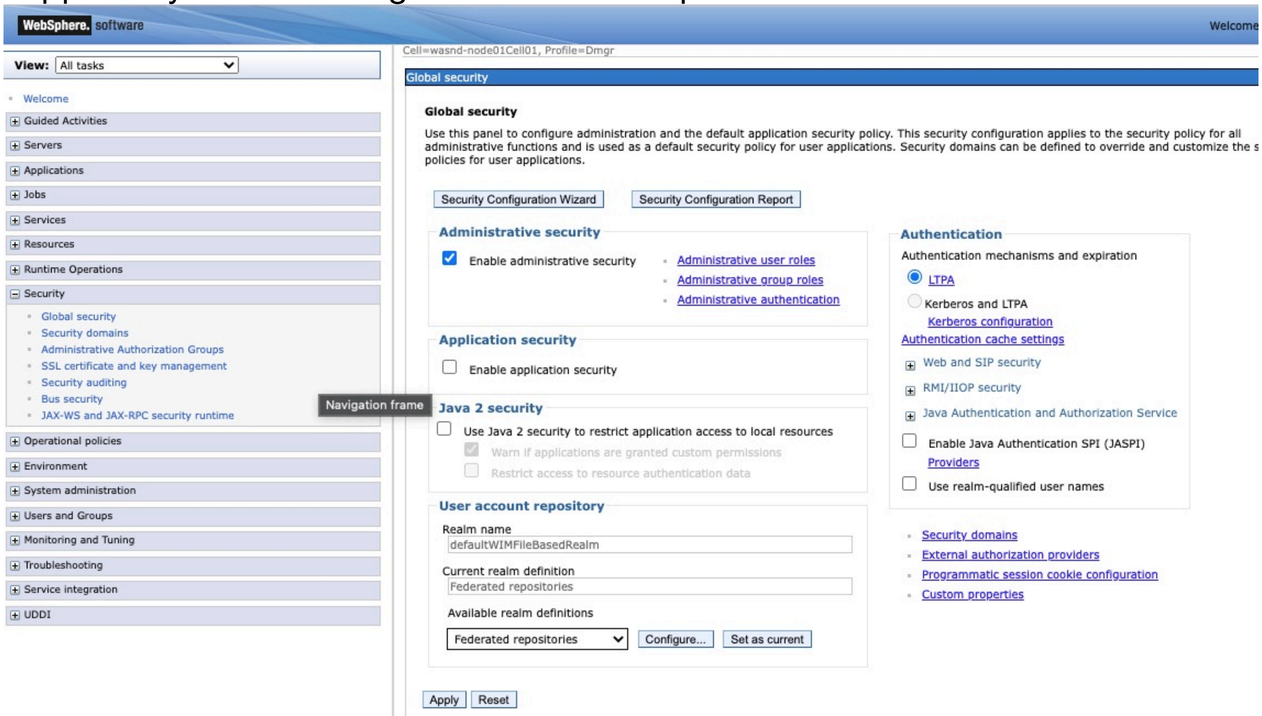
Exercise 12 – Configuring WebSphere Security

At the end of this exercise, you should be able to:
• Enable WebSphere security
• Configure administrative security by configuring access to administrative functions
• Configure fine-grained administrative security

Section 1: Verify administrative security

This exercise configures security access to the administrative tools. Before any security access takes effect, administrative security must be enabled, which happens by default during the creation of a profile.



Cell=wasnd-node01Cell01, Profile=Dmgr

Global security

Global security

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

Administrative security

☑ Enable administrative security

Application security

☐ Enable application security

Java 2 security

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

User account repository

Realm name: defaultWIMFileBasedRealm

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

Authentication

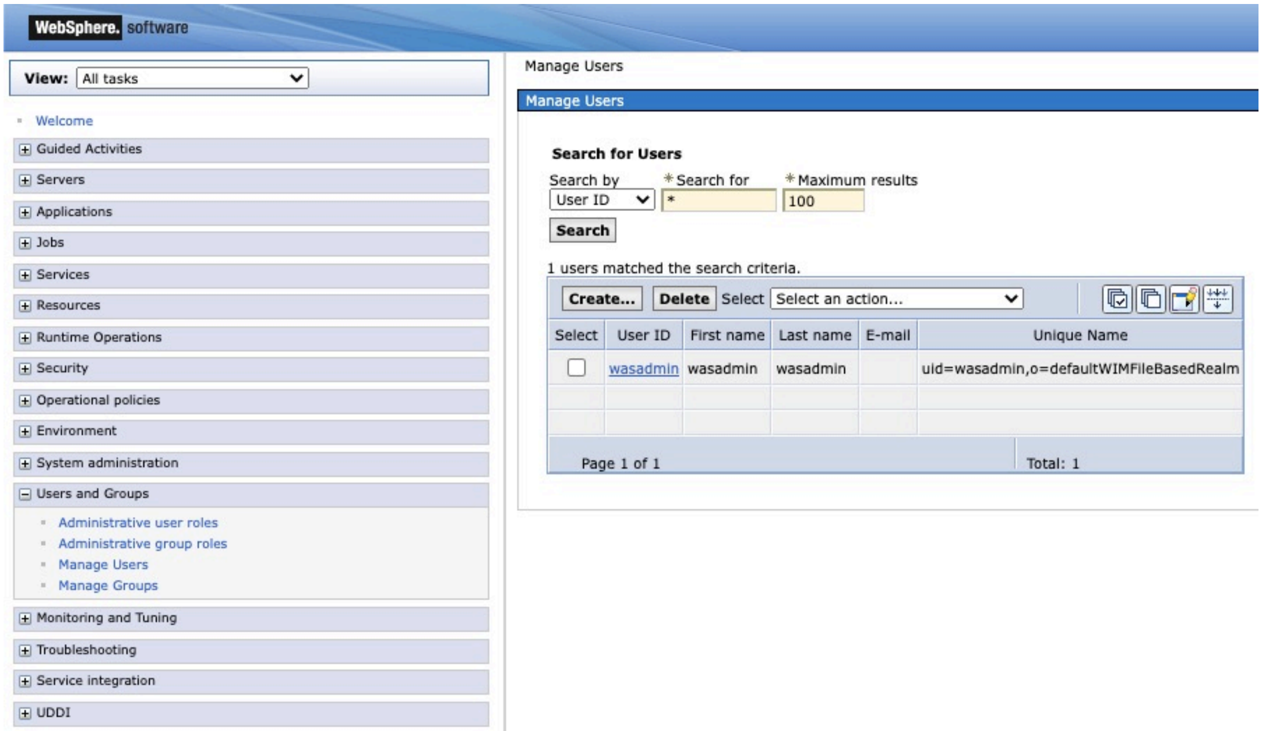
Authentication mechanisms and expiration
● LTPA
○ Kerberos and LTPA

☐ Enable Java Authentication SPI (JASPI)

☐ Use realm-qualified user names

Section 2: Defining WebSphere administrative console users

When WebSphere Application Server is installed and profiles are created, administrative security is enabled by default. Initially, the only user with access to the administrative console is the primary user that is specified during the profile creation, which is the wasadmin user. Initially, in the case of these labs, the only user that can access the administrative console is wasadmin. In a real environment, it is desirable to have multiple administrative users and possibly have different rights for each user.



