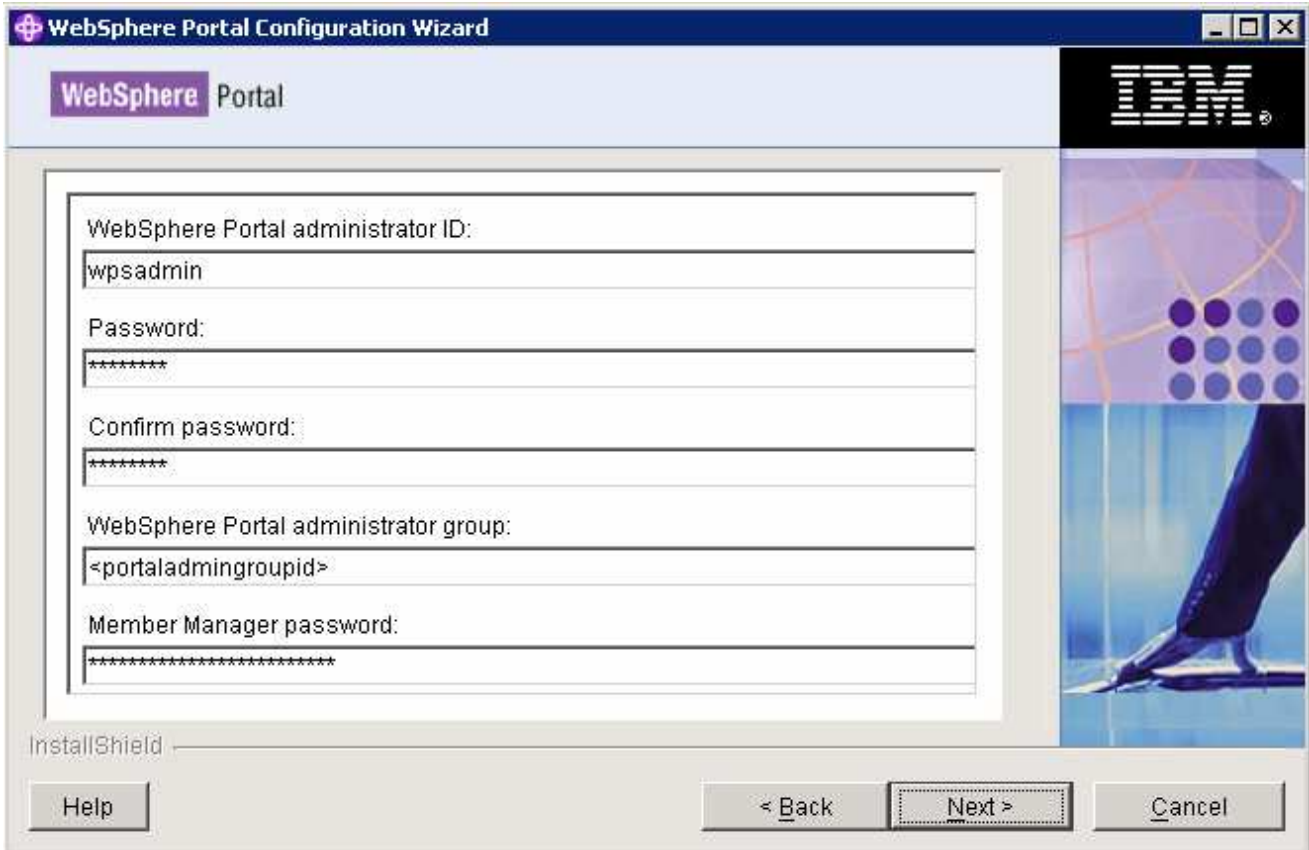


__ k. Click **Next**

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

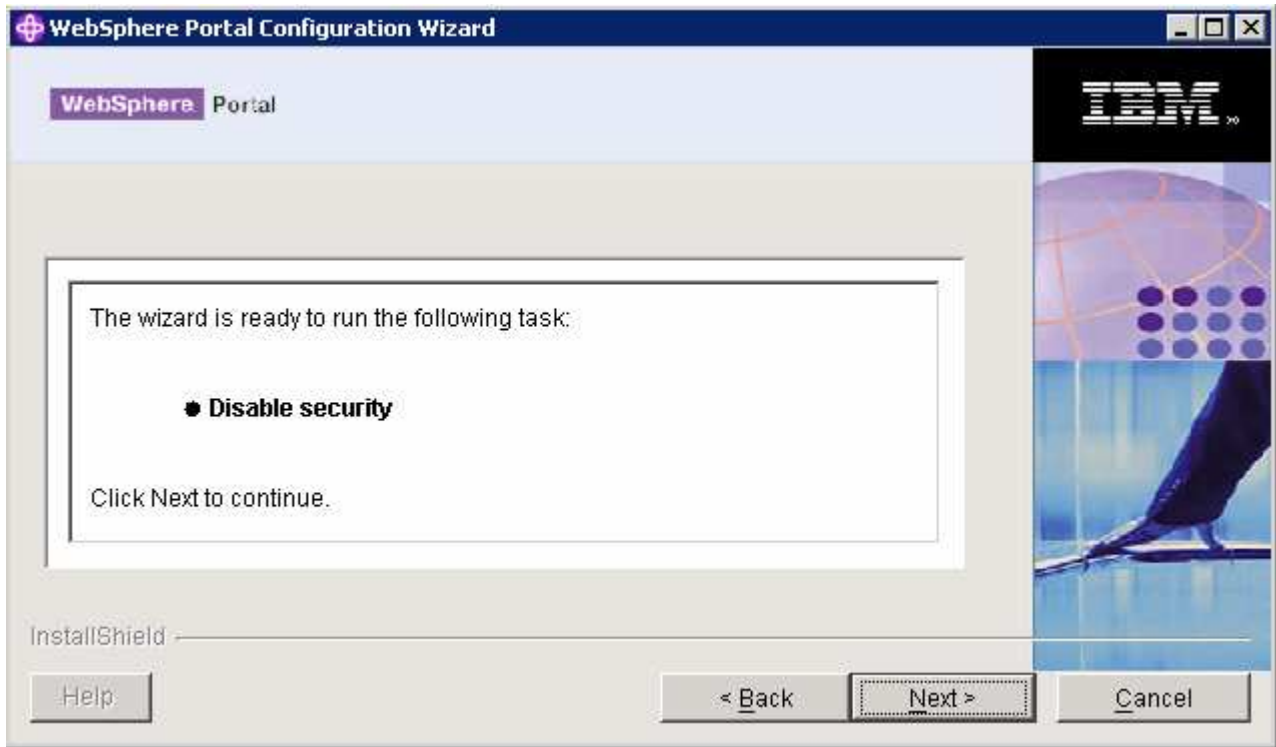
- WebSphere Portal Administrator ID : **wpsadmin**

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



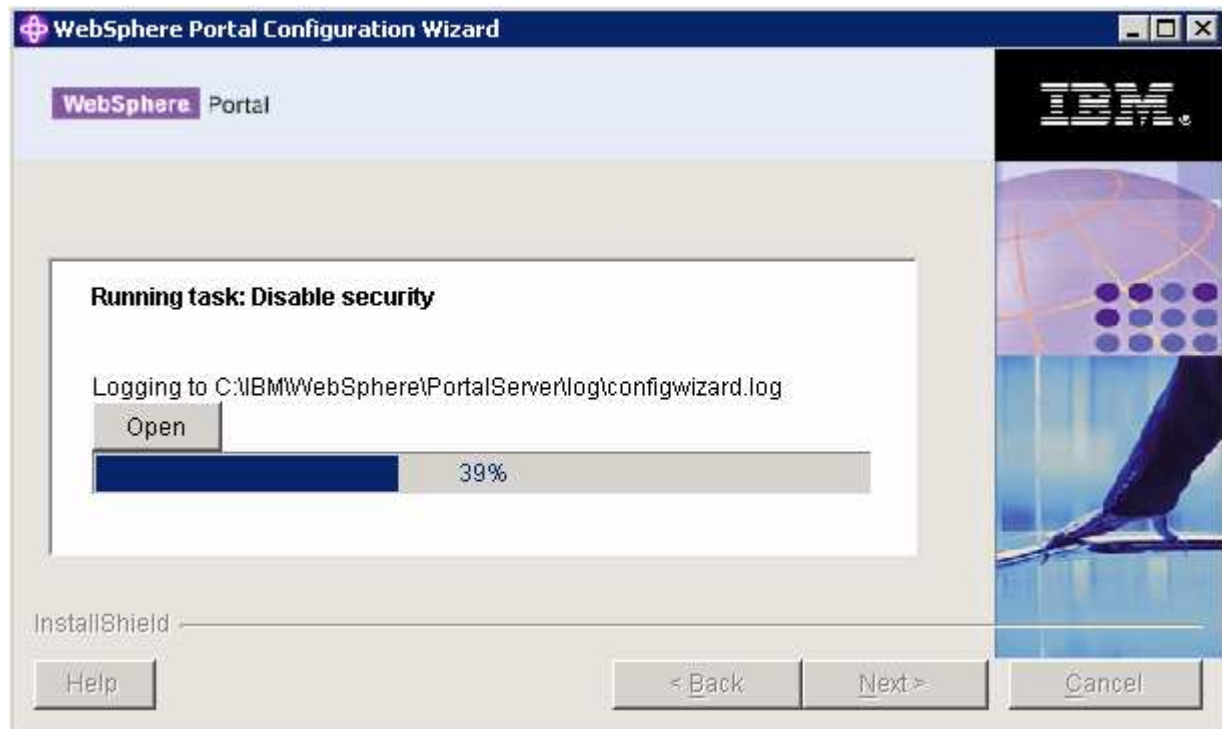
__ m. Click **Next**

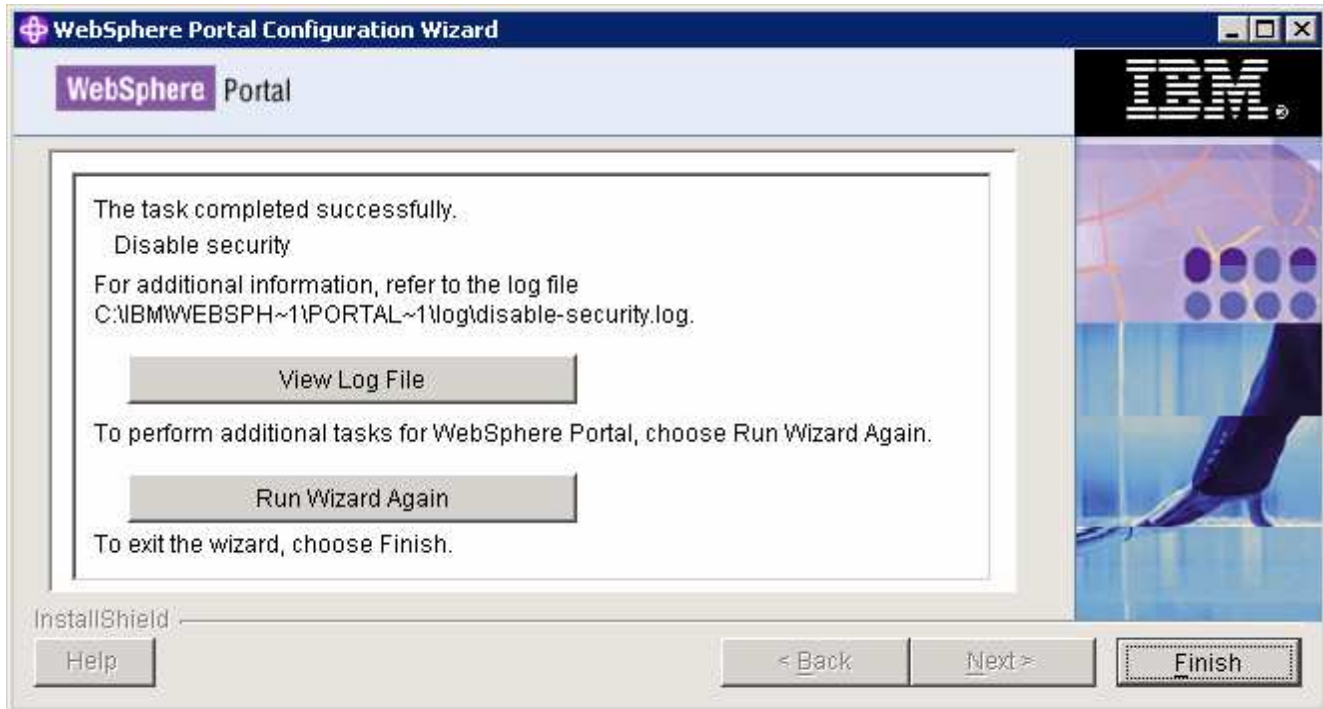
__ n. Review the Summary



___ 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**

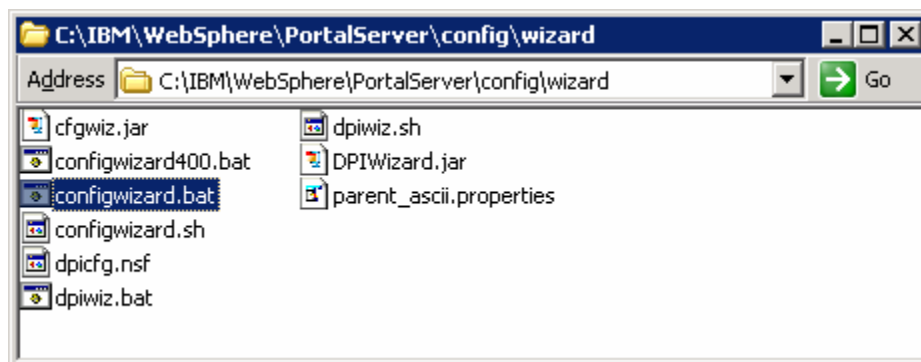




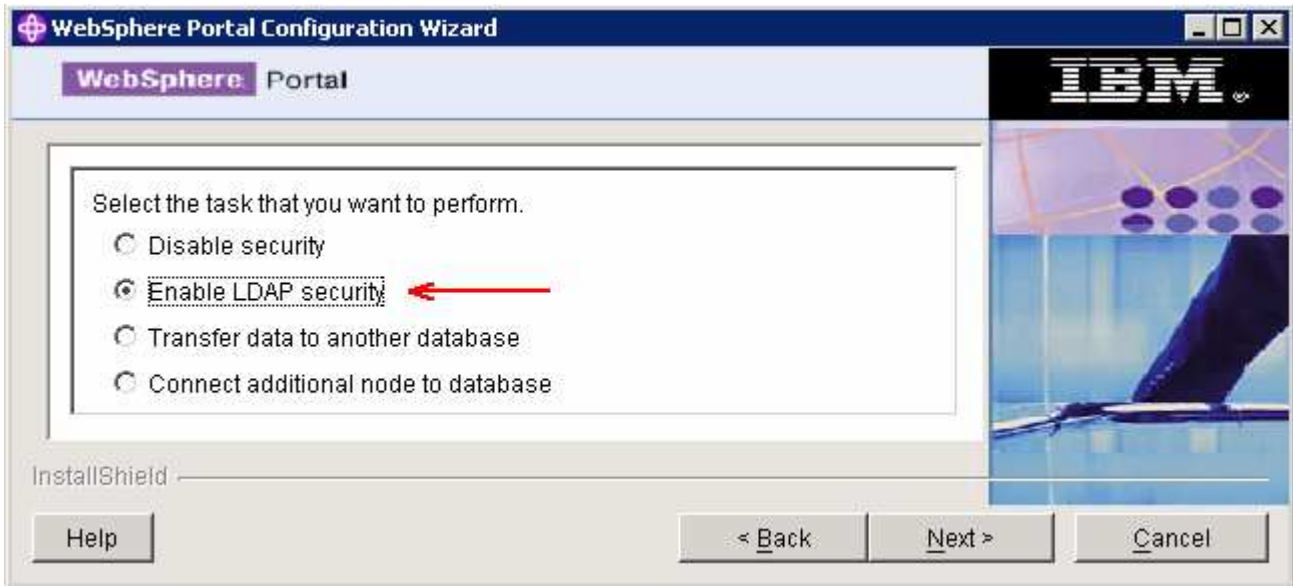
- ___ 2. Click **Finish**
- ___ 3. You have now disabled the WebSphere Application Server security and Portal Server security

