

# Exercise 13 – Configuring application security

At the end of the exercise, you should be able to:

- Define Java EE security roles
- Define access for resources in an application
- Enable and verify application security

## Section 1: Enabling application security

In a previous exercise, administrative security was configured. This exercise enables and configures application security. The application security allows WebSphere to provide authentication and authorization for the enterprise applications. So, unlike administrative security (which secures the administrative interfaces), application security controls who has access to which parts of the enterprise applications that are run within the application servers.

In this section of the lab, WebSphere application security is enabled through the administrative console.

The screenshot shows the WebSphere administrative console interface. The left sidebar contains a navigation tree with categories like 'Welcome', 'Guided Activities', 'Servers', 'Applications', 'Jobs', 'Services', 'Resources', 'Runtime Operations', 'Security', 'Operational policies', 'Environment', 'System administration', 'Users and Groups', 'Monitoring and Tuning', 'Troubleshooting', 'Service integration', and 'UDDI'. The 'Security' category is expanded, showing sub-items like 'Global security', 'Security domains', 'Administrative Authorization Groups', 'SSL certificate and key management', 'Security auditing', 'Bus security', and 'JAX-WS and JAX-RPC security runtime'. The main content area is titled 'Global security' and includes a description of its purpose. It features two tabs: 'Security Configuration Wizard' (active) and 'Security Configuration Report'. Under 'Administrative security', the 'Enable administrative security' checkbox is checked, with links for 'Administrative user roles', 'Administrative group roles', and 'Administrative authentication'. Under 'Application security', the 'Enable application security' checkbox is also checked. The 'Java 2 security' section has the 'Use Java 2 security to restrict application access to local resources' checkbox unchecked. The 'User account repository' section shows the 'Realm name' as 'defaultWIMFileBasedRealm' and the 'Current realm definition' as 'Federated repositories'. There are buttons for 'Configure...' and 'Set as current'.

The screenshot shows the 'WebSphere application server clusters' page in the administrative console. The left sidebar is similar to the previous screenshot, but the 'Servers' category is expanded, showing 'New server', 'All servers', 'Server Types', 'Clusters', 'DataPower', and 'Core Groups'. The 'Clusters' category is further expanded, showing 'WebSphere application server clusters', 'Proxy server clusters', 'Generic server clusters', 'Cluster topology', 'On Demand Router clusters', and 'Dynamic clusters'. The main content area is titled 'WebSphere application server clusters' and includes a description of a server cluster. It features a 'Preferences' section with buttons for 'New...', 'Delete', 'Start', 'Stop', 'Ripplestart', and 'ImmediateStop'. Below this is a table with columns 'Select', 'Name', and 'Status'. The table lists one cluster, 'PlantsCluster', which is currently stopped. A message box at the top of the main content area states: 'Cluster member server2 will not be started because the Node Agent on node wasnd-node01Node02 is not active. Cluster members can be started individually from the cluster member collection panel. The ripple start operation on cluster PlantsCluster has been initiated. Each cluster member will be stopped and started in sequence. It may take several minutes for this operation to complete.'

## Section 2: Securing the PlantsByWebSphere application

When running with application security enabled, enterprise applications can take advantage of role-based application security to restrict access to servlet and EJB resources. The PlantsByWebSphere application administration module is already configured to take advantage of application security by having a security role that is called SampAdmin and mapping to the administration module. All that the administrator is still required to do is to map the SampAdmin security role to the users or groups that exist in the runtime environment.

**Java 2 security** can also be used to provide fine-grained access to system resources, such as ports or sockets. Java 2 security is orthogonal to Java Platform, Enterprise Edition or Java EE security and does not require the enforcement of administrative security. In this exercise, you do not use Java 2 security.

Manage Users

Manage Users

### Create a User

\* User ID

PlantsUser

Group Membership

\* First name

Plants

\* Last name

User

E-mail

\* Password

.....

\* Confirm password

.....

Create

Cancel

## Manage Users

### Manage Users



The user was created successfully.