Manage Users

Manage Users

Search for Users

Search by: User ID

* Search for: *

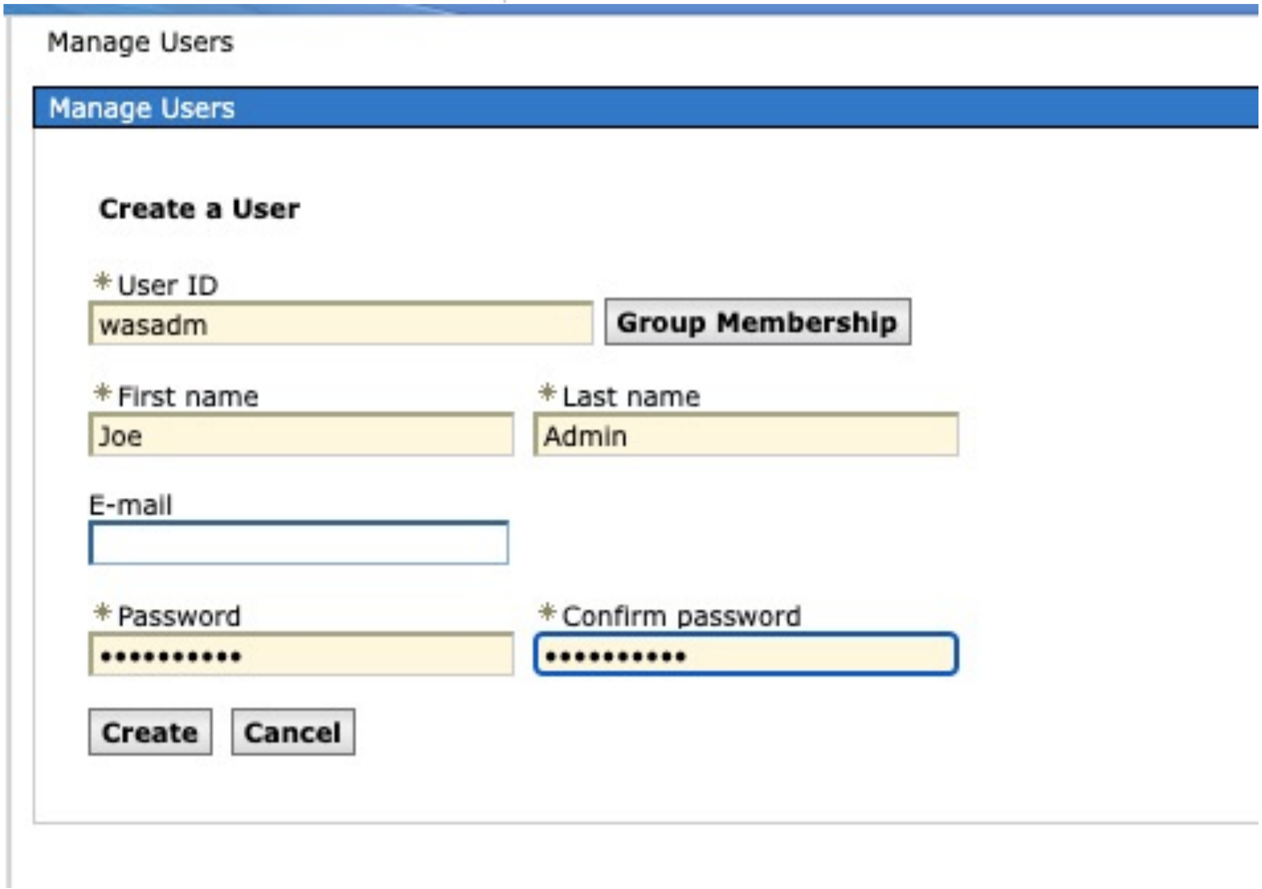
* Maximum results: 100

Search

1 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
□	wasadmin	wasadmin	wasadmin		uid=wasadmin,o=defaultWIMFileBasedRealm

Page 1 of 1 Total: 1



Manage Users

Manage Users

Create a User

* User ID: wasadm

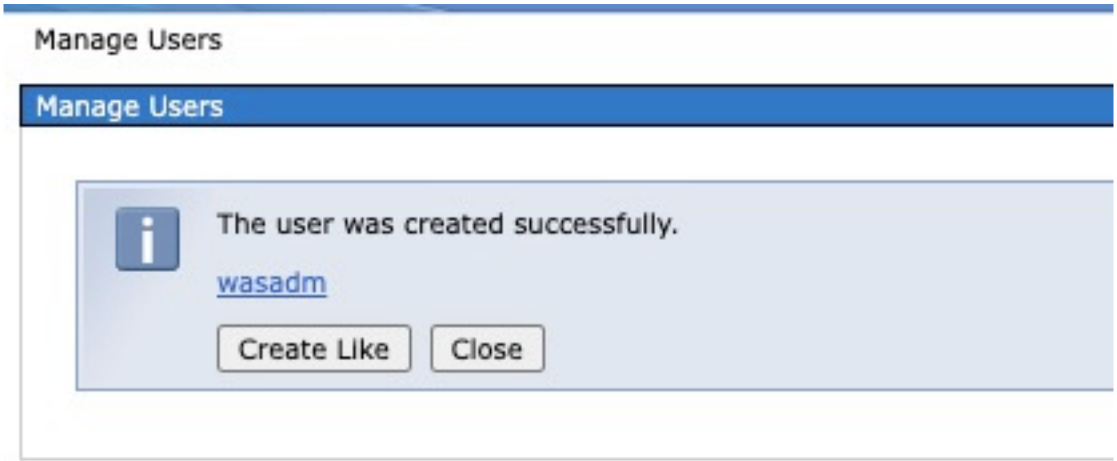
* First name: Joe

* Last name: Admin

E-mail:

* Password: ••••••••••

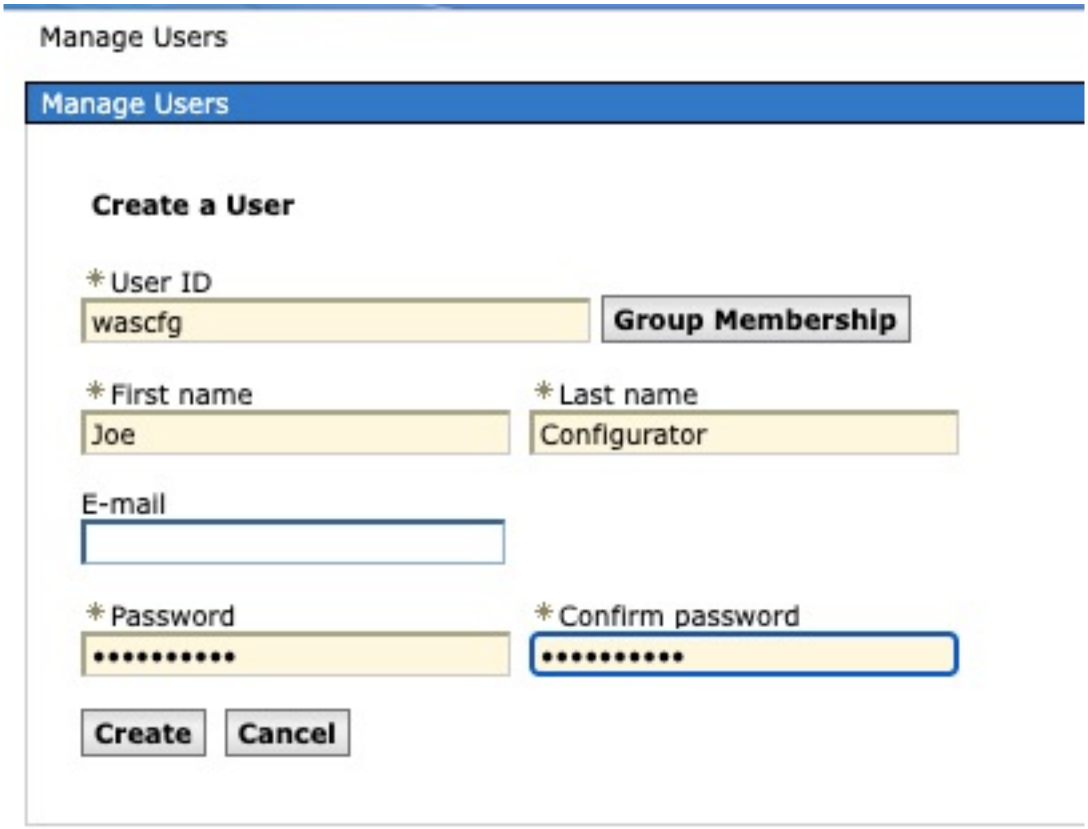
* Confirm password: ••••••••••


Manage Users

Manage Users

The user was created successfully.

wasadm


Manage Users

Manage Users

Create a User

*User ID: wascfg

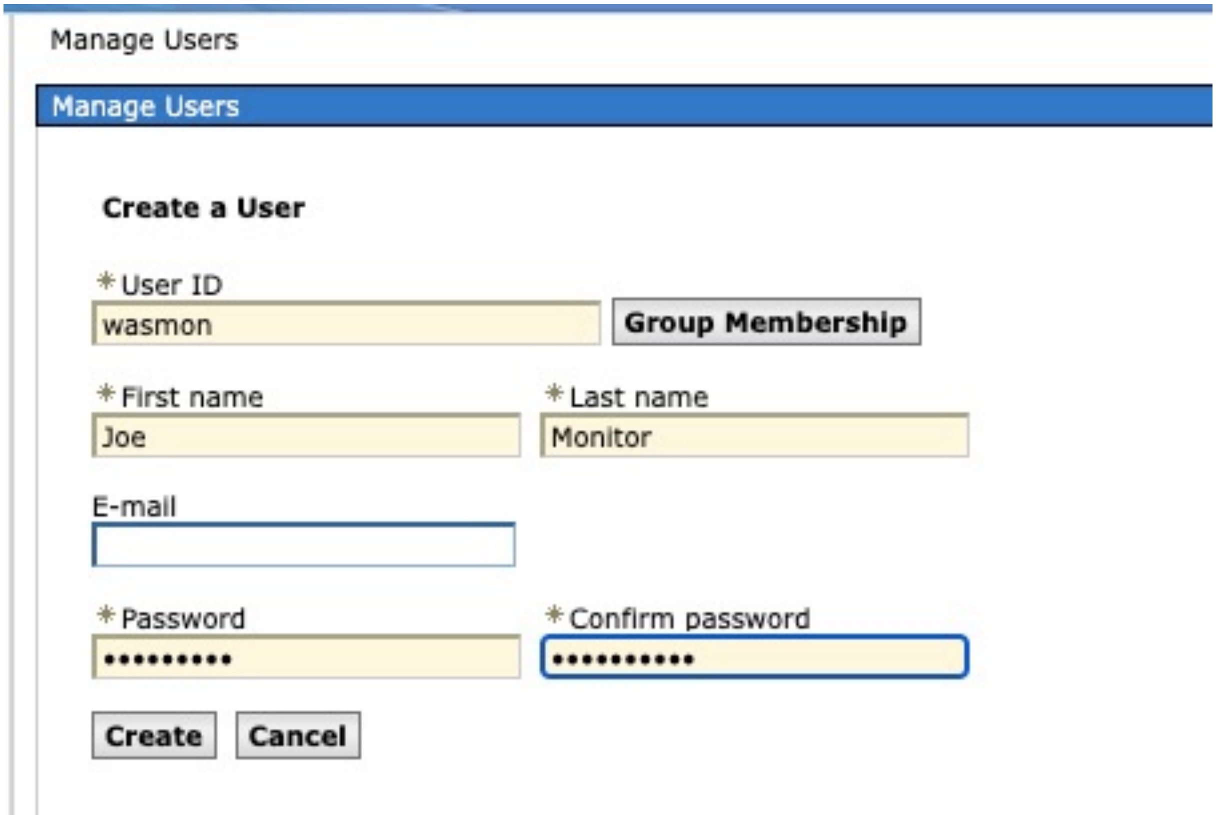
*First name: Joe

*Last name: Configurator

E-mail:

*Password: •••••••••••

*Confirm password: •••••••••••



Manage Users

Manage Users

Create a User

* User ID: wasmon

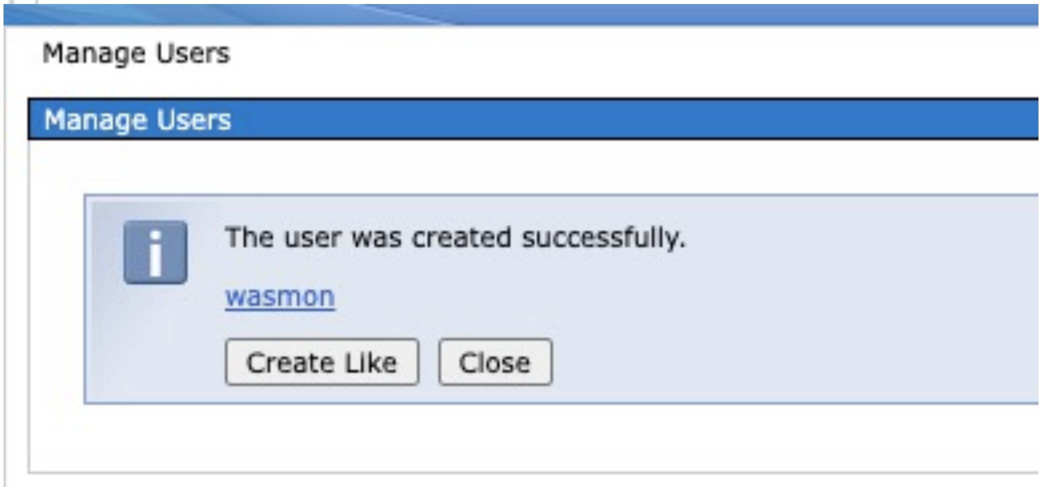
* First name: Joe

* Last name: Monitor

E-mail:

* Password: ●●●●●●●●●●

* Confirm password: ●●●●●●●●●●●

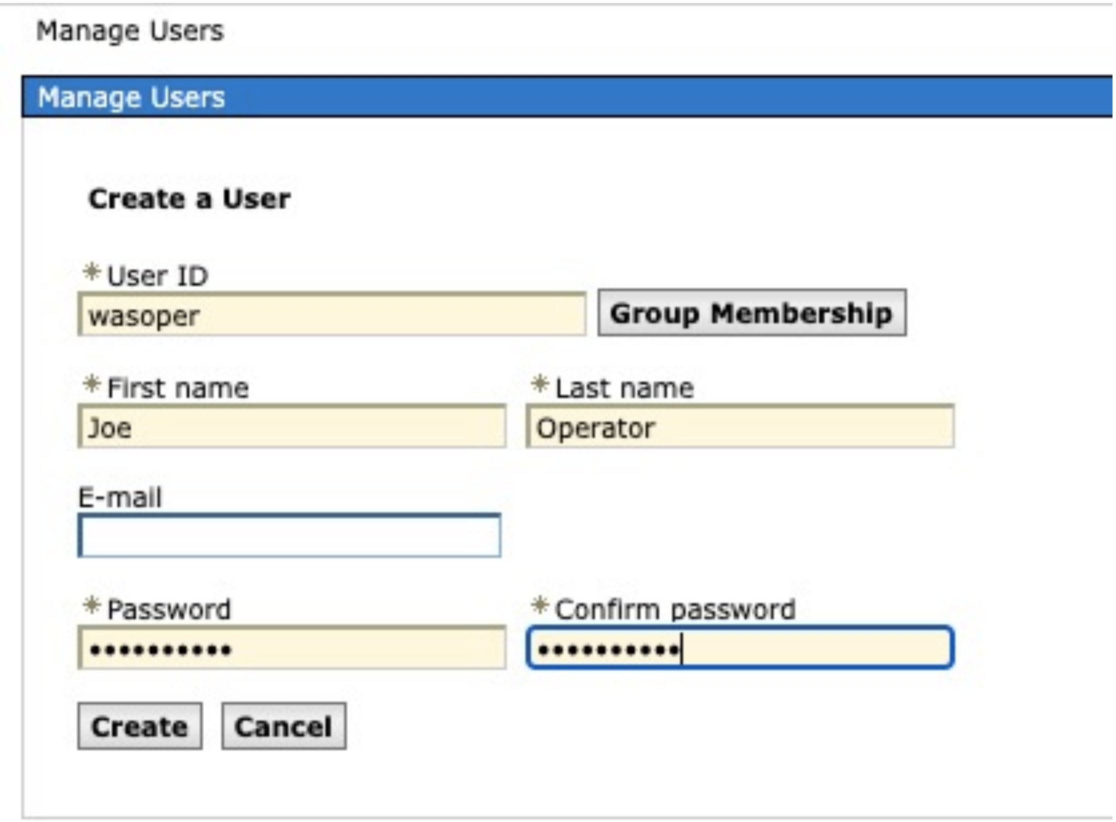


Manage Users

Manage Users

The user was created successfully.

wasmon

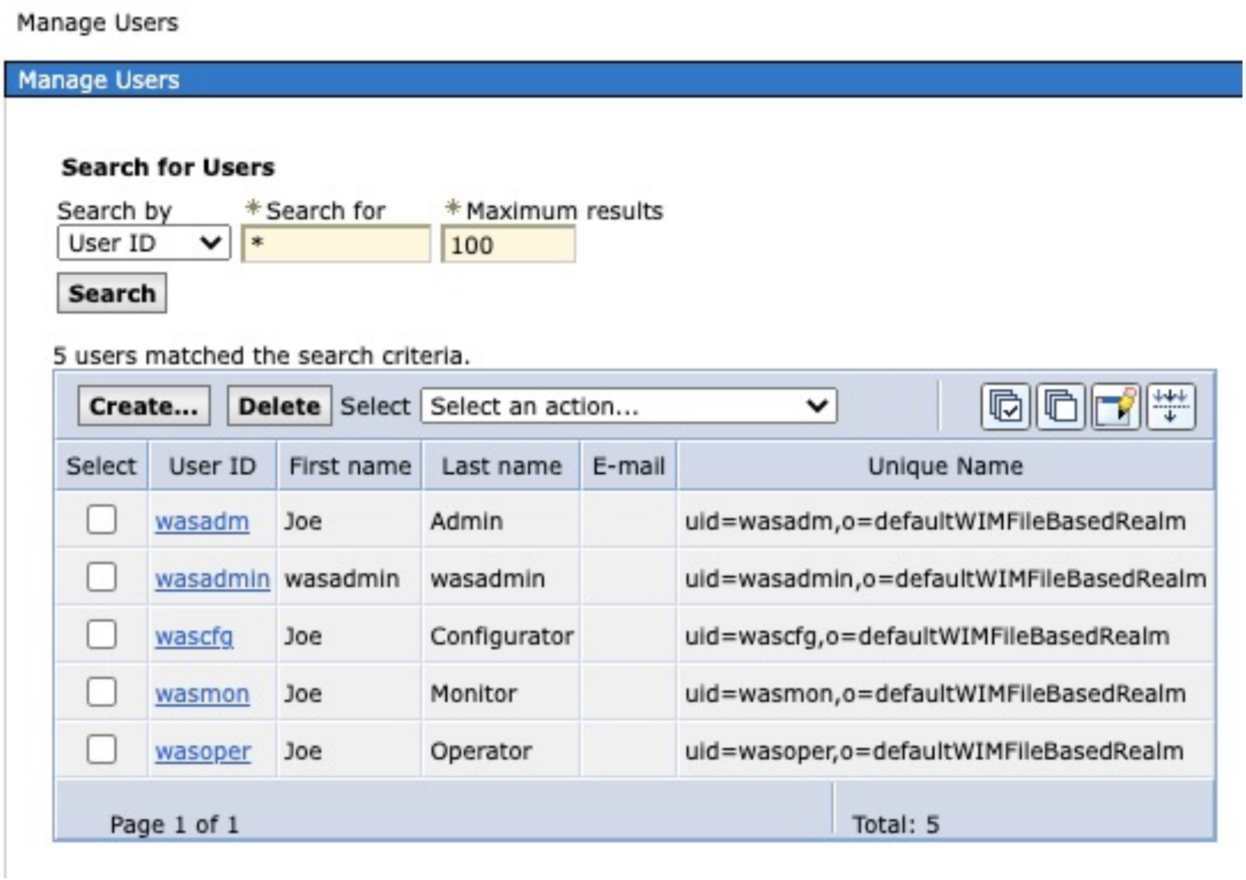


Manage Users

Manage Users

Create a User

* User ID	wasoper
* First name	Joe
* Last name	Operator
E-mail	
* Password	•••••••••••
* Confirm password	•••••••••••