→ 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**

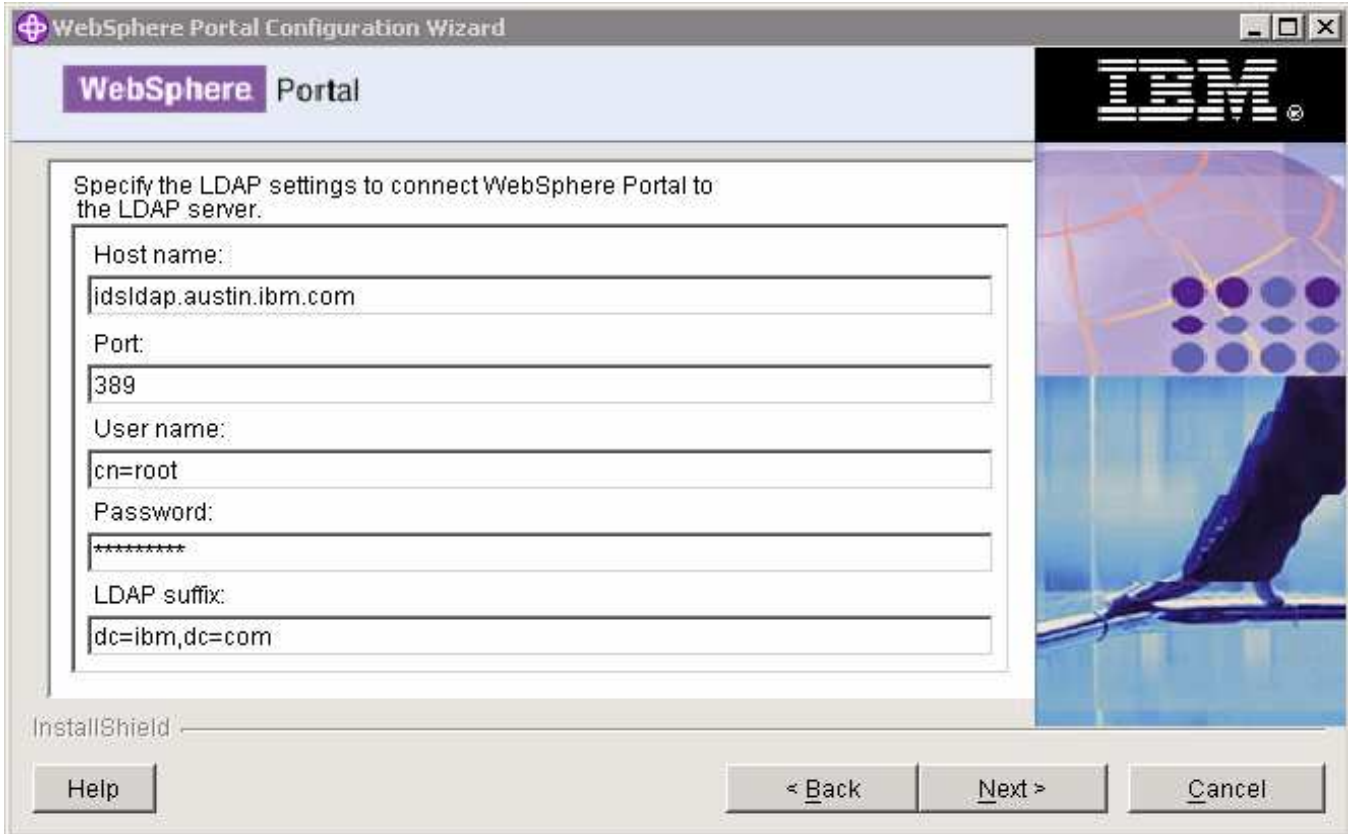
___ 13. In the following panel, specify the LDAP settings to connect WebSphere Portal to LDAP server:

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

Example: idsldap.austin.ibm.com

___ b. Port : **389**

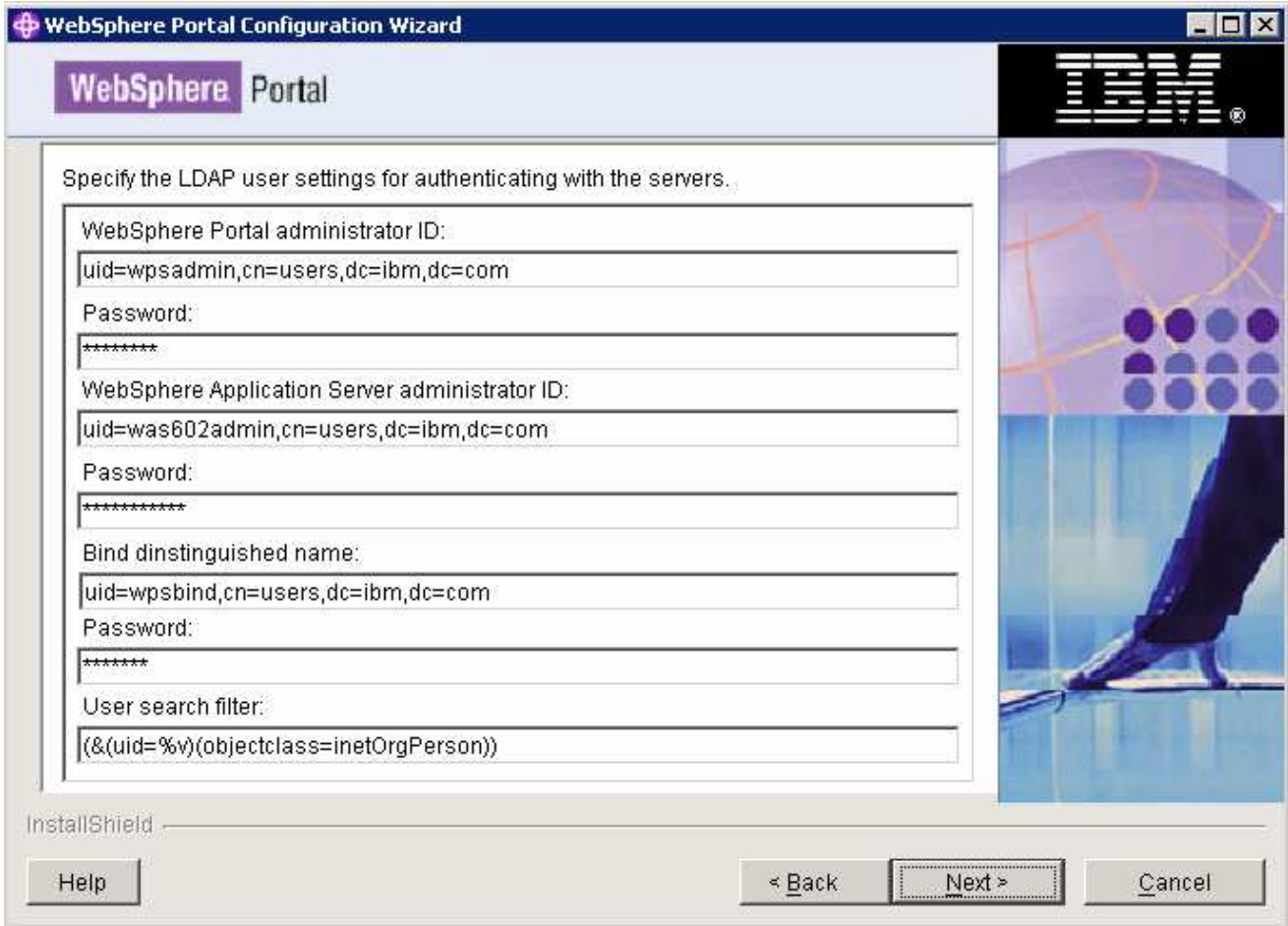
- __ c. User name : **cn=root**
- __ d. Password : **ldapadmin**
- __ e. LDAP suffix : **dc=ibm,dc=com**



___ 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 >**

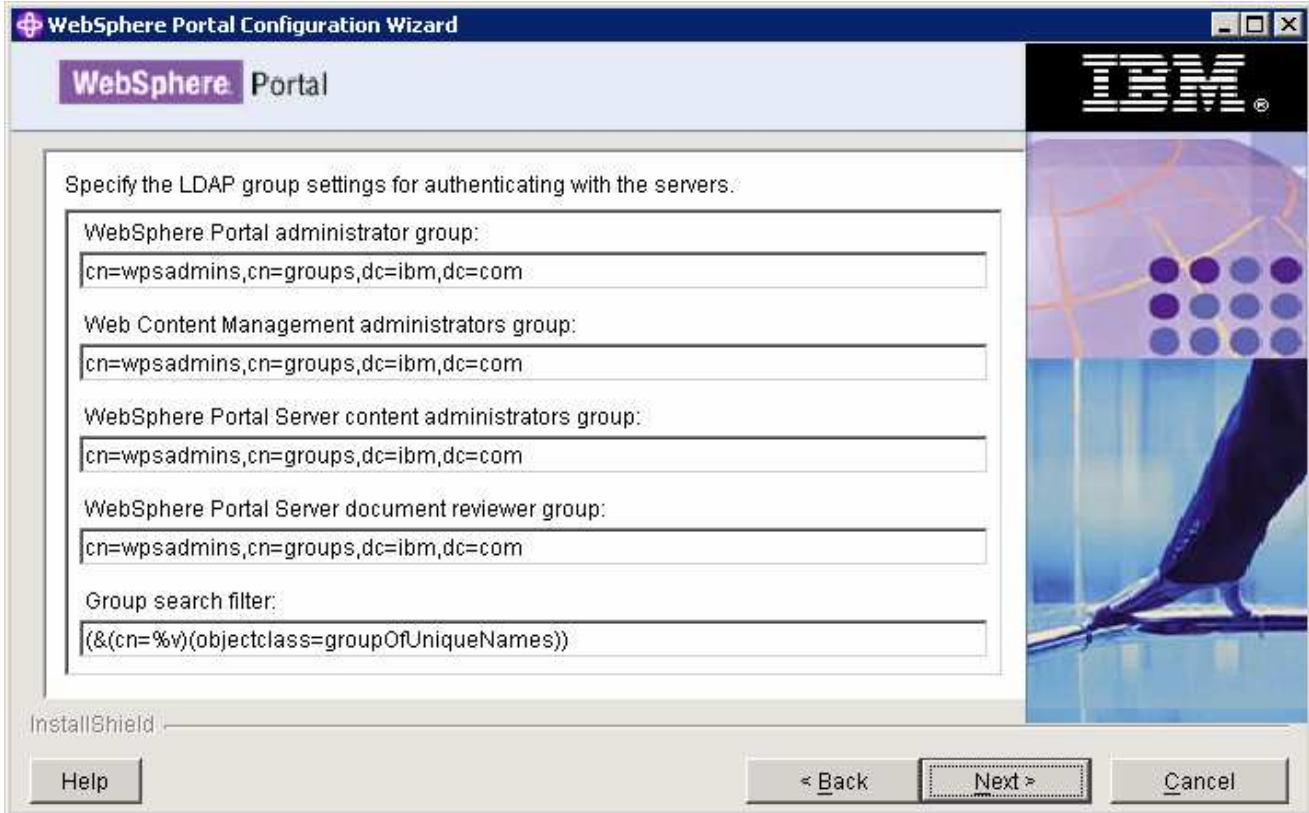


___ 16. Click **Next**

___ 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:

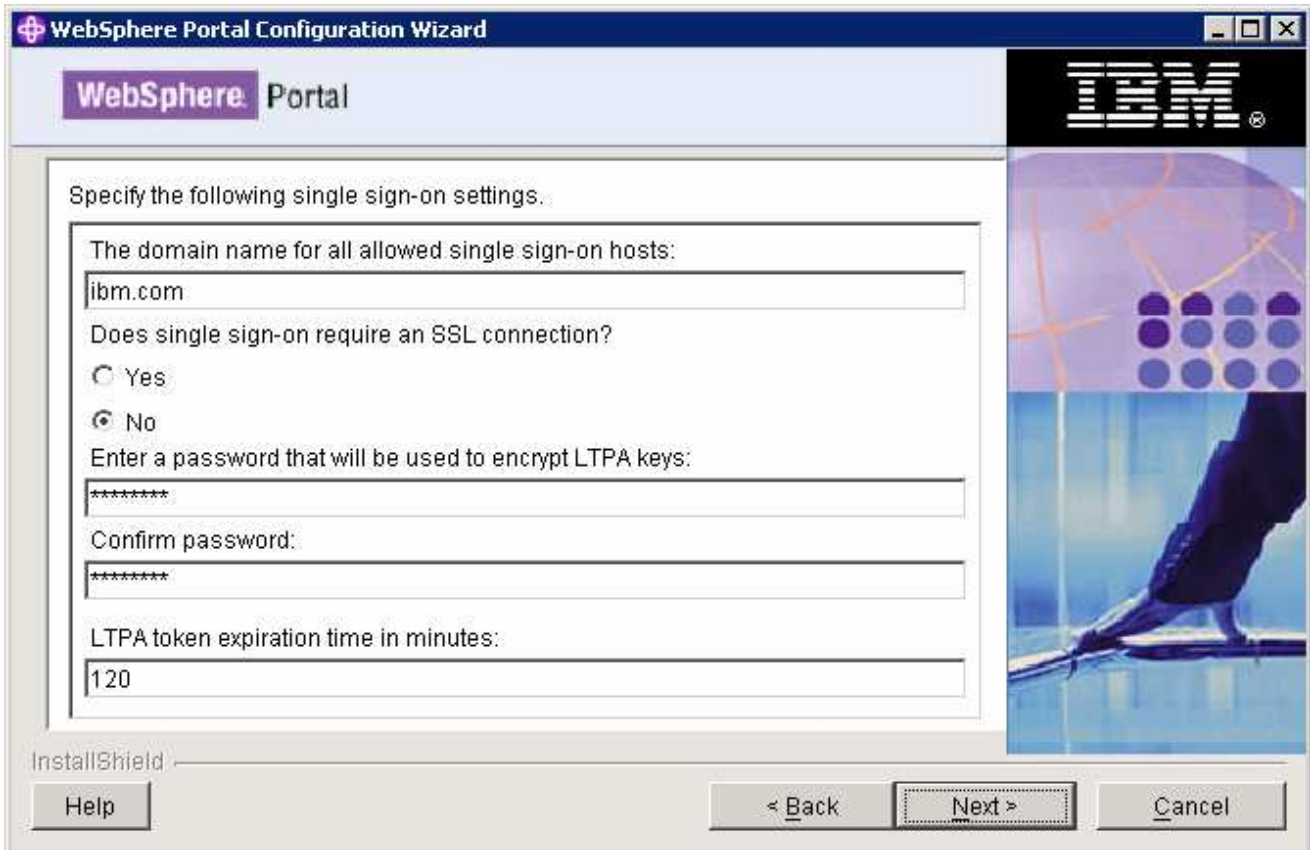
- ___ a. User prefix : **uid**
- ___ b. User suffix : **cn=users**
- ___ c. Group prefix : **cn**
- ___ d. Group suffix : **cn=groups**