[PlantsUser](#)

Create Like

Close



Not Secure | 34.141.79.132/PlantsByWebSphere/admin.html

Error 403: AuthorizationFailed

Error 403: AuthorizationFailed

**WebSphere** software

**View:** All tasks ▾

- Welcome
- Guided Activities
- Servers
- Applications
- Jobs
- Services
- Resources
- Runtime Operations
- Security
- Operational policies
- Environment
- System administration
- Users and Groups
  - Administrative user roles
  - Administrative group roles
  - Manage Users
  - Manage Groups

### Manage Groups

#### Create a Group

\* Group name

Description

**Create** **Cancel**

## Manage Groups

### Manage Groups



The group was created successfully.

[PlantsGroup](#)

Create Like

Close

## Manage Groups

### Manage Groups

#### Add Users to a Group

Group name

PlantsGroup

Search for users that will be members of this group.

Search by

User ID ▼

\* Search for

\*

\* Maximum results

100

Search

9 users matched the search criteria.

DefaultAppAdmin  
PlantsAppAdmin  
PlantsUser  
wasadm  
wasadmin  
wascfg  
wasmon  
wasoper  
wassecmgr

Add

Close

## Manage Groups

### Manage Groups






#### Group Properties

**General** Members **Groups**

Group name

PlantsGroup

The group has 1 members.

<b>Add Users...</b>		<b>Add Groups...</b>		<b>Remove</b>				
Select	ID	Type	Unique Name					
<input type="checkbox"/>	PlantsUser		uid=PlantsUser,o=defaultWIMFileBasedRealm					
Page 1 of 1					Total: 1			

**Enterprise Applications****Enterprise Applications > pbw-ear**

Use this page to configure an enterprise application. Click the links to ac

**Configuration**

Service Policies

Routing Policies

Reports

C

**General Properties**

\* Name

pbw-ear

Application reference validation

Issue warnings

**Detail Properties**

- [Target specific application status](#)
- [Startup behavior](#)
- [Application binaries](#)
- [Class loading and update detection](#)
- [Request dispatcher properties](#)
- [Security role to user/group mapping](#)

Cell=wasnd-node01Cell01, Profile=Dmgr

**Enterprise Applications****Enterprise Applications > pbw-ear > Security role to user/group mapping**

Security role to user/group mapping

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

Map Users...

Map Groups...

Map Special Subjects



Select	Role	Special subjects	Mapped users	Mapped groups
<input checked="" type="checkbox"/>	SampAdmin	None		

OK

Cancel

## Enterprise Applications

[Enterprise Applications](#) > [pbw-ear](#) > [Security role to user/group mapping](#) > **Map users/groups**

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

- SampAdmin

## Search and Select Groups

Decide how many results to display, enter a search string (use \* for wildcard), and click Search. Select groups in the Available list and add them to role list.

Display a maximum of  
20 results

Search string

\*

Search

Available:



Selected:

PlantsGroup

OK Cancel

## Enterprise Applications

[Enterprise Applications](#) > [pbw-ear](#) > **Security role to user/group mapping**