Manage Users

Manage Users

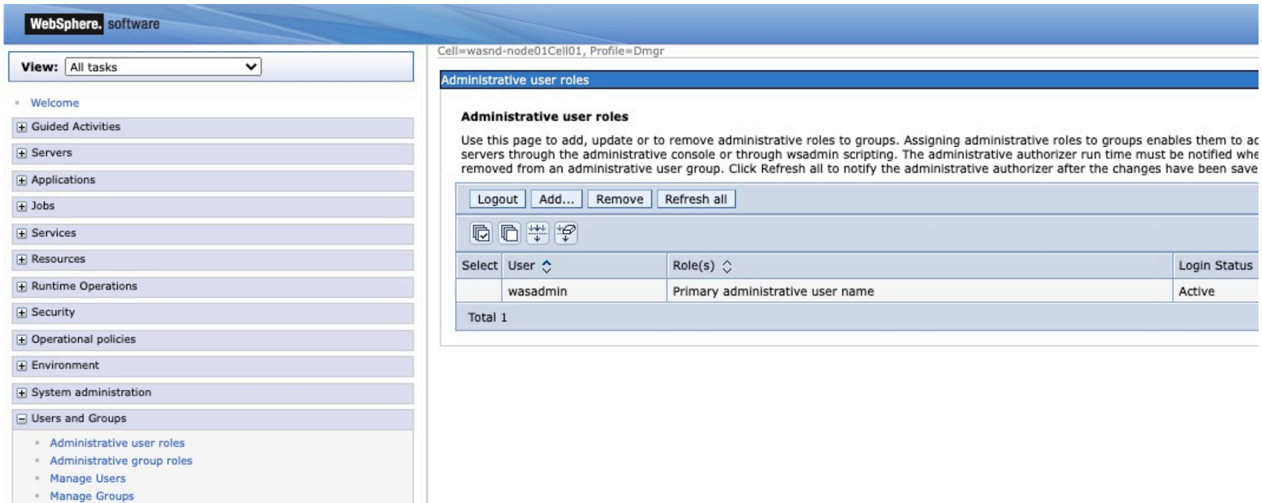
Search for Users

Search by	User ID
* Search for	*
* Maximum results	100

5 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
□	wasadm	Joe	Admin		uid=wasadm,o=defaultWIMFileBasedRealm
□	wasadmin	wasadmin	wasadmin		uid=wasadmin,o=defaultWIMFileBasedRealm
□	wascfg	Joe	Configurator		uid=wascfg,o=defaultWIMFileBasedRealm
□	wasmon	Joe	Monitor		uid=wasmon,o=defaultWIMFileBasedRealm
□	wasoper	Joe	Operator		uid=wasoper,o=defaultWIMFileBasedRealm

Page 1 of 1   Total: 5



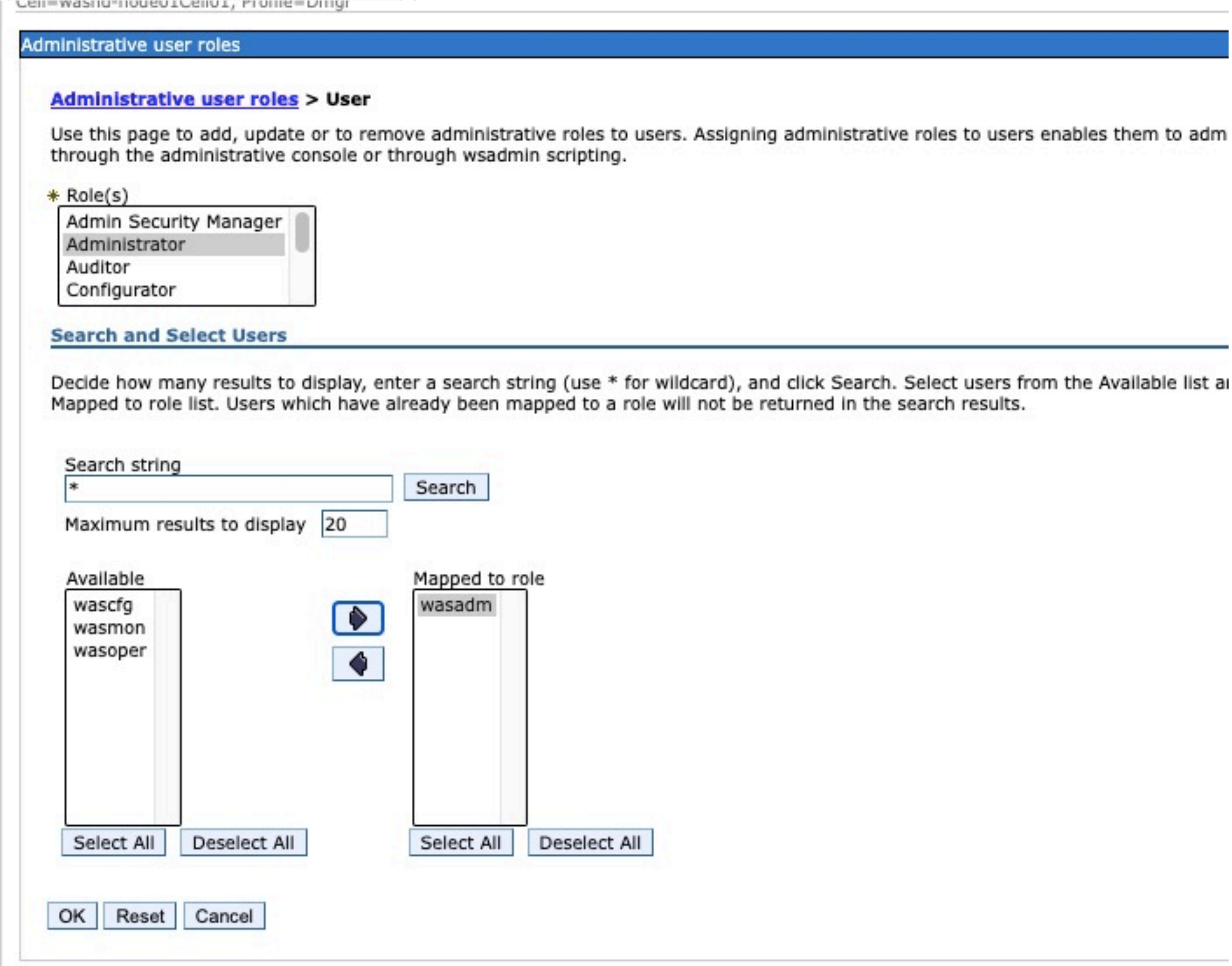
Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative user roles

Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to ac servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified whe removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been save

Select	User	Role(s)	Login Status
	wasadmin	Primary administrative user name	Active
Total 1			



Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative user roles

Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to adm through the administrative console or through wsadmin scripting.