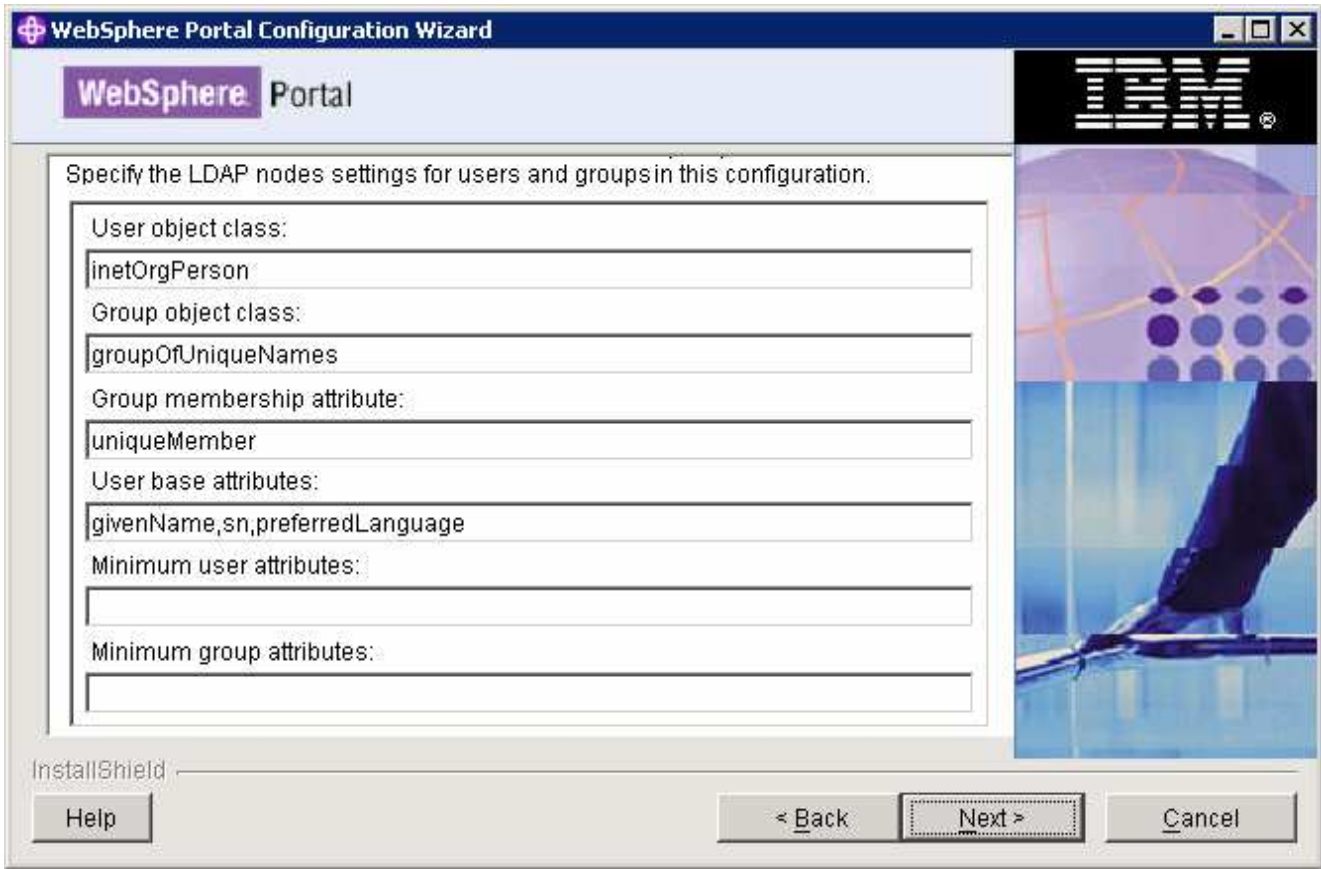
___ 22. Click **Next**

___ 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**

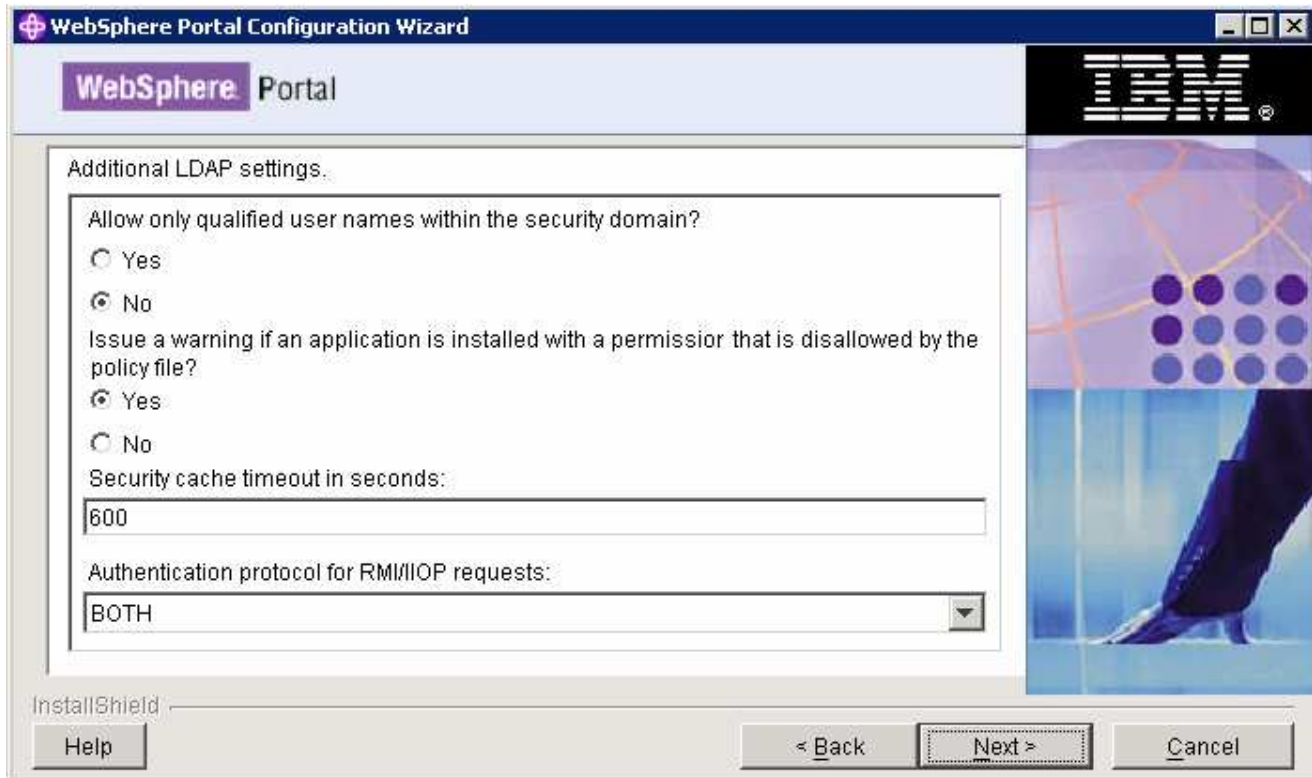


- ___ 24. Click **Next**
- ___ 25. In the following panel, accept the default parameters or specify the parameters as per your environment:



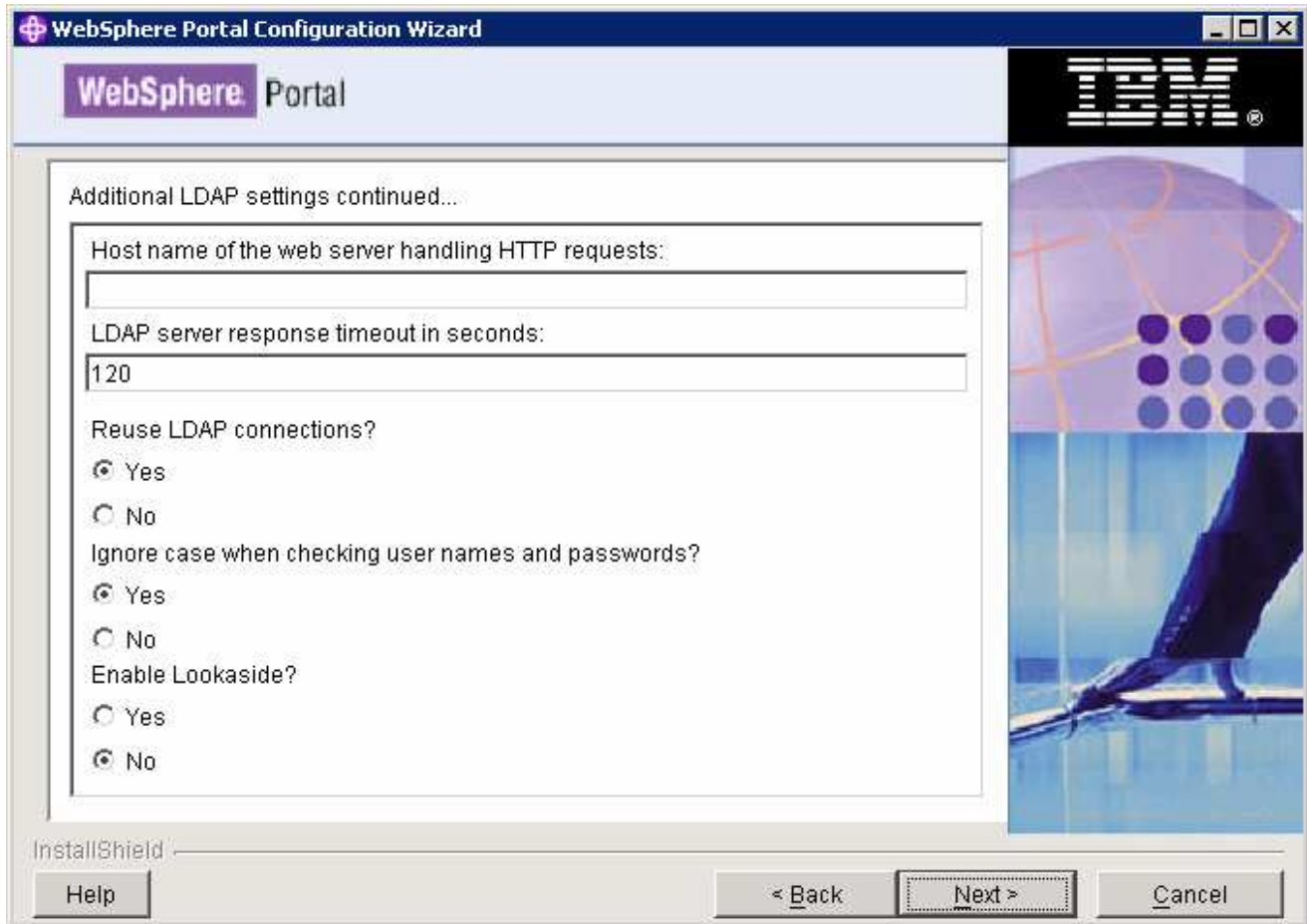
___ 26. Click **Next**

___ 27. In the following 'Additional LDAP settings' panel, accept the defaults:



___ 28. Click **Next**

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



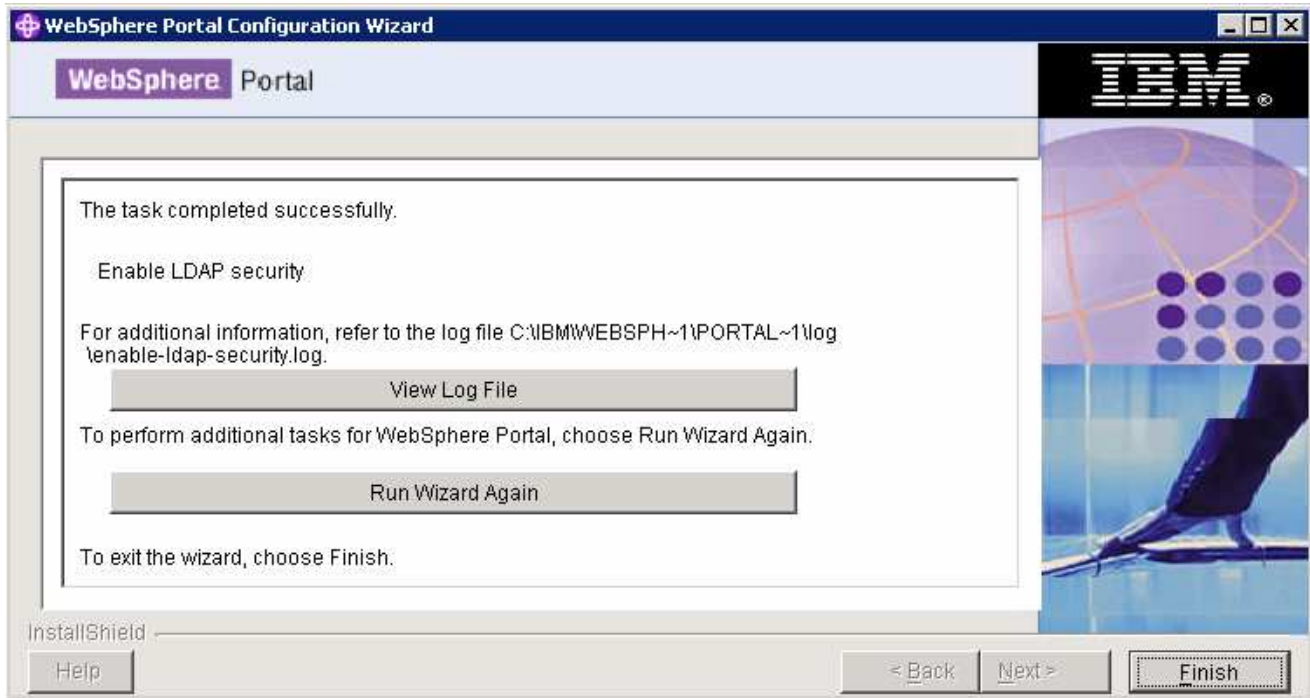
___ 30. Click **Next**

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

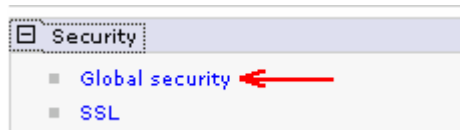


___ 32. Click **Next**

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



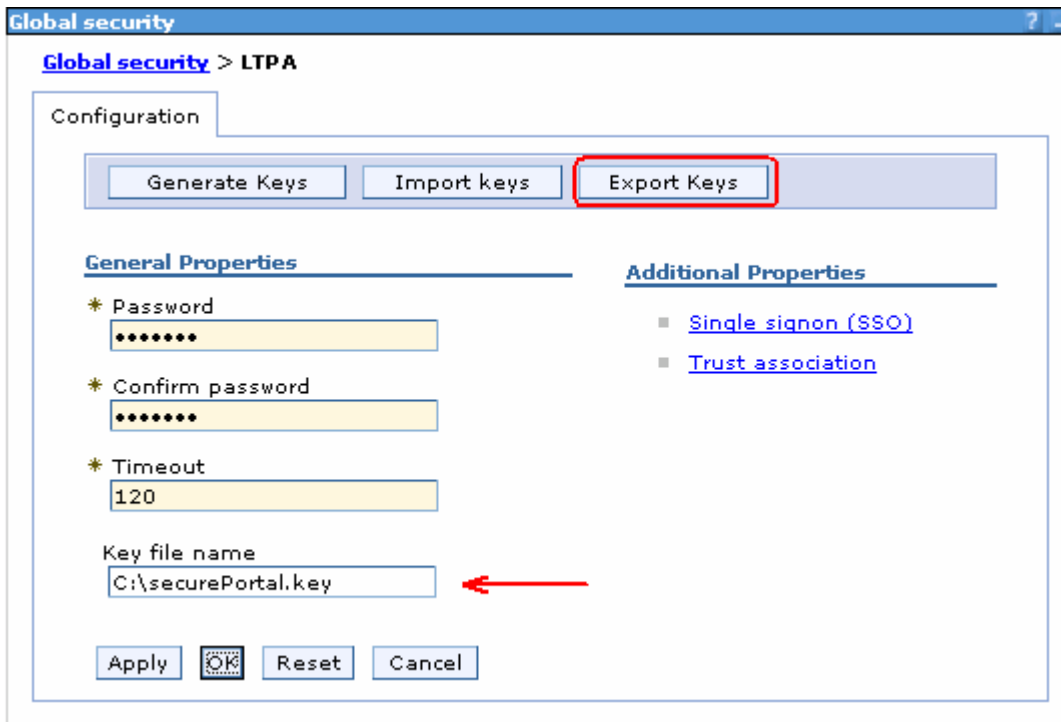
- ___ 34. Once the Security configuration is complete, click **Finish**
- ___ 35. Restart the Portal Server and review the System Out log file and ensure the server is started successfully
- ___ 36. The Enable Security Task for Portal sever with Tivoli Directory Server is complete
- ___ 37. Export LTPA 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

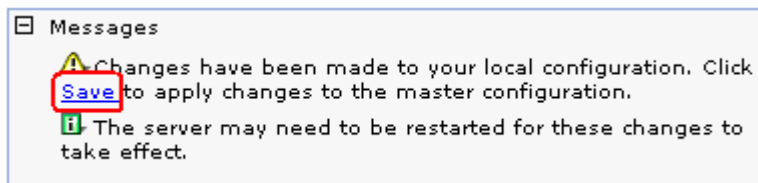


__ e. In the following 'LTPA' panel, enter the 'Key file name' (Example: C:\securePortal.key)



__ 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)

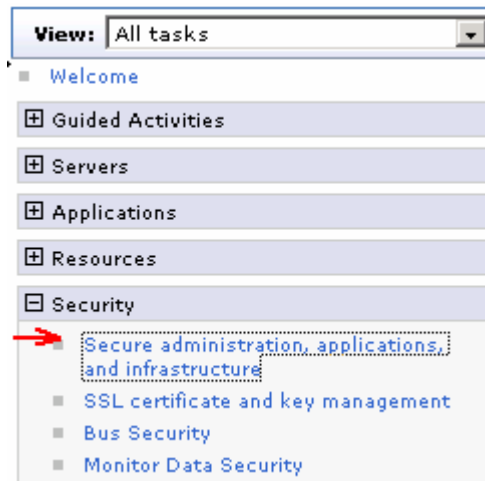
In this part of the lab, you will enable the LDAP security for Monitor Server which includes Web-based Dashboard and REST Server. In this process, you will configure WebSphere Application Server V6.1 to use LDAP in a federated repository.