Security role to user/group mapping

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

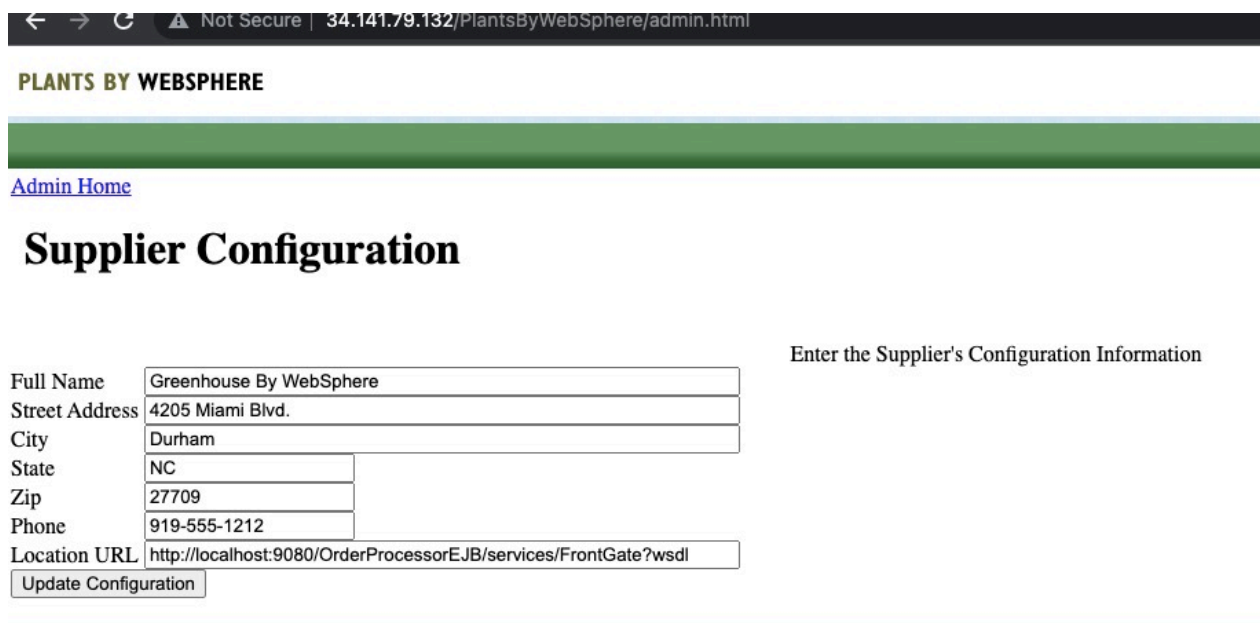
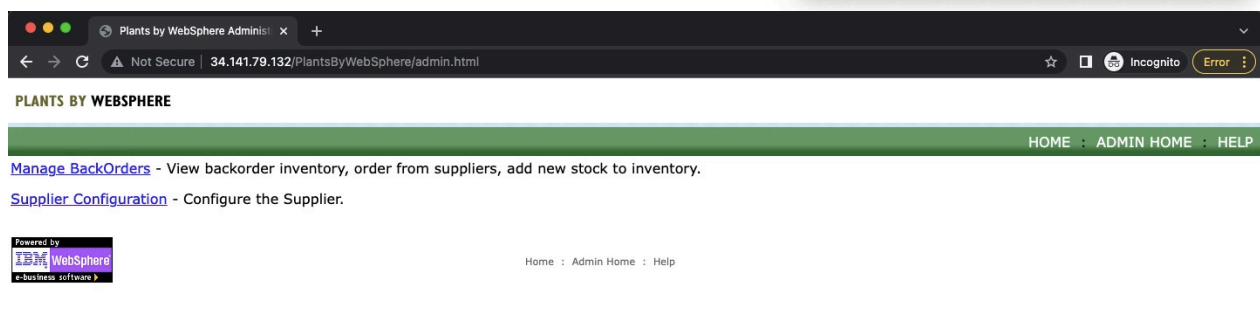
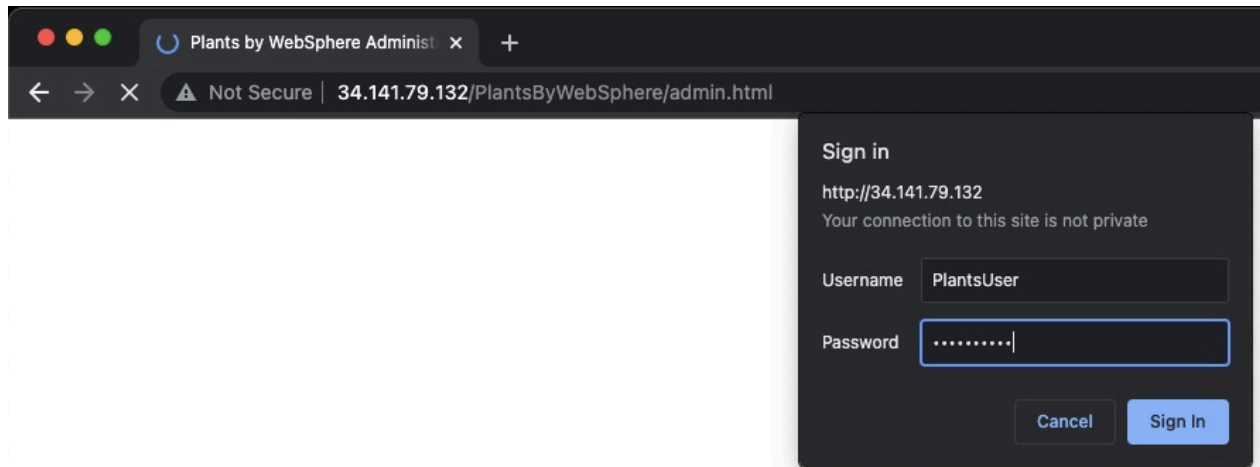
Map Users... Map Groups... Map Special Subjects ▾