* Role(s)

Search and Select Users

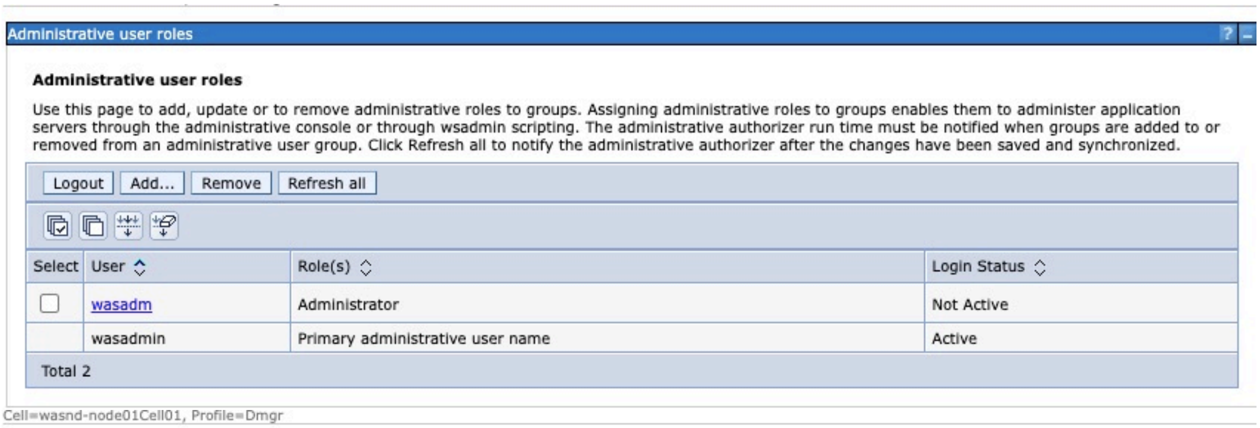
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list ai Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: *

Maximum results to display: 20

Available: wascfg, wasmon, wasoper

Mapped to role: wasadm

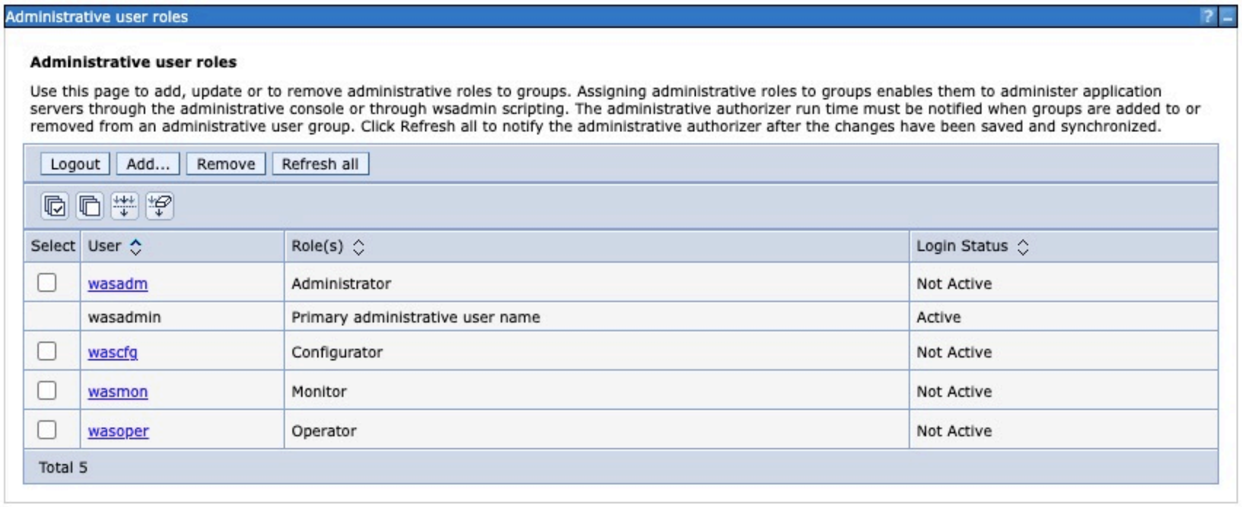


Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Select	User	Role(s)	Login Status
☐	wasadm	Administrator	Not Active
	wasadmin	Primary administrative user name	Active
Total 2			