Prerequisite:-

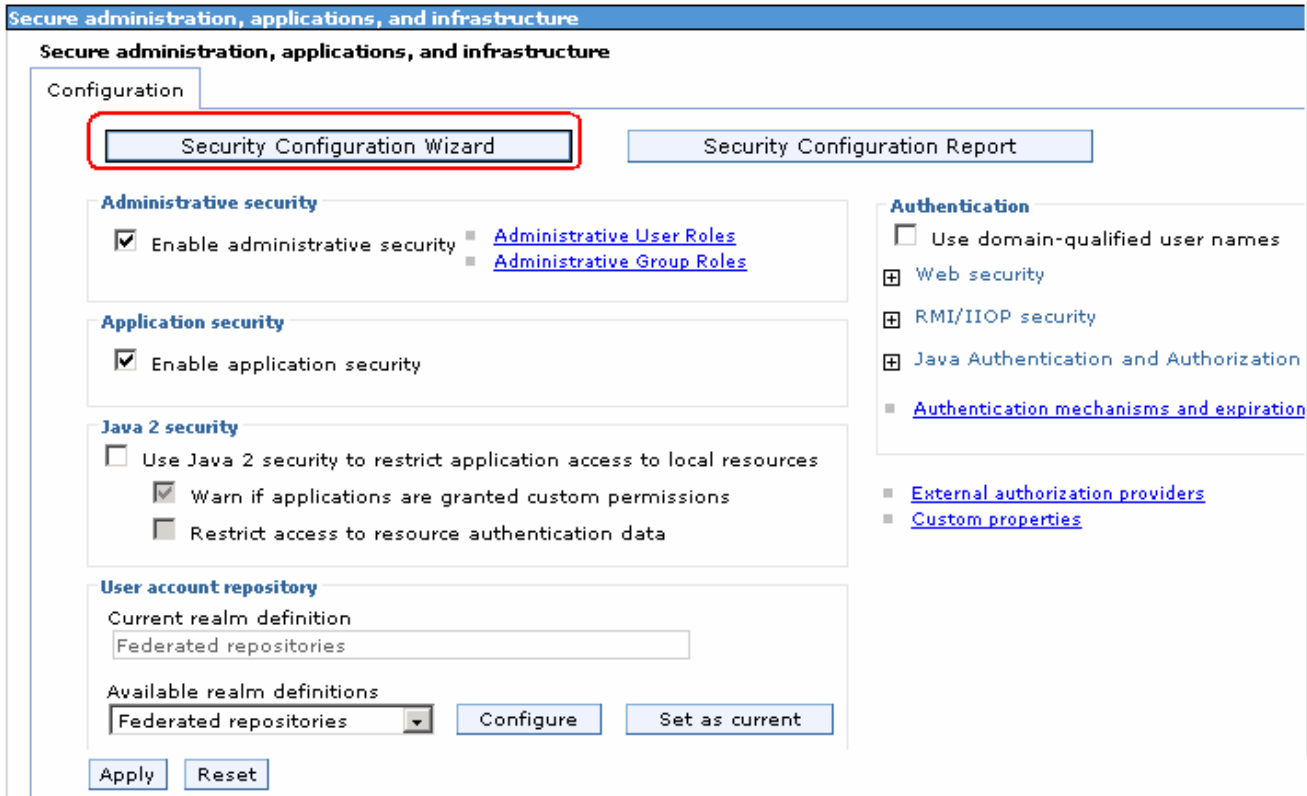
Copy the **securePortal.key** file that you have exported to a temporary location on to the Monitor Server machine

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

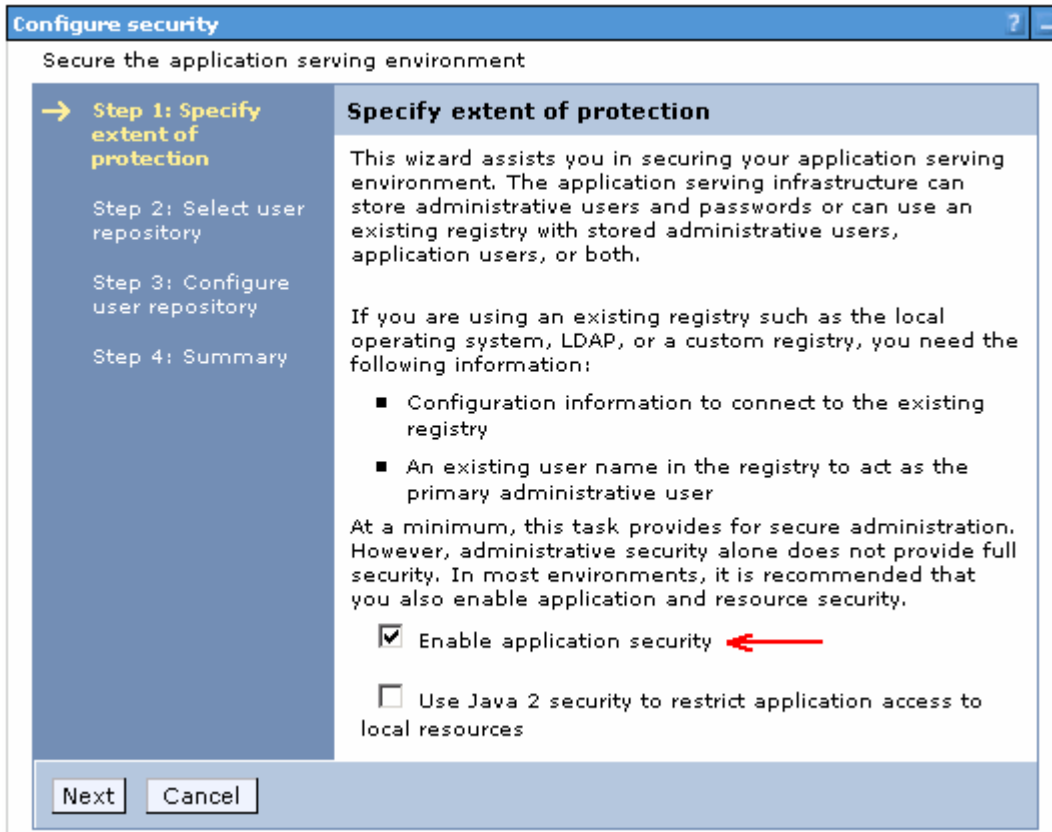
- ___ 1. Start the monitor server profile and launch the administrative console
- ___ 2. Login to the administrative console using the user name and password if the default security is enabled
- ___ 3. In the administrative console's left navigation pane, expand '**Security**' and click the '**Secure administration, applications and infrastructure**' link



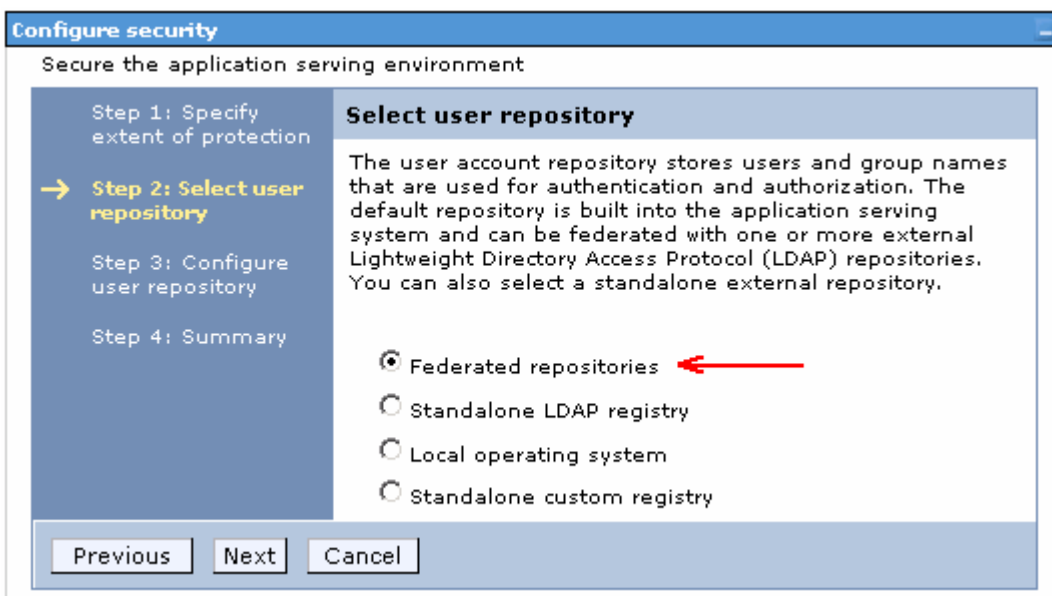
- ___ 4. In the following '**Secure administration, applications and infrastructure**' panel to the left, click the '**Security Configuration Wizard**' button



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

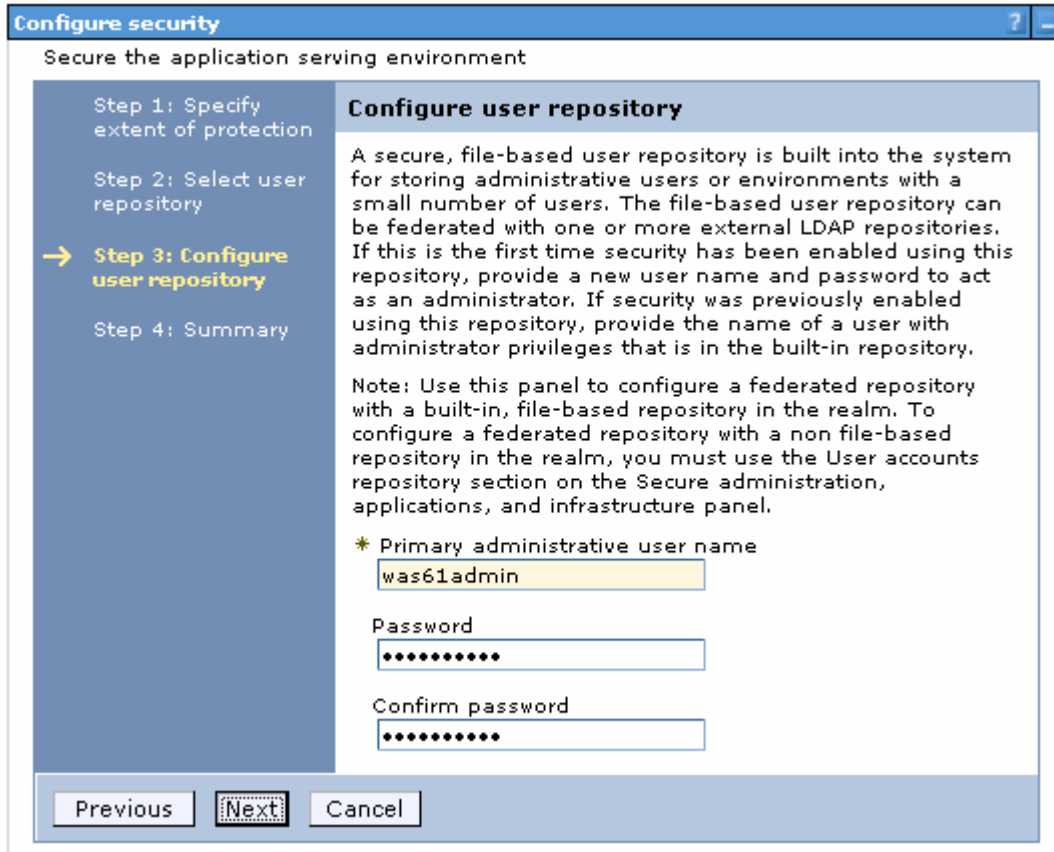


- ___ 6. Click **Next**
- ___ 7. In the following '**Step2: Select user repository**' panel, ensure the radio button for '**Federated repositories**' is selected

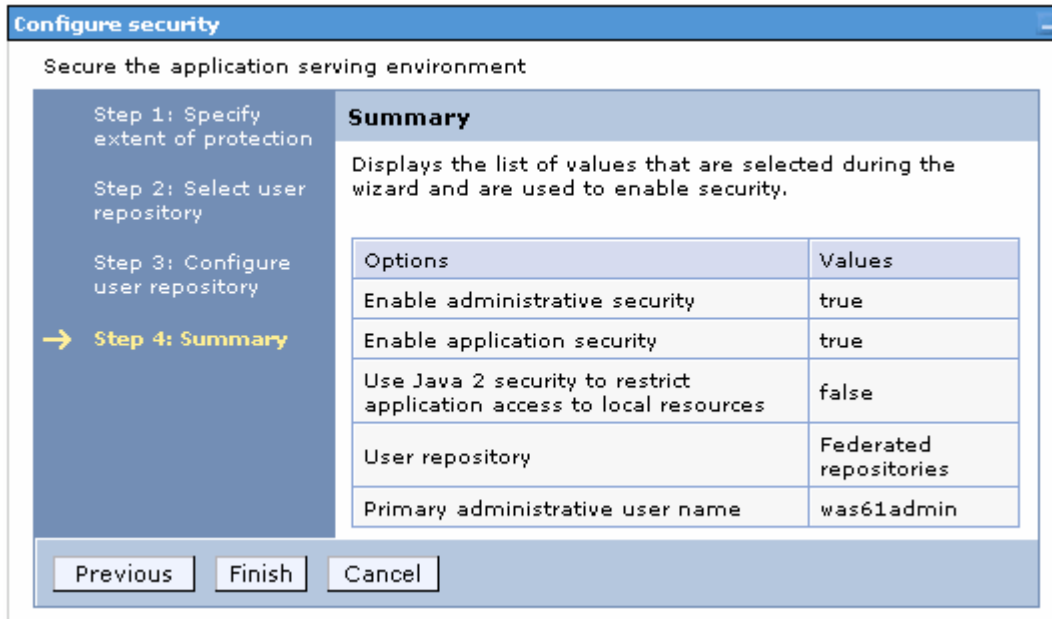


- ___ 8. Click **Next**

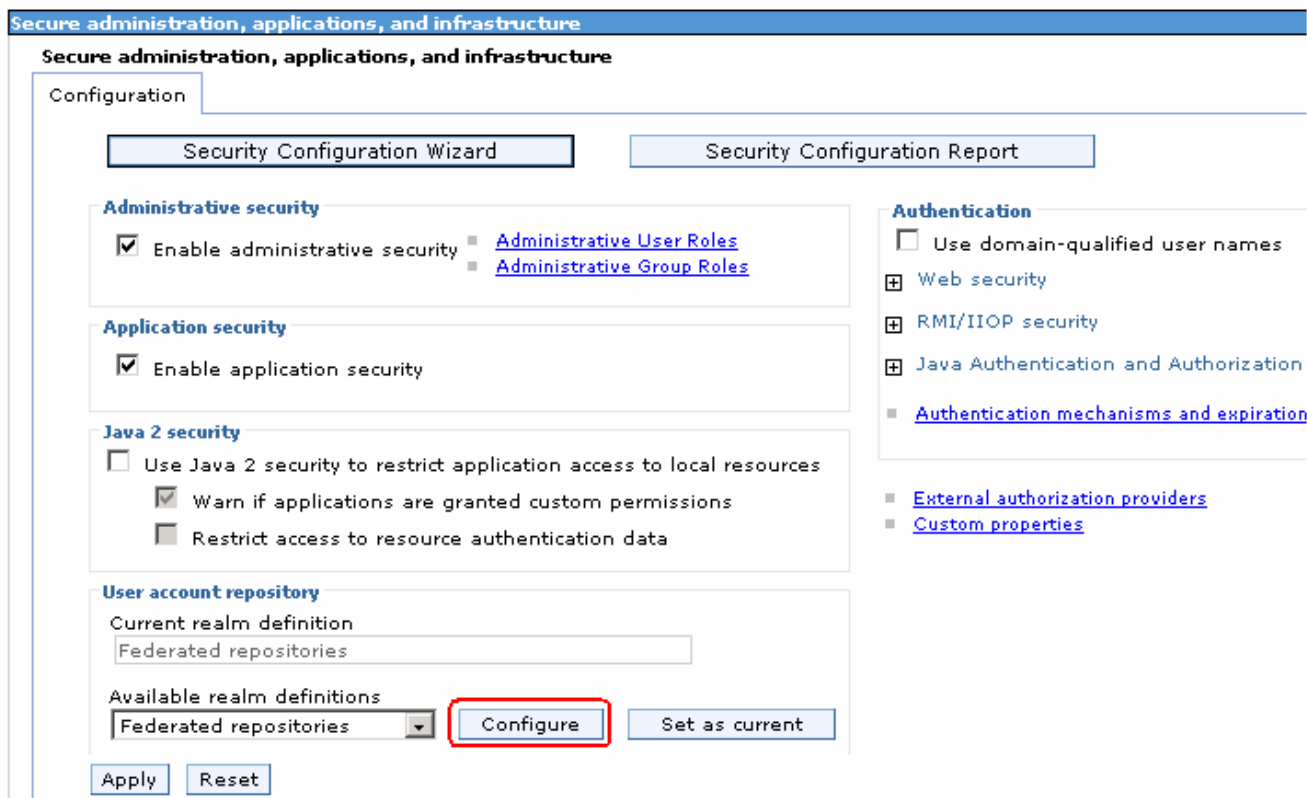
- ___ 9. In the following '**Step 3: Configure user repository**' panel, enter the primary administrative user name and password
 - ___ a. Primary administrative user name : **was61admin**
 - ___ b. Password : **was61admin**
 - ___ c. Confirm password : **was61admin**



- ___ 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**

General Properties

* Realm name
idsldap.austin.ibm.com:389

* Primary administrative user name
was61admin

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

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

Password

Ignore case for authorization

Repositories in the realm:

Add Base entry to Realm... Use built-in repository Remove

Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

Additional Properties

- Property extension repository
- Entry mapping repository
- Supported entity types

Related Items

- Manage repositories

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

Secure administration, applications, and infrastructure

Secure administration, applications, and infrastructure > Federated repositories > Repository reference

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

Configuration

General Properties

* Repository
 none defined

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

Distinguished name of a base entry in this repository

- ___ 16. Click the '**Add Repository**' button
- ___ 17. In the following new repository reference panel, enter the following:
- ___ a. Repository identifier : **LDAP-idldap** (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

General Properties

* Repository identifier
LDAP-idslldap

LDAP server

* Directory type
IBM Tivoli Directory Server Version 6

* Primary host name Port
idslldap.austin.ibm.com 389

Failover server used when primary is not available:

Delete
Select Failover host name Port
None

Add

Support referrals to other LDAP servers
ignore

Security

Bind distinguished name
uid=wpsbind,cn=users,dc=ibr

Bind password

Login properties
uid

Certificate mapping
EXACT_DN

Certificate filter

Require SSL communications

Centrally managed

- [Manage endpoint security configurations](#)

Use specific SSL alias
 NodeDefaultSSLSettings

- ___ 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-idslldap**' 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**

General Properties

* Repository
LDAP-idslldap Add Repository...