Select	Role	Special subjects	Mapped users	Mapped groups
<input type="checkbox"/>	SampAdmin	None		PlantsGroup

OK Cancel







## BackOrder Administration

Refresh

<input type="checkbox"/>	BACK ORDER #	ITEM #	ITEM DESCRIPTION	QUANTITY TO ORDER	CURRENT INVENTORY QUANTITY	LOW INVENTORY DATE
--------------------------	--------------	--------	------------------	-------------------	----------------------------	--------------------

Order Stock      Cancel

<input type="checkbox"/>	BACK ORDER #	SUPPLIER ORDER #	ITEM #	ITEM DESCRIPTION	QUANTITY ORDERED	CURRENT INVENTORY QUANTITY	LOW INVENTORY DATE	ORDERED DATE
--------------------------	--------------	------------------	--------	------------------	------------------	----------------------------	--------------------	--------------

## Global security

## Global security

Use this panel to configure administration and the default application security policies for user applications.

[Security Configuration Wizard](#)
[Security Configuration Report](#)

## Administrative security



Enable administrative security

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

## Application security



Enable application security

## Nodes

## Messages

- ⚠ Synchronization operations are not valid for unmanaged node lhsnode.
- ℹ Successfully initiated synchronization of the repository on node wasnd-node01Node01 with the deployment manager's repository.
- ✖ The synchronize operation can not be performed on node wasnd-node01Node02 because its node agent is not active.
- ℹ Refresh the page to see the current synchronization status.

## Nodes

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

[Preferences](#)

Add Node

Remove Node

Force Delete

Synchronize

Full Resynchronize



Stop

Select	Name	Host Name	Version	Discovery Protocol	Status
You can administer the following resources:					
<input type="checkbox"/>	<a href="#">lhsnode</a>	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	Not applicable	TCP	
	<a href="#">wasnd-node01CellManager01</a>	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	
<input type="checkbox"/>	<a href="#">wasnd-node01Node01</a>	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	
<input type="checkbox"/>	<a href="#">wasnd-node01Node02</a>	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	

Total 4

## WebSphere application server clusters








## Messages

-  Cluster member server2 will not be started because the Node Agent on node wasnd-node01Node02 is not active. Cluster members can be started individually from the cluster member collection panel.
-  The ripple start operation on cluster PlantsCluster has been initiated. Each cluster member will be stopped and started in sequence. It may take several minutes for this operation to complete.

## WebSphere application server clusters

Use this page to change the configuration settings for a cluster. A server cluster consists of a group of application servers. If one of the member servers fails, requests will be routed to other members of the cluster. Learn more about this task in a [guided activity](#). A guided activity provides a list of task steps and more general information about the topic.

## Preferences

New... Delete Start Stop Ripplestart ImmediateStop		
   		
Select	Name 	Status 
You can administer the following resources:		
<input type="checkbox"/>	<a href="#">PlantsCluster</a>	
Total 1		