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

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

Apply Reset Cancel

- ___ 20. Click **OK**
- ___ 21. The 'Federated repositories' panel should look like the picture shown below:

General Properties

* Realm name

* Primary administrative user name

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

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

Password

Ignore case for authorization

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

- ___ 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.

General Properties

- * Realm name
idsldap.austin.ibm.com:389
- * Primary administrative user name
was61admin

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

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

Password

Ignore case for authorization

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6

___ 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

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6

Additional Properties

Related Items

- [Property extension repository](#)
- [Entry mapping repository](#)
- [Supported entity types](#) ←
- [Manage repositories](#)

- ___ 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:

Secure administration, applications, and infrastructure

[Secure administration, applications, and infrastructure](#) > [Federated repositories](#) > **Supported entity types**

Use this page to configure entity types that are supported by the member repositories.

Preferences

Entity type	Base entry for the default parent	Relative Distinguished Name properties
Group	dc=ibm,dc=com	cn
OrgContainer	dc=ibm,dc=com	o;ou;dc;cn
PersonAccount	dc=ibm,dc=com	uid
Total 3		

__ 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-idslldap**)

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idslldap	LDAP:IDS6

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

Additional Properties

- [Performance](#)
- [LDAP entity types](#) ←
- [Group attribute definition](#)

__ 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)**

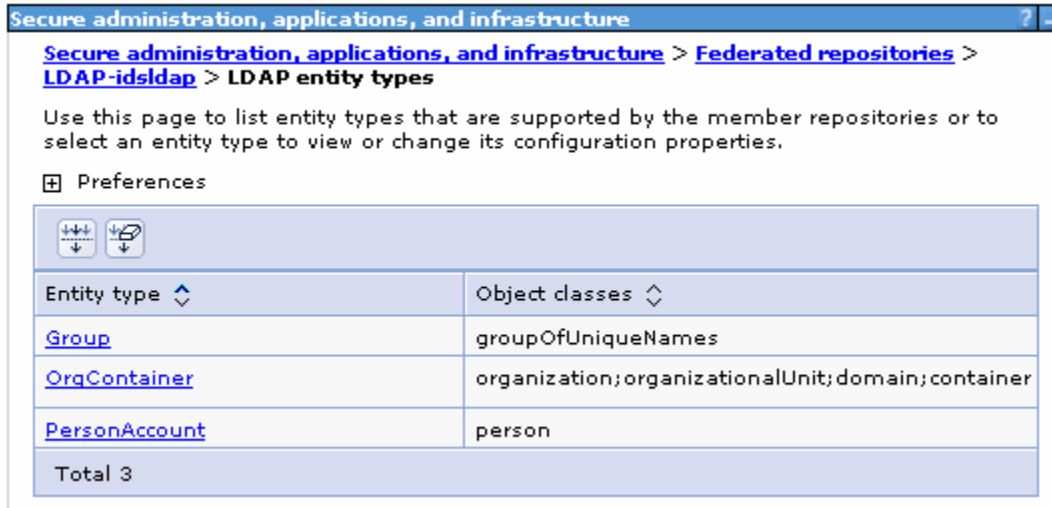
2) OrgContainer

- <Accept the defaults>

3) PersonAccount

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

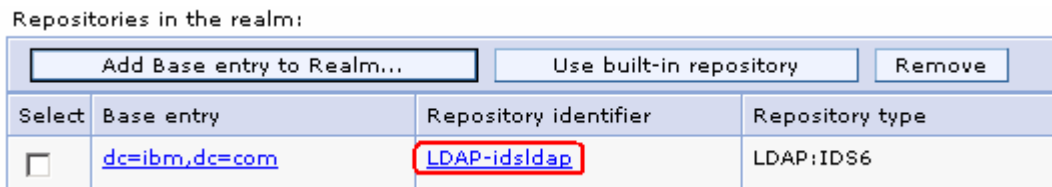
2) The 'LDAP entity' panel will look like the picture below:



___ 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**'

Configuration

General Properties

Name of group membership attribute
 ←

Scope of group membership attribute

Direct - Contains only immediate members of the group without members of subgroups

Nested - Contains direct members and members nested within subgroups of this group

→ All - Contains all direct, nested, and dynamic members

Apply OK Reset Cancel

Additional Properties

- Member attributes
- [Dynamic member attributes](#)

- Click **Apply**

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

Secure administration, applications, and infrastructure

[Secure administration, applications, and infrastructure](#) >
 [Federated repositories](#) >
 [LDAP-idsldap](#) >
 [Group attribute definition](#) >
 [Member attributes](#)

Use this page to manage Lightweight Directory Access Protocol (LDAP) member attributes.

⊕ Preferences

New Delete

Select	Name	Scope	Object class
<input type="checkbox"/>	member	all	groupOfNames
Total 2			

___ 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**'

General Properties

* Name of member attribute
uniqueMember

Object class
groupOfUniqueNames

Scope

Direct - Contains only immediate members of the group without members of subgroups

Nested - Contains direct members and members nested within subgroups of this group

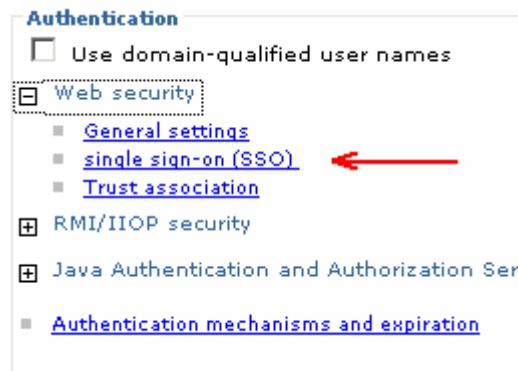
All - Contains all direct, nested, and dynamic members

- Click **OK**

___ g. Save to the master configuration

___ 26. Configure 'Single Sign-on'

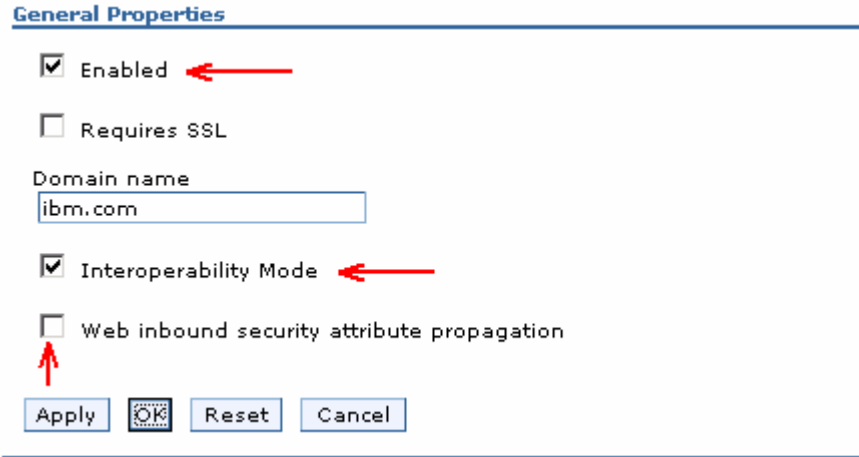
___ a. Navigate to the '**Secure administration, applications and infrastructure**' panel, expand '**Web Security**' under the '**Authentication**' category



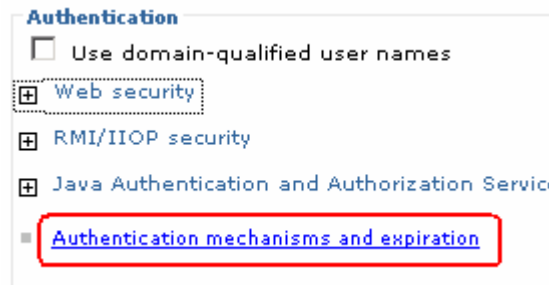
___ b. Click the '**single sign-on (SSO)**' link

___ 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**

Key generation

Authentication data is encrypted and decrypted by using keys that are kept in one or more key stores.

Key set group

■ [Key set groups](#)

Authentication expiration

Authentication information persists in the system for a limited amount of time before it expires and must be refreshed.

Authentication cache timeout
 minutes seconds

Timeout value for forwarded credentials between servers
 minutes

Cross-cell single sign-on

Single sign-on across cells can be provided by sharing keys and passwords. To share the keys and password, log on to one cell, specify a key file, and click Export keys. Then, log on to the other cell, specify the key file, and click Import keys.

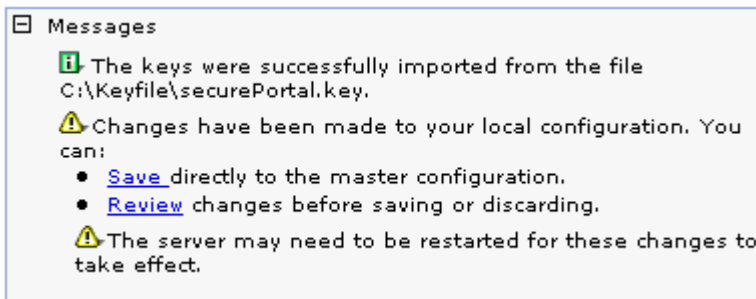
* Password ←

* Confirm password ←

Fully qualified key file name

Use SWAM-no authenticated communication between servers

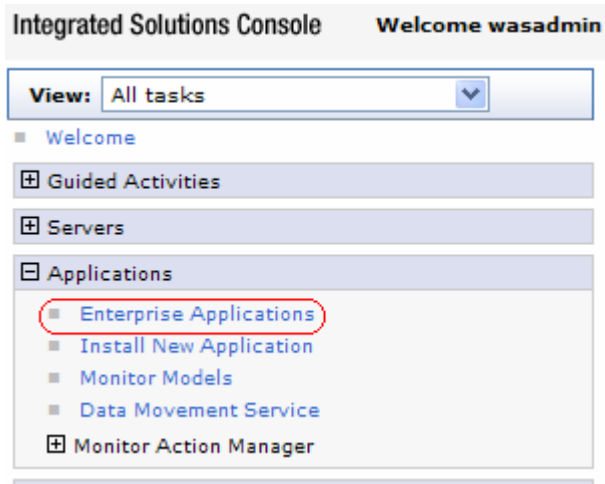
- ___ 30. Click the **'Import Keys'** button
- ___ 31. Click the **Save** link, to save the configuration



- ___ 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

Select	Name	Application Status
<input type="checkbox"/>	AlphabloxPlatform ←	➡
<input type="checkbox"/>	ApplicationStudio ←	➡
<input type="checkbox"/>	DefaultApplication	➡
<input type="checkbox"/>	IBM_WBM_ABX_WEB_DASHBOARD	➡
<input type="checkbox"/>	IBM_WBM_ACTIONSERVICES	➡
<input type="checkbox"/>	IBM_WBM_DMS_SERVICE	➡
<input type="checkbox"/>	IBM_WBM_REST_SERVICES ←	➡
<input type="checkbox"/>	IBM_WBM_WEB_DASHBOARD ←	➡
<input type="checkbox"/>	ivtApp	➡
<input type="checkbox"/>	query	➡
Total 10		

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

General Properties

* Name

Application reference validation

Detail Properties

- [Target specific application status](#)
- [Startup behavior](#)
- [Application binaries](#)
- [Class loading and update detection](#)
- [Remote request dispatcher properties](#)
- [Security role to user/group mapping](#)
- [View Deployment Descriptor](#)
- [Last participant support extension](#)

References

- [Shared library references](#)

Modules

- [Manage Modules](#)

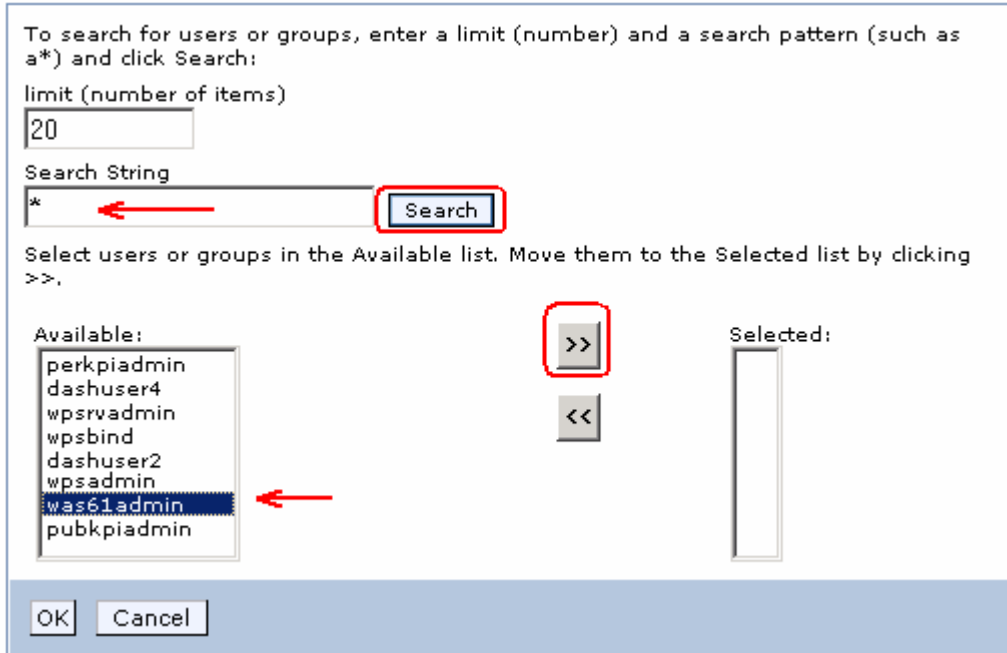
Web Module Properties

- [Session management](#)
- [Context Root For Web Modules](#)
- [Initialize parameters for servlets](#)
- [JSP reload options for web modules](#)
- [Virtual hosts](#)

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

<input type="button" value="Look up users"/> <input type="button" value="Look up groups"/>					
<input type="checkbox"/> <input type="checkbox"/>					
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
<input checked="" type="checkbox"/>	AlphabloxAdministrator	<input type="checkbox"/>	<input type="checkbox"/>		
<input type="checkbox"/>	AlphabloxUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	AlphabloxDeveloper	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

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:

Look up users		Look up groups			
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
<input type="checkbox"/>	AlphabloxAdministrator	<input type="checkbox"/>	<input type="checkbox"/>	was61admin	
<input type="checkbox"/>	AlphabloxUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	AlphabloxDeveloper	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

- ___ 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:

Look up users		Look up groups			
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
<input type="checkbox"/>	AlphabloxAdministrator	<input type="checkbox"/>	<input type="checkbox"/>	was61admin	
<input type="checkbox"/>	AlphabloxUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

___ 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

General Properties

* Name

Application reference validation

Detail Properties

- [Target specific application status](#)
- [Startup behavior](#)
- [Application binaries](#)
- [Class loading and update detection](#)
- [Remote request dispatcher properties](#)
- [Security role to user/group mapping](#)
- [View Deployment Descriptor](#)
- [Last participant support extension](#)

References

- [Shared library references](#)

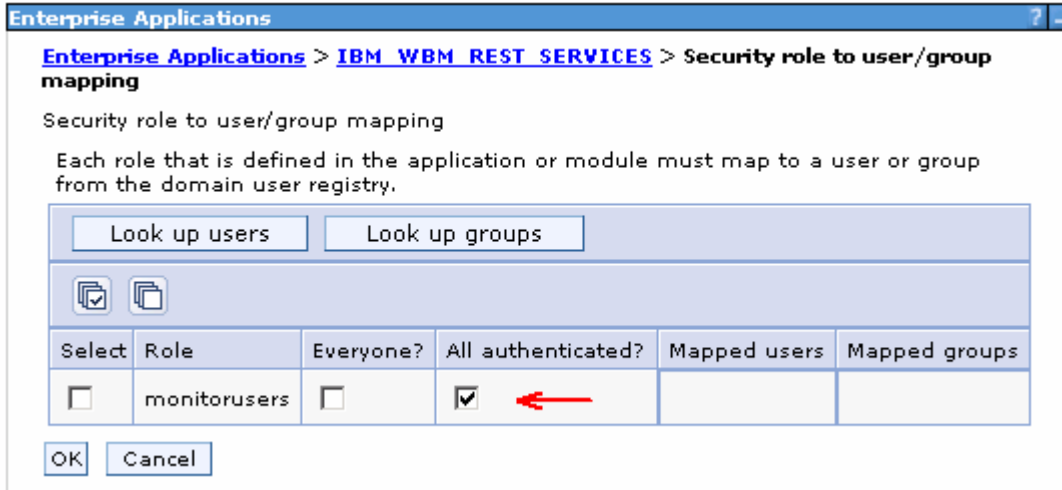
Modules

- [Manage Modules](#)

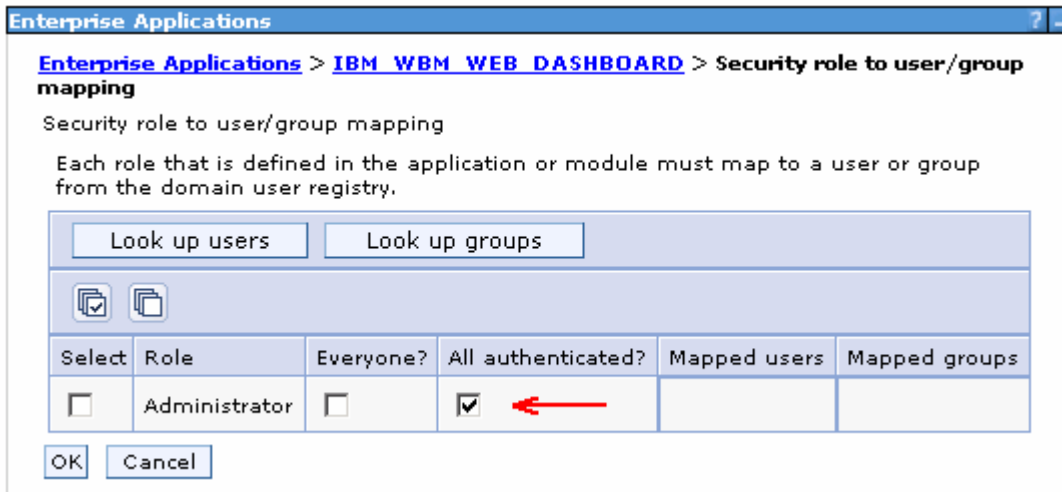
Web Module Properties

- [Session management](#)
- [Context Root For Web Modules](#)
- [JSP reload options for web modules](#)
- [Virtual hosts](#)

___ 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

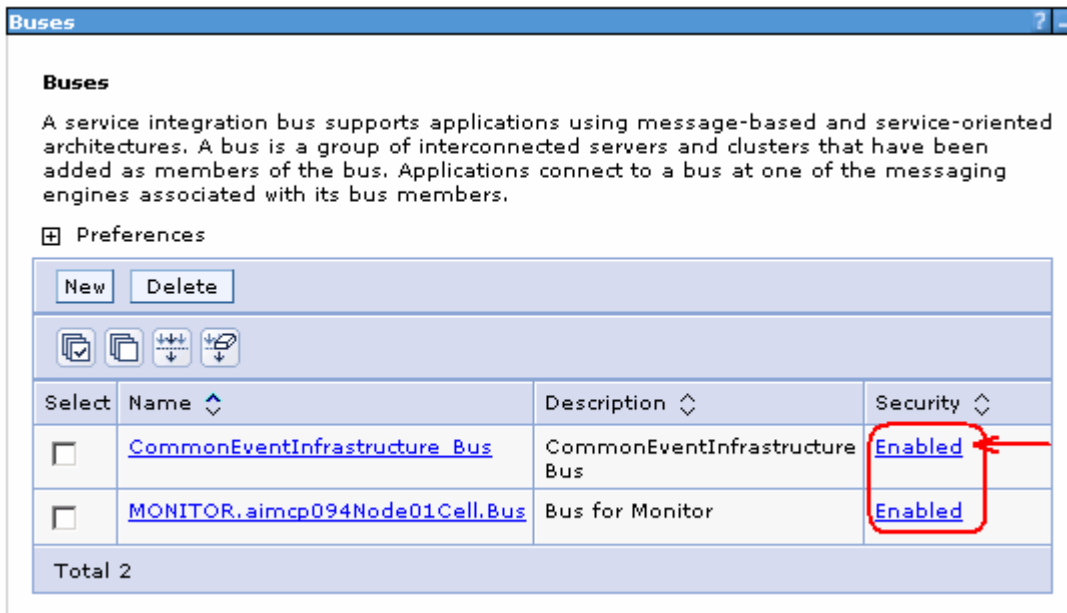
→Update J2C authentication data entries for messaging buses

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**

General Properties

* Alias

* User ID
 ←

* Password
 ←

Description

Apply OK Reset Cancel

___ 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

General Properties

Security

Enable bus security

Inter-engine authentication alias

Permitted transports

Allow the use of all defined transport channel chains

Restrict the use of defined transport channel chains to those protected by SSL

Restrict the use of defined transport channel chains to the list of permitted transports

Mediations authentication alias

Apply OK Reset Cancel

Additional Properties

- Users and groups in the bus connector role
- Permitted transports

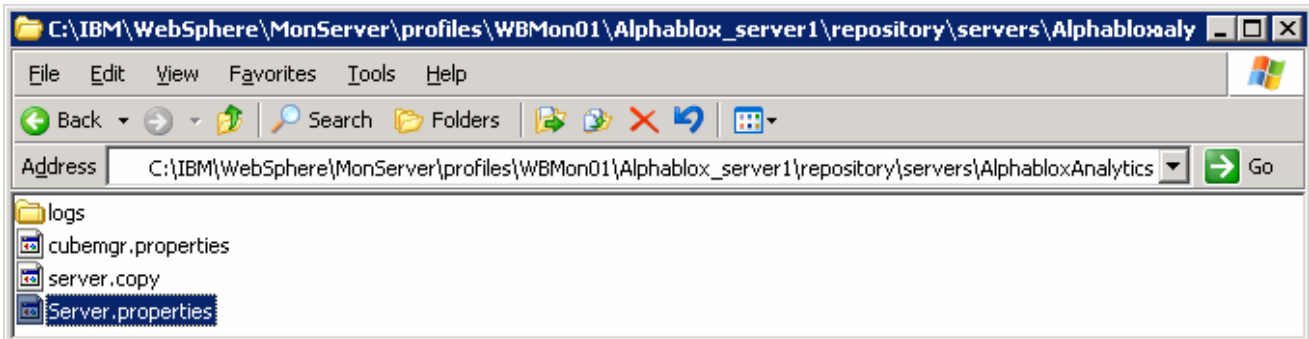
Related Items

- JAAS - J2C authentication data
- Secure Administration and Applications

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

New Delete		
Select	Name	Type
<input type="checkbox"/>	Server	Group
<input type="checkbox"/>	was61admin	User
Total 2		

- ___ 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 with 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:-

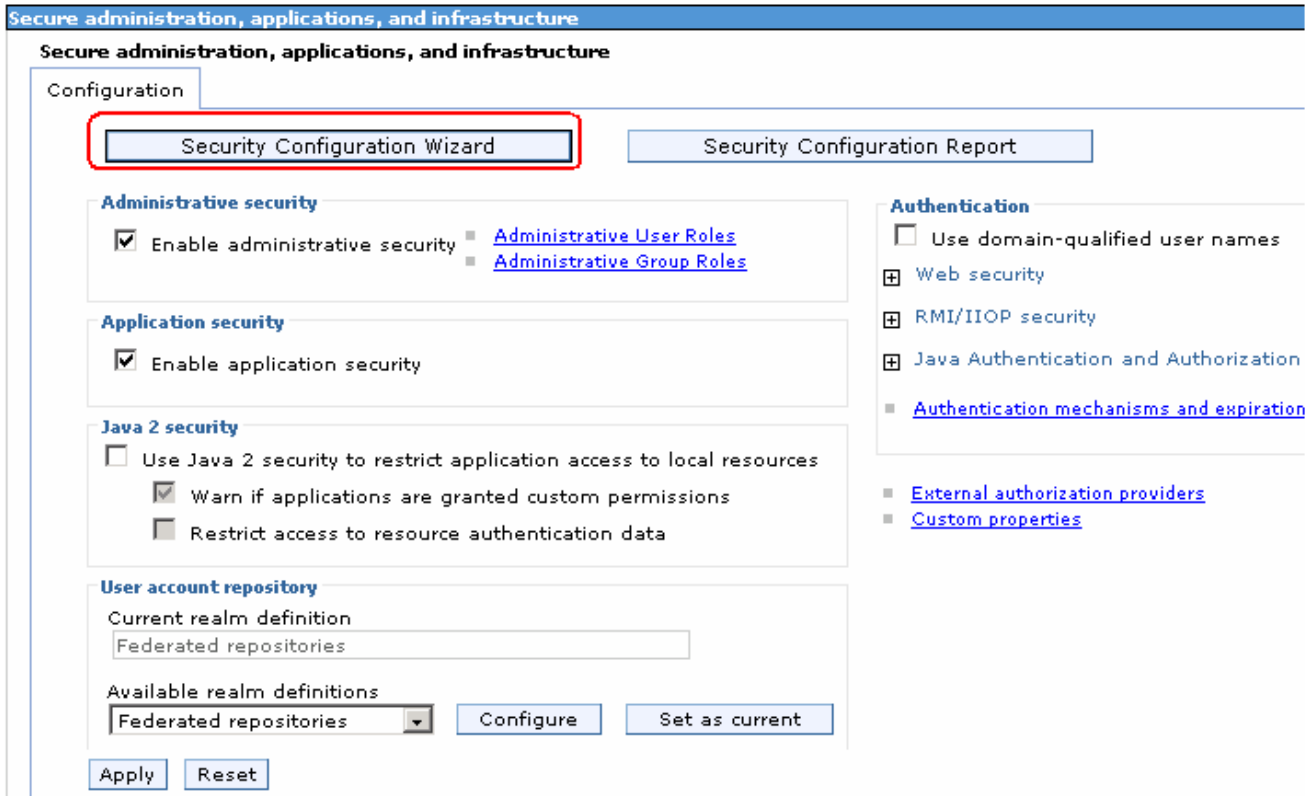
Copy the **securePortal.key** file that you have exported to a temporary location on to the Process Server machine

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

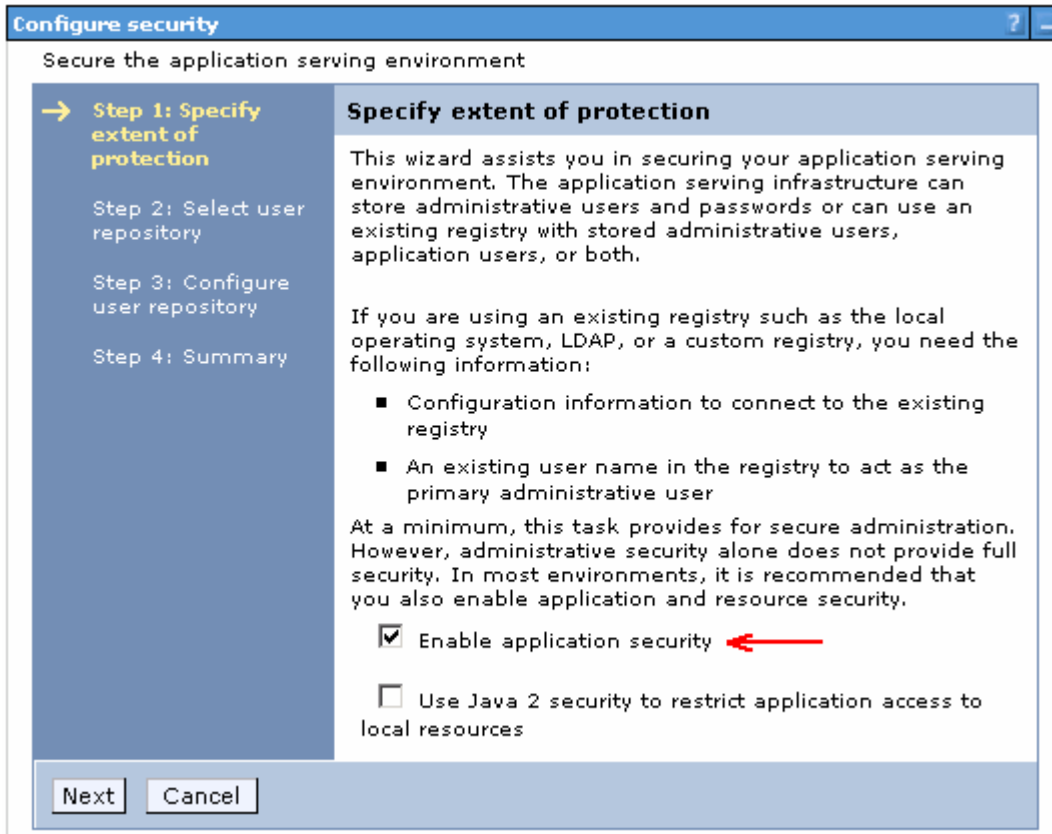
- ___ 1. Start the process server profile and launch the administrative console
- ___ 2. Login to the administrative console using the user name and password if the default security is enabled at this time
- ___ 3. In the administrative console's left navigation pane, expand '**Security**' and click 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

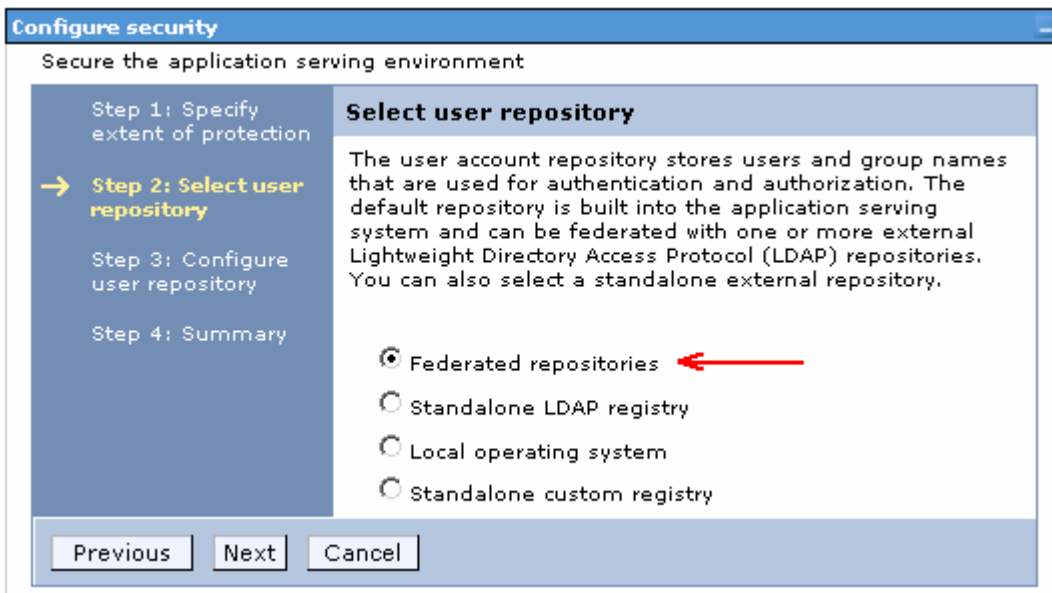


5. In the following 'Step1: Specify extent of protection' panel, ensure the check box for 'Enable application security' is selected



___ 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.

Configure user repository

A secure, file-based user repository is built into the system for storing administrative users or environments with a small number of users. The file-based user repository can be federated with one or more external LDAP repositories. If this is the first time security has been enabled using this repository, provide a new user name and password to act as an administrator. If security was previously enabled using this repository, provide the name of a user with administrator privileges that is in the built-in repository.

Note: Use this panel to configure a federated repository with a built-in, file-based repository in the realm. To configure a federated repository with a non file-based repository in the realm, you must use the User accounts repository section on the Secure administration, applications, and infrastructure panel.

* Primary administrative user name

Password

Confirm password

Previous Next Cancel

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

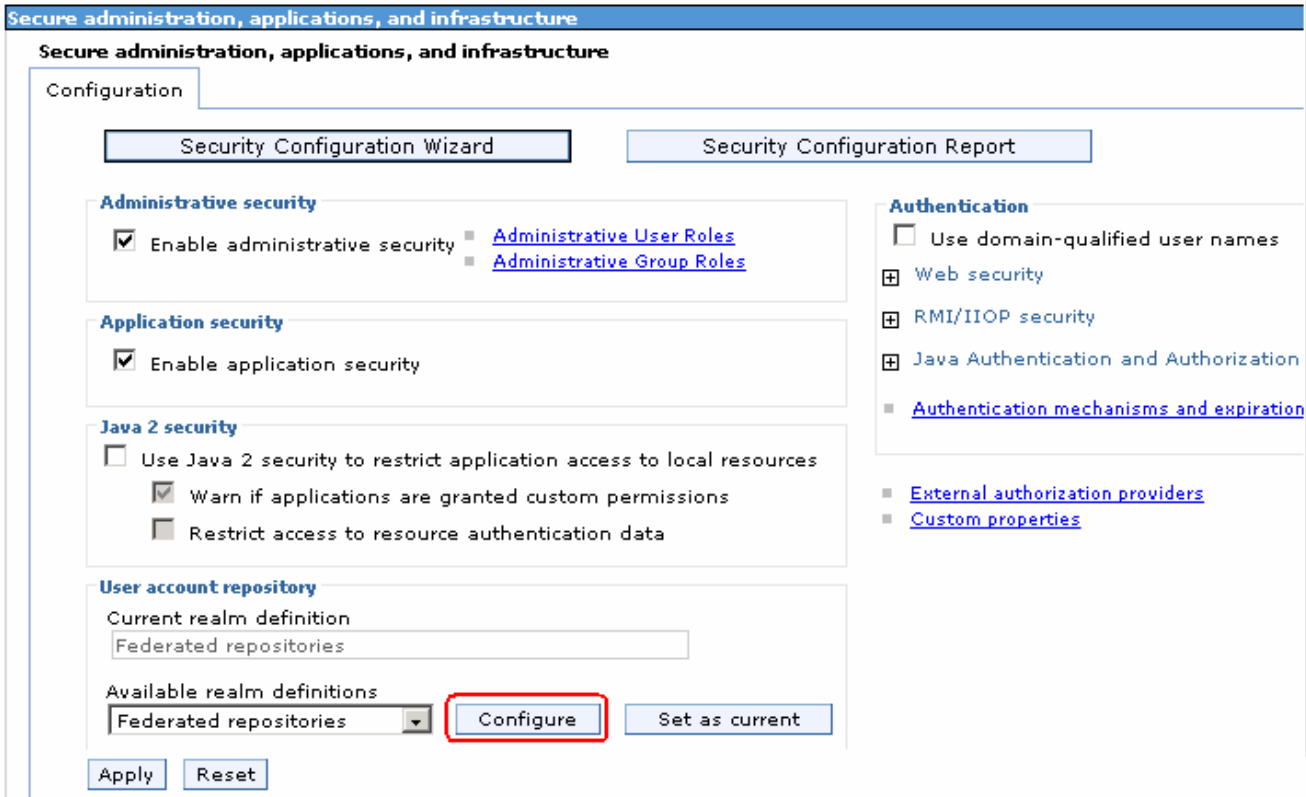
Summary

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

Options	Values
Enable administrative security	true
Enable application security	true
Use Java 2 security to restrict application access to local resources	false
User repository	Federated repositories
Primary administrative user name	wpsrvadmin

Previous Finish Cancel

- ___ 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**

General Properties

- * Realm name
idsldap.austin.ibm.com:389
- * Primary administrative user name
wpsrvadmin

Server user identity

- Automatically generated server identity
- Server identity that is stored in the repository
Server user ID or administrative user on a Version 6.0.x node
Password

- Ignore case for authorization

Repositories in the realm:

Add Base entry to Realm... Use built-in repository Remove

Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File

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

Secure administration, applications, and infrastructure > Federated repositories > Repository reference

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

Configuration

General Properties

- * Repository
none defined Add Repository...
- * Distinguished name of a base entry that uniquely identifies this set of entries in the realm
- Distinguished name of a base entry in this repository

Apply OK Reset Cancel

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

General Properties

* Repository identifier

LDAP server

* Directory type

* Primary host name Port

Failover server used when primary is not available:

Delete
Select
Failover host name
Port
None

Add

Support referrals to other LDAP servers

Security

Bind distinguished name

Bind password

Login properties

Certificate mapping

Certificate filter

Require SSL communications

Centrally managed
 [Manage endpoint security configurations](#)

Use specific SSL alias
 [SSL configurations](#)

___ 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**

General Properties

* Repository

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

Distinguished name of a base entry in this repository

___ 19. Click **OK**

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

General Properties

* Realm name

* Primary administrative user name

Server user identity

Automatically generated server identity

Server identity that is stored in the repository
Server user ID or administrative user on a Version 6.0.x node

Password

Ignore case for authorization

Repositories in the realm:

Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6
<input type="checkbox"/>	o=defaultWIMFileBasedRealm	InternalFileRepository	File ←

___ 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.

General Properties

* Realm name

* Primary administrative user name

Server user identity

Automatically generated server identity

Server identity that is stored in the repository

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

Password

Ignore case for authorization

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6

___ 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

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idsldap	LDAP:IDS6

Additional Properties

Related Items

- [Property extension repository](#)
- [Entry mapping repository](#)
- [Supported entity types](#) ←
- [Manage repositories](#)

___ 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:

Secure administration, applications, and infrastructure

[Secure administration, applications, and infrastructure](#) > [Federated repositories](#) > **Supported entity types**

Use this page to configure entity types that are supported by the member repositories.

Preferences

Entity type	Base entry for the default parent	Relative Distinguished Name properties
Group	dc=ibm,dc=com	cn
OrgContainer	dc=ibm,dc=com	o;ou;dc;cn
PersonAccount	dc=ibm,dc=com	uid
Total 3		

__ 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-idslldap**)

Repositories in the realm:

<input type="button" value="Add Base entry to Realm..."/>		<input type="button" value="Use built-in repository"/>	<input type="button" value="Remove"/>
Select	Base entry	Repository identifier	Repository type
<input type="checkbox"/>	dc=ibm,dc=com	LDAP-idslldap	LDAP:IDS6

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

Additional Properties

- [Performance](#)
- [LDAP entity types](#) ←
- [Group attribute definition](#)

__ 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)**

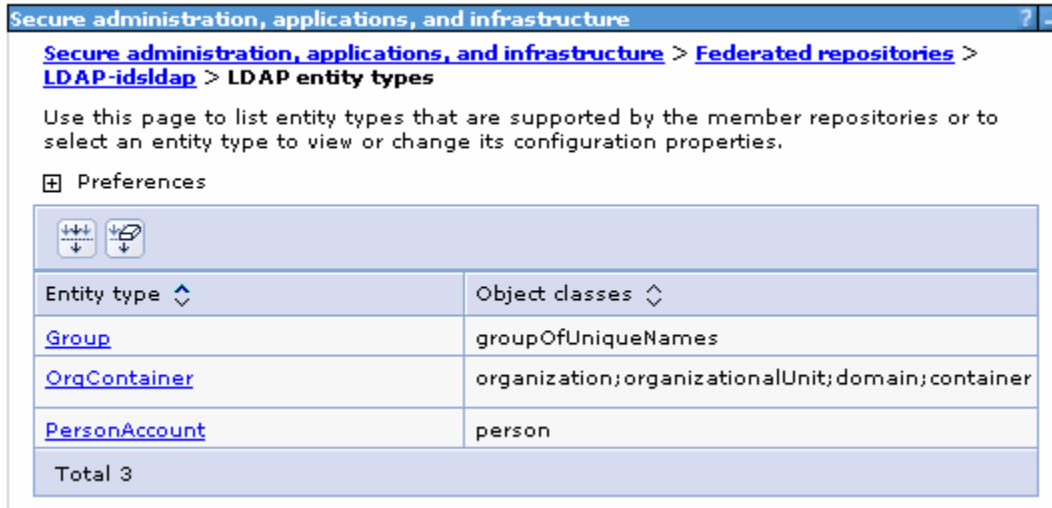
2) OrgContainer

- <Accept the defaults>

3) PersonAccount

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

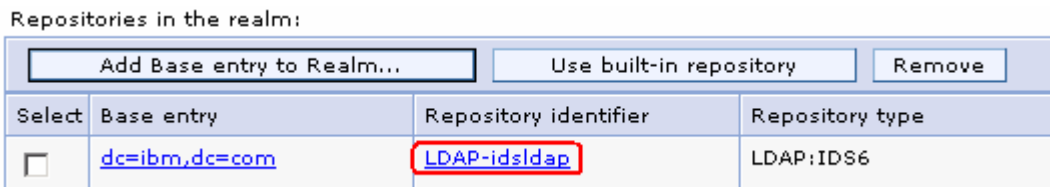
4) The 'LDAP entity' panel will look like the picture below:



___ 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**'

Configuration

General Properties

Name of group membership attribute
 ←

Scope of group membership attribute

Direct - Contains only immediate members of the group without members of subgroups

Nested - Contains direct members and members nested within subgroups of this group

→ All - Contains all direct, nested, and dynamic members

Apply OK Reset Cancel

Additional Properties

- Member attributes
- [Dynamic member attributes](#)

- Click **Apply**

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

Secure administration, applications, and infrastructure

[Secure administration, applications, and infrastructure](#) >
 [Federated repositories](#) >
 [LDAP-idsldap](#) >
 [Group attribute definition](#) >
 [Member attributes](#)

Use this page to manage Lightweight Directory Access Protocol (LDAP) member attributes.

⊕ Preferences

New Delete

☑
📄
↕
↕

Select	Name	Scope	Object class
<input type="checkbox"/>	member	all	groupOfNames

Total 2

___ 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**'

General Properties

* Name of member attribute
uniqueMember

Object class
groupOfUniqueNames

Scope

Direct - Contains only immediate members of the group without members of subgroups

Nested - Contains direct members and members nested within subgroups of this group

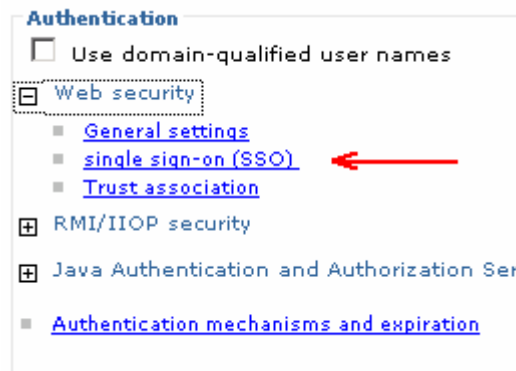
All - Contains all direct, nested, and dynamic members

- Click **OK**

___ g. Save to the master configuration

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

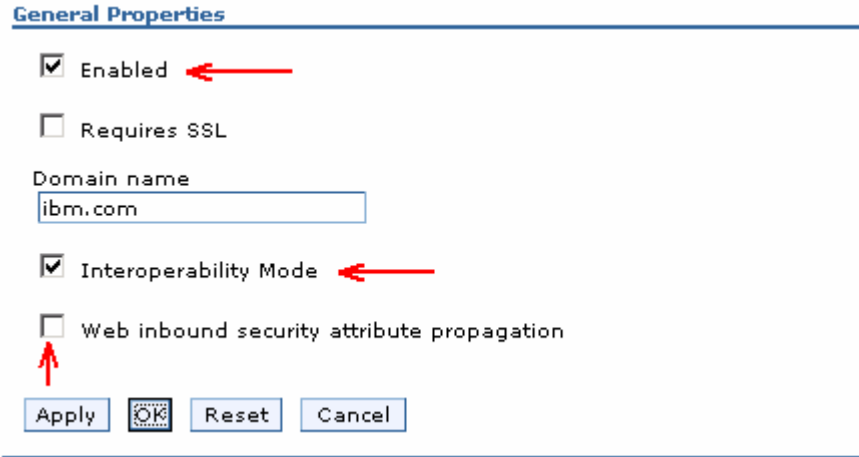
___ a. While you are in the '**Secure administration, applications and infrastructure**' panel, expand '**Web Security**' under the '**Authentication**' category



___ 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**

Key generation
Authentication data is encrypted and decrypted by using keys that are kept in one or more key stores.

Key set group
NodeLTPAKeySetGroup

■ [Key set groups](#)

Authentication expiration
Authentication information persists in the system for a limited amount of time before it expires and must be refreshed.

Authentication cache timeout
10 minutes 0 seconds

Timeout value for forwarded credentials between servers
120 minutes

Cross-cell single sign-on ←

Single sign-on across cells can be provided by sharing keys and passwords. To share the keys and password, log on to one cell, specify a key file, and click Export keys. Then, log on to the other cell, specify the key file, and click Import keys.

* Password ←

* Confirm password ←

Fully qualified key file name
C:\Keyfile\securePortal.key

Use SWAM-no authenticated communication between servers

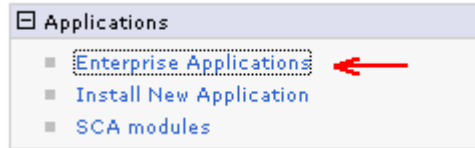
___ 30. Click the **'Import Keys'** button

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

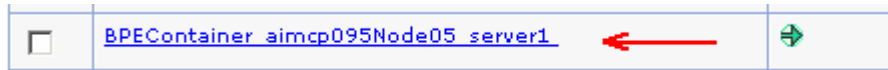
Note: To restart the server at this time, you should enter the old user name and password configured during the WebSphere Process Server profile creation.

→ 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

Enterprise Applications > **BPEContainer_aimcp095Node05_server1**

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

Configuration

General Properties

- * Name: BPEContainer_aimcp095Node05_server1
- Application reference validation: Issue warnings

Detail Properties

- [Target specific application status](#)
- [Startup behavior](#)
- [Application binaries](#)
- [Class loading and update detection](#)
- [Remote request dispatcher properties](#)
- [Security role to user/group mapping](#)
- [User RunAs roles](#)
- [View Deployment Descriptor](#)
- [Last participant support extension](#)

References

- [Resource references](#)

Modules

- [Manage Modules](#)

Web Module Properties

- [Session management](#)
- [Context Root For Web Modules](#)
- [JSP reload options for web modules](#)
- [Virtual hosts](#)

Enterprise Java Bean Properties

- [Application profiles](#)
- [Message Driven Bean listener bindings](#)
- [EJB JNDI names](#)

Web Services Properties

- [Provide JMS and EJB endpoint URL information](#)
- [Publish WSDL files](#)
- [Provide HTTP endpoint URL information](#)

4. In the following 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

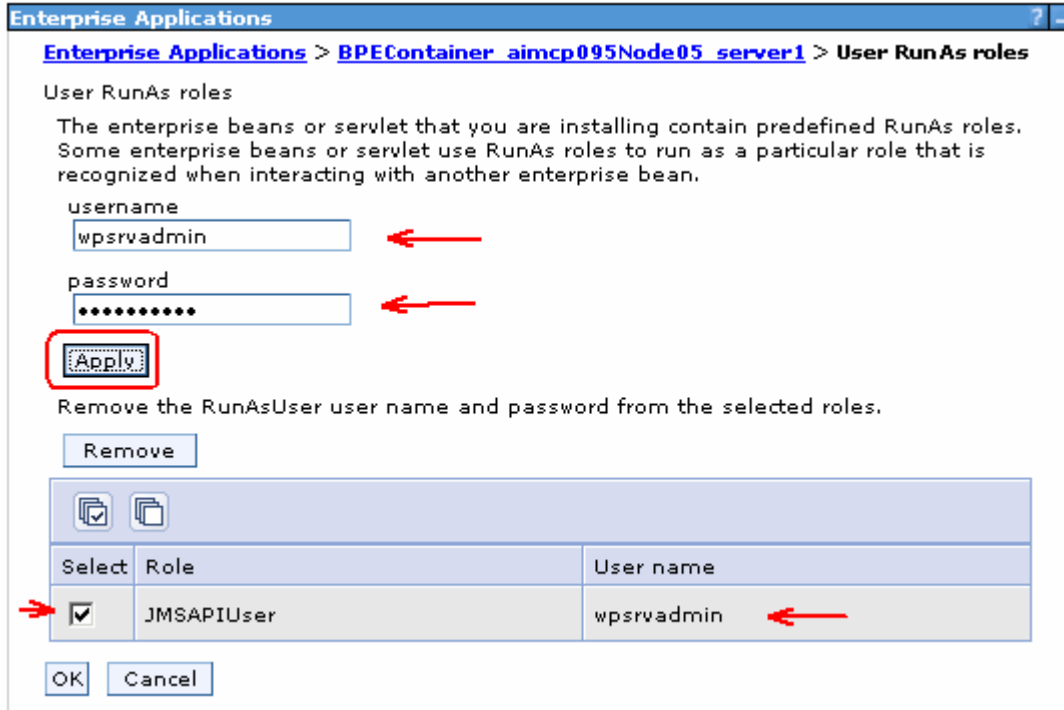
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
<input type="checkbox"/>	BPEAPIUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	BPESystemAdministrator	<input type="checkbox"/>	<input type="checkbox"/>	wpsrvadmin	
<input type="checkbox"/>	BPESystemMonitor	<input type="checkbox"/>	<input type="checkbox"/>	wpsrvadmin	
<input type="checkbox"/>	WebClientUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		
<input type="checkbox"/>	JMSAPIUser	<input type="checkbox"/>	<input checked="" type="checkbox"/>		

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

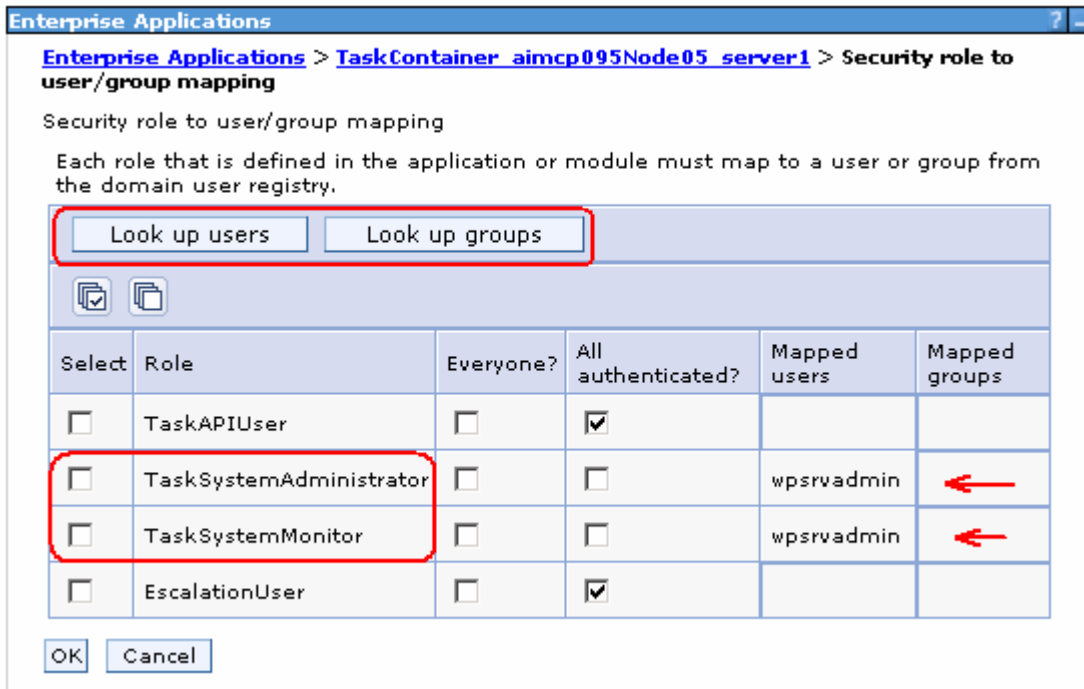
Detail Properties

- [Target specific application status](#)
- [Startup behavior](#)
- [Application binaries](#)
- [Class loading and update detection](#)
- [Remote request dispatcher properties](#)
- [Security role to user/group mapping](#)
- [User RunAs roles](#)
- [View Deployment Descriptor](#)
- [Last participant support extension](#)

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**

Enterprise Applications > **BPCExplorer_aimcp095Node05_server1** > **Security role to user/group mapping**

Security role to user/group mapping
Each role that is defined in the application or module must map to a user or group from the domain user registry.

Look up users Look up groups

Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
<input type="checkbox"/>	WebClientUser	<input type="checkbox"/>	<input checked="" type="checkbox"/> ←		

OK Cancel

___ 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'

Buses

A service integration bus supports applications using message-based and service-oriented architectures. A bus is a group of interconnected servers and clusters that have been added as members of the bus. Applications connect to a bus at one of the messaging engines associated with its bus members.

⊕ Preferences

New Delete

Select	Name	Description	Security
<input type="checkbox"/>	BPC.aimcp095Node03Cell.Bus	Messaging bus for Process Choreographer	Enabled
<input checked="" type="checkbox"/>	CommonEventInfrastructure_Bus	CommonEventInfrastructure Bus	Enabled
<input type="checkbox"/>	SCA.APPLICATION.aimcp095Node03Cell.Bus	Messaging bus for Service	Enabled
<input type="checkbox"/>	SCA.SYSTEM.aimcp095Node03Cell.Bus	Messaging bus for Service	Enabled

Total 5

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

Related Items

- [JAAS - J2C authentication data](#)
- [Secure Administration and Applications](#)

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**

General Properties

* Alias
CommonEventInfrastructureJMSAuthAlias

* User ID
wpsrvadmin ←

* Password
***** ←

Description
Authentication alias for the C

Apply OK Reset Cancel

- ___ 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

General Properties

Security

Enable bus security

Inter-engine authentication alias
MonitorBusAuth

Permitted transports

Allow the use of all defined transport channel chains

Restrict the use of defined transport channel chains to those protected by SSL

Restrict the use of defined transport channel chains to the list of permitted transports

Mediations authentication alias
(none)

Apply OK Reset Cancel

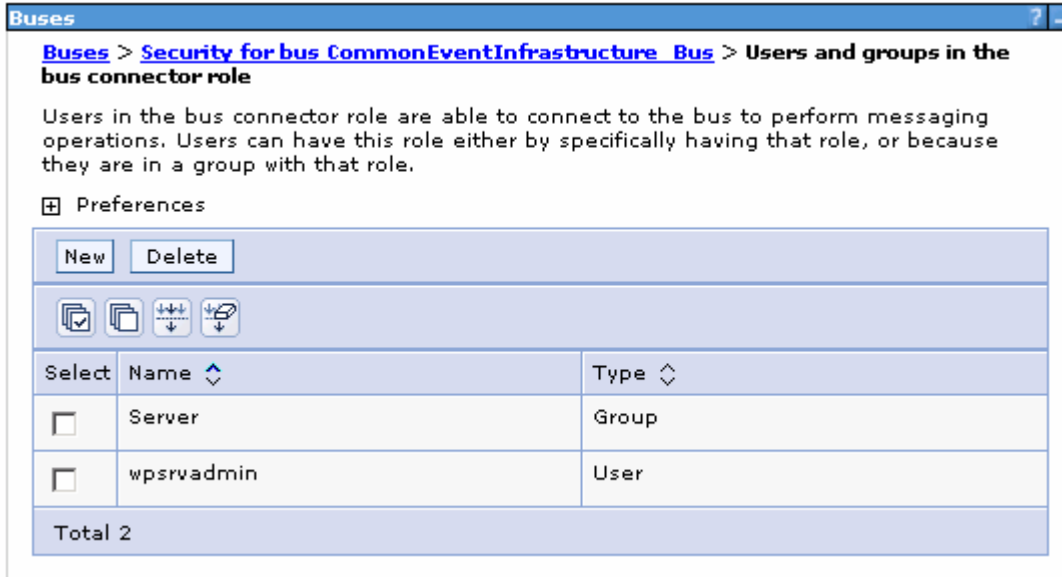
Additional Properties

- [Users and groups in the bus connector role](#)
- [Permitted transports](#)

Related Items

- [JAAS - J2C authentication data](#)
- [Secure Administration and Applications](#)

- ___ 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

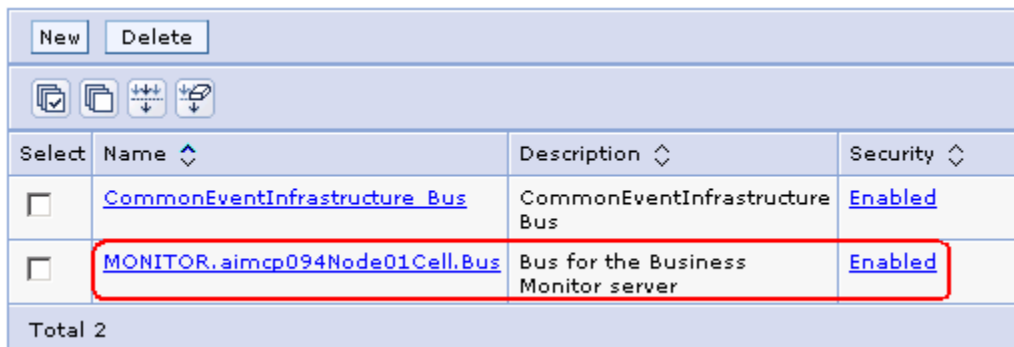
Part 5: Configure Remote CEI server to use WebSphere Business Monitor in a secured environment

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 without 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**'



Select	Name	Description	Security
<input type="checkbox"/>	CommonEventInfrastructure Bus	CommonEventInfrastructure Bus	Enabled
<input type="checkbox"/>	MONITOR.aimcp094Node01Cell.Bus	Bus for the Business Monitor server	Enabled

Total 2

- 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:\IBM\WebSphere\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

Select	Name	Path
<input type="checkbox"/>	NodeDefaultKeyStore	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/key.p12
<input type="checkbox"/>	NodeDefaultTrustStore	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/trust.p12
<input type="checkbox"/>	NodeLTPAKeys	\${CONFIG_ROOT}/cells/aimcp094Node01Cell/nodes/aimcp094Node01/ltpa.jceks

Total 3

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

Additional Properties

- **Signer certificates**
- [Personal certificates](#)
- [Personal certificate requests](#)
- [Custom properties](#)

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

<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Extract"/> <input type="button" value="Retrieve from port"/>				
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>				
Select	Alias	Issued to	Fingerprint (SHA digest)	Expiration
<input type="checkbox"/>	default	CN=██████████.austin.ibm.com, O=IBM, C=US	5F:7D:2C:48:EF:D8:E1:49:A6:C0	Valid from February 25,
<input type="checkbox"/>	dummyclientsigner	CN=jdient, OU=SWG, O=IBM, C=US	0B:3F:C9:E0:70:54:58:F7:FD:81	Valid from July 30, 2003
<input type="checkbox"/>	dummyserversigner	CN=jserver, OU=SWG, O=IBM, C=US	FB:38:FE:E6:CF:89:BA:01:67:8F:	Valid from July 30, 2003

- 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**

General Properties

* Host

* Port

SSL configuration for outbound connection

* Alias

- Click the 'Retrieve signer information' button
- You should see the following signer information that is retrieved from the remote CEI server

General Properties

* Host

* Port

SSL configuration for outbound connection

* Alias

Retrieved signer information

Serial number

Issued to

Issued by

Fingerprint (SHA digest)

Validity period

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

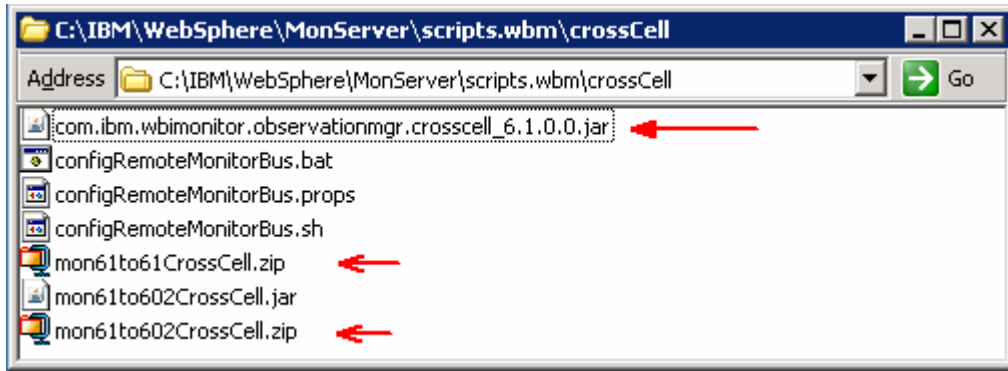
Remote CEI Server (WebSphere Process Server V6.1):

- 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)

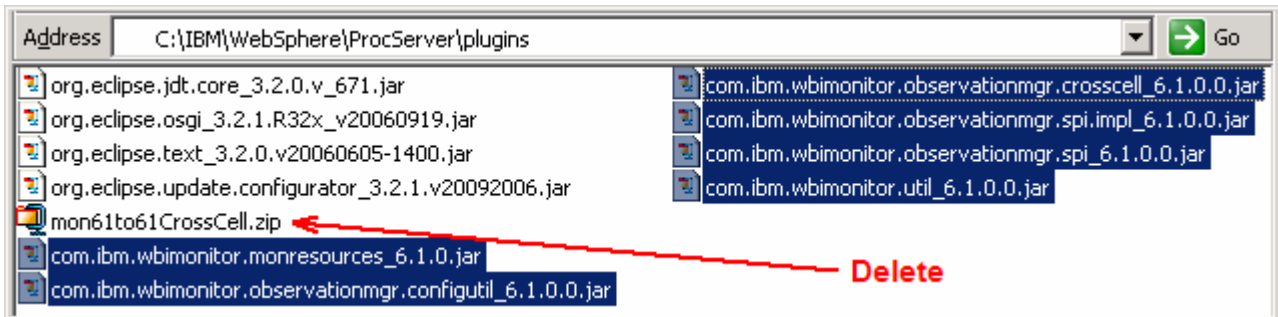


___ 2. Depending on the type of remote CEI server, take the appropriate action.

___ 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



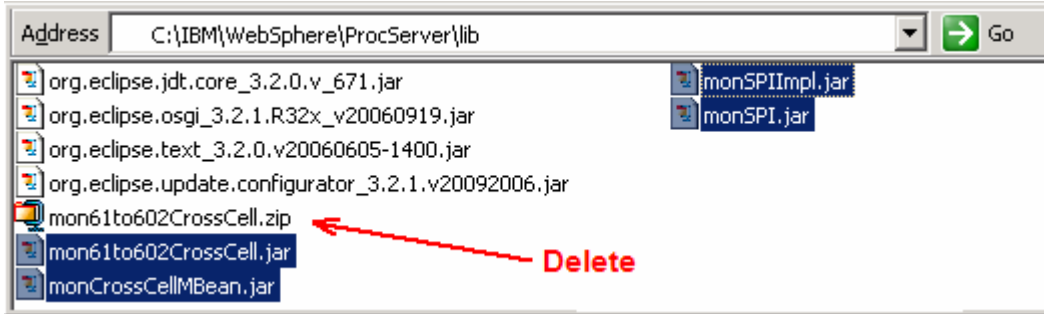
2) If WebSphere Business Monitor 6.1 is installed both locally and on the remote CEI server:

From the **<WBM_HOME>/scripts.wbm/crossCell** directory of the local Business Monitor server installation, copy the **com.ibm.wbmonitor.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

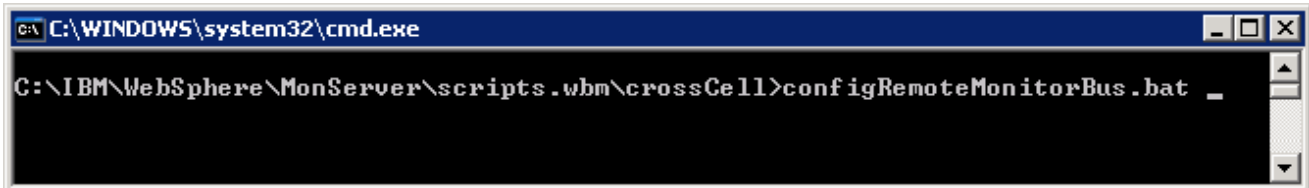


2) Restart the WebSphere Process Server

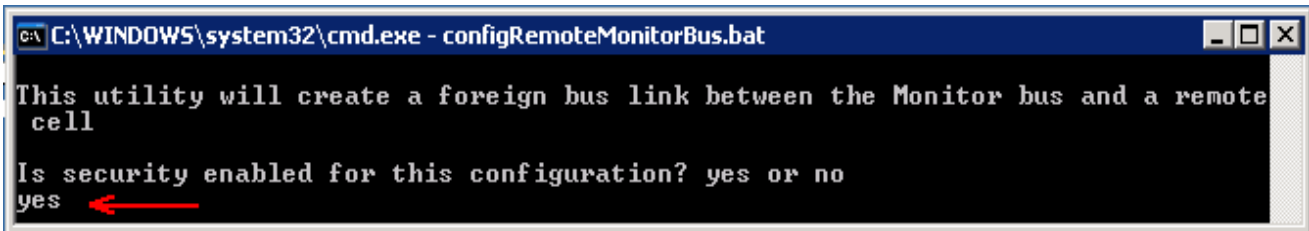
3. Run the '**configRemoteMonitorBus.bat**' script on the local WebSphere Business Monitor server

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

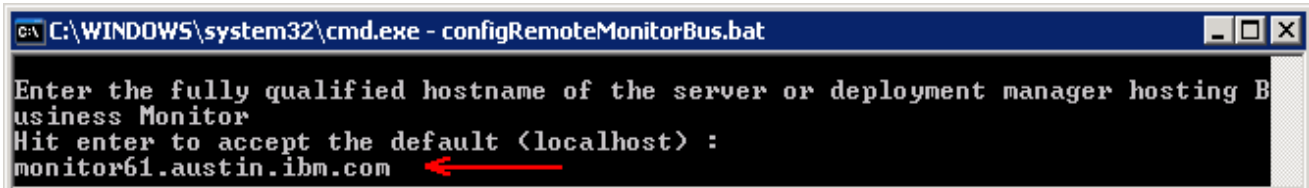


b. Type '**yes**' when prompted to answer the question '**Is security enabled for this configuration?**'



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 Business 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: wpsradmin)

```
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.

```
C:\WINDOWS\system32\cmd.exe - configRemoteMonitorBus.bat
The Monitor bus link requires a userid where the user name is valid in both cells.
The password can be unique to each cell, but the name must be the same
Enter a user name that is valid in both cells :
buslinkuser
```

- __ 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.