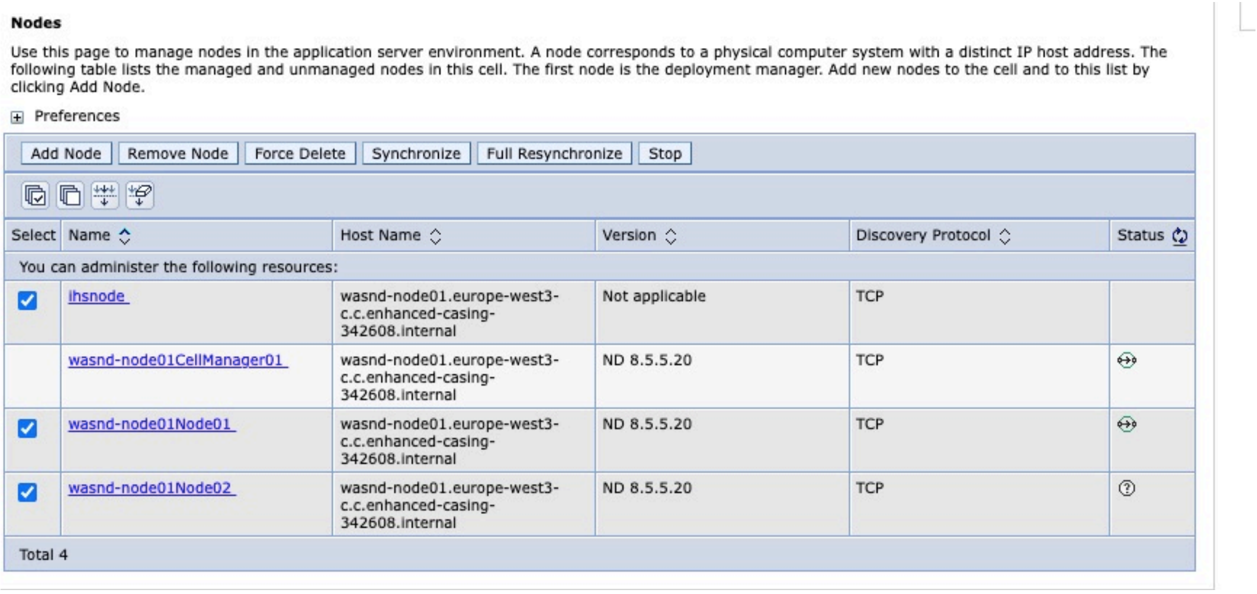
Cell=wasnd-node01Cell01, Profile=Dmgr



Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

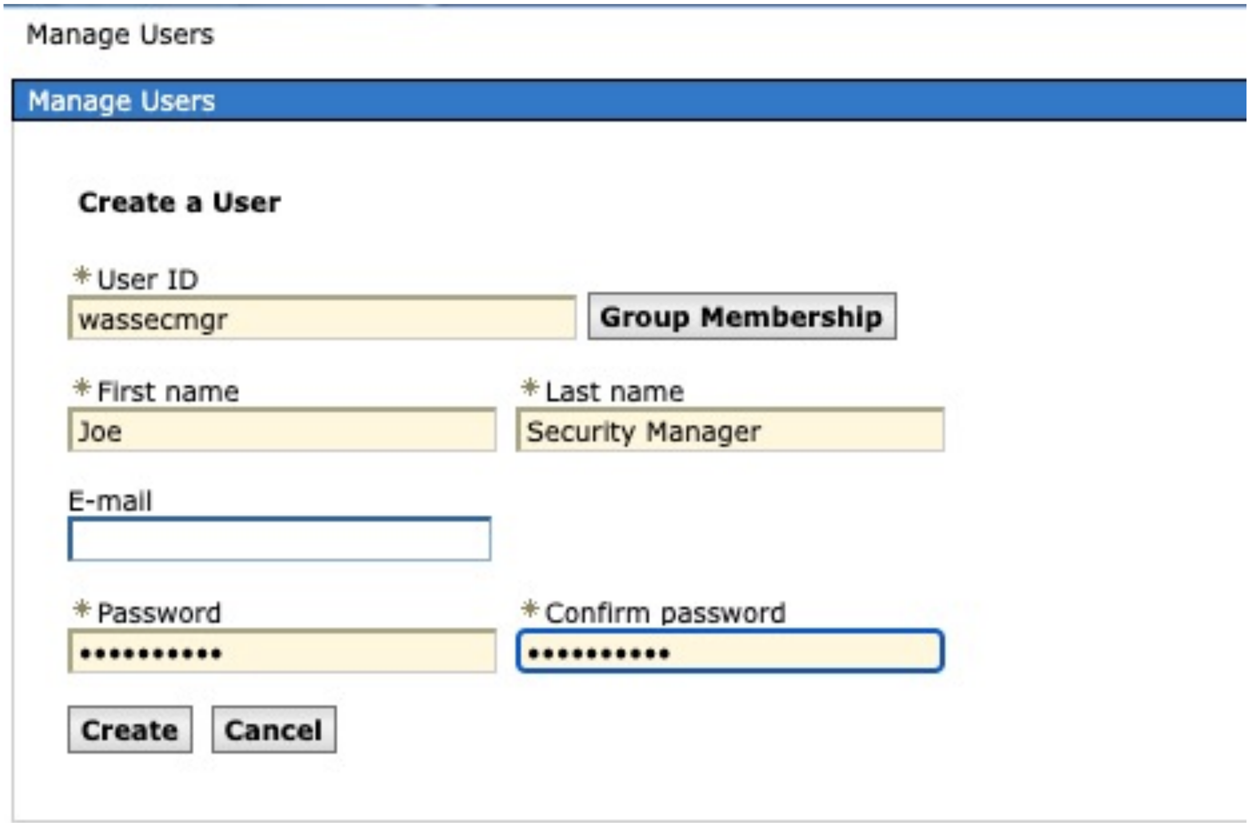
Select	User	Role(s)	Login Status
☐	wasadm	Administrator	Not Active
	wasadmin	Primary administrative user name	Active
☐	wascfg	Configurator	Not Active
☐	wasmon	Monitor	Not Active
☐	wasoper	Operator	Not Active
Total 5			



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.

Select	Name	Host Name	Version	Discovery Protocol	Status
You can administer the following resources:					
☑	ihsnode	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	Not applicable	TCP	
	wasnd-node01CellManager01	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	↔
☑	wasnd-node01Node01	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	↔
☑	wasnd-node01Node02	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	TCP	?
Total 4					



Manage Users

Manage Users

Create a User

* User ID: wassecmgr

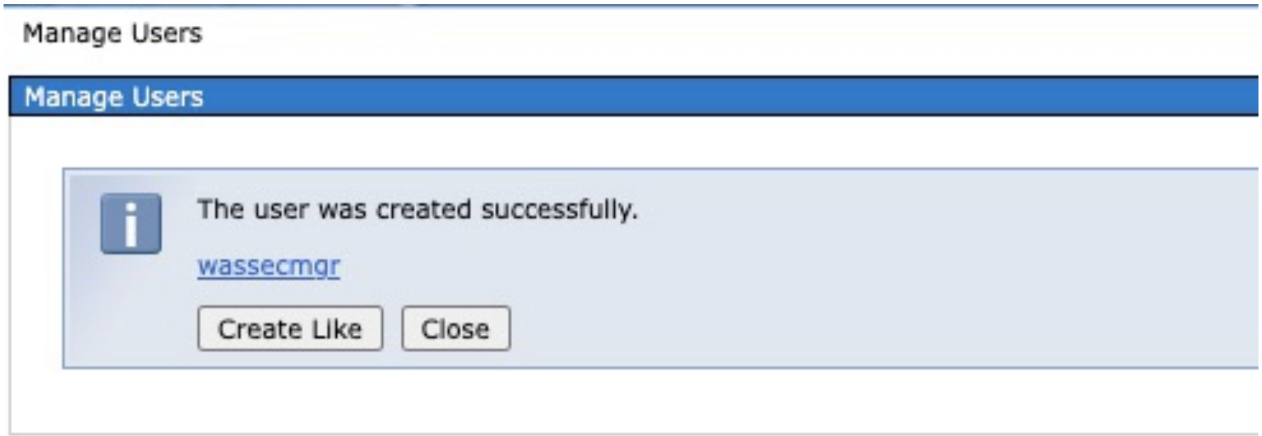
* First name: Joe

* Last name: Security Manager

E-mail:

* Password: •••••••••••

* Confirm password: •••••••••••

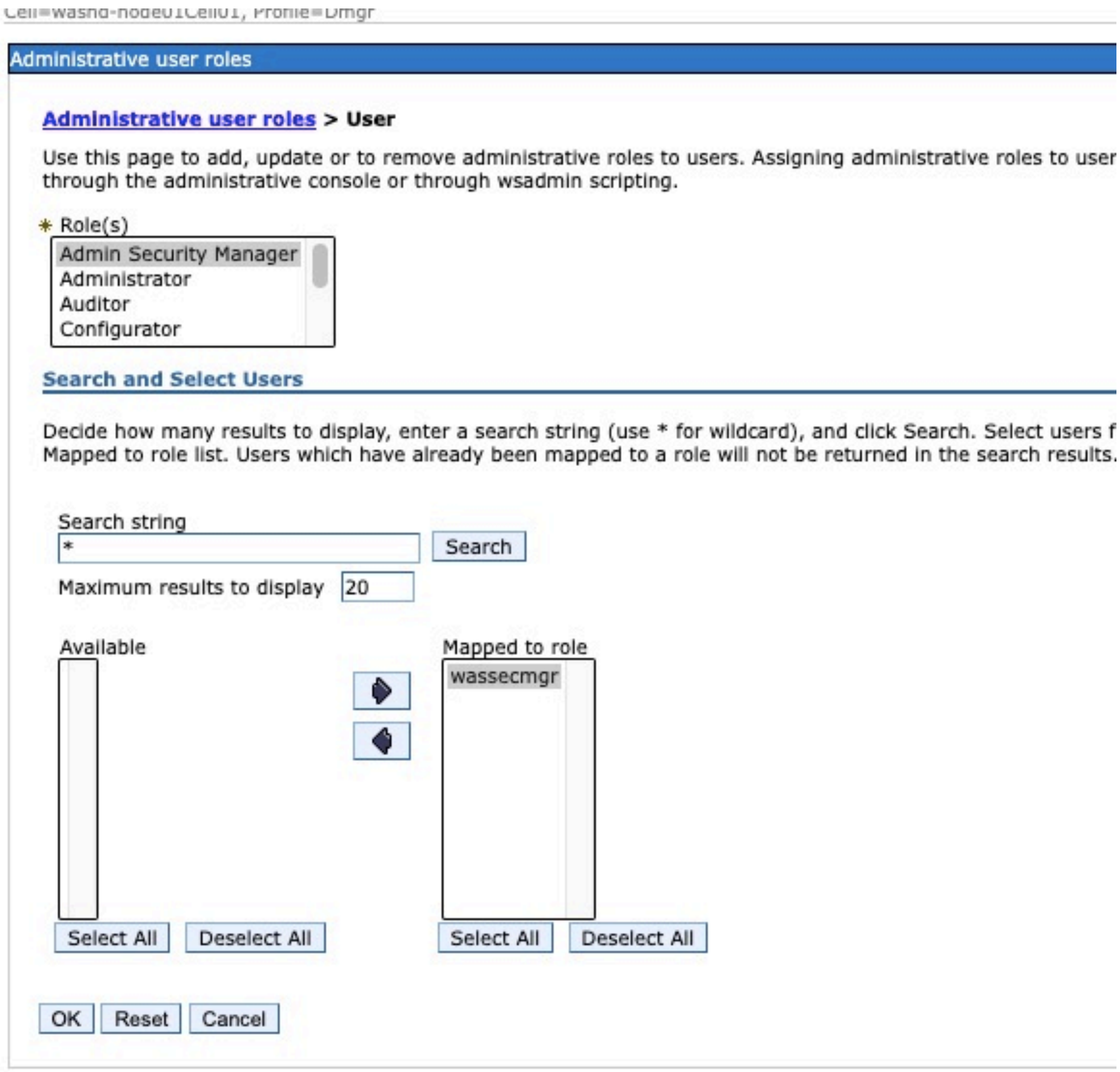


Manage Users

Manage Users

The user was created successfully.

wassecmgr



Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative user roles

Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to user through the administrative console or through wsadmin scripting.

* Role(s)

- Admin Security Manager
- Administrator
- Auditor
- Configurator

Search and Select Users

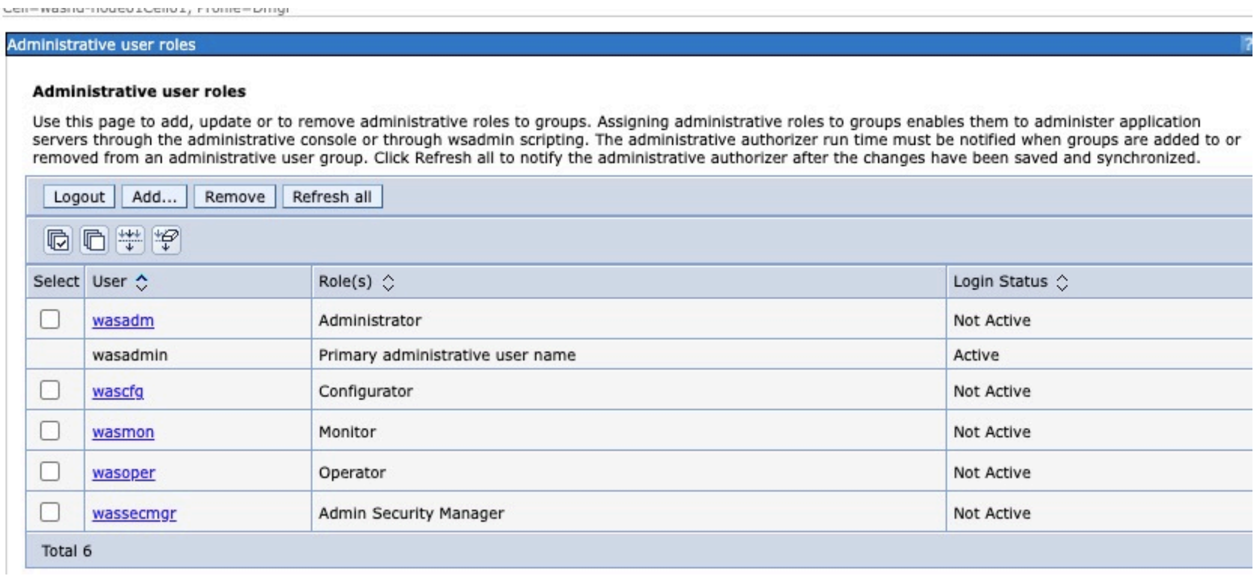
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users f Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: *

Maximum results to display: 20

Available:

Mapped to role: wassecmgr


Cell=wasnd-node01Cell01, Profile=Dmgr
Administrative user roles
Logout
Add...
Remove
Refresh all

Administrative user roles

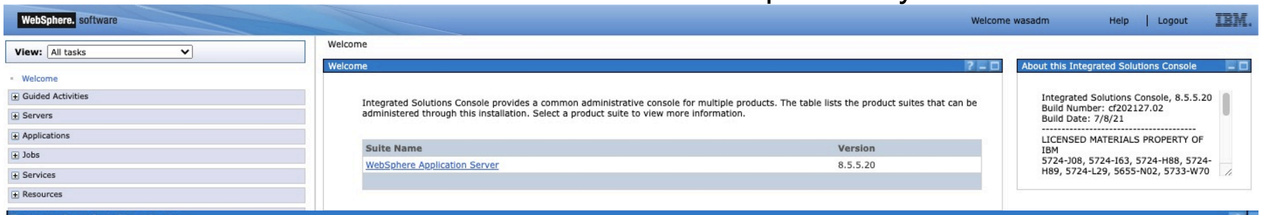
Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Select	User	Role(s)	Login Status
□	wasadm	Administrator	Not Active
	wasadmin	Primary administrative user name	Active
□	wascfg	Configurator	Not Active
□	wasmon	Monitor	Not Active
□	wasoper	Operator	Not Active
□	wassecmgr	Admin Security Manager	Not Active

Total 6

Section 3: Authenticate to the WebSphere administrative console and test mapped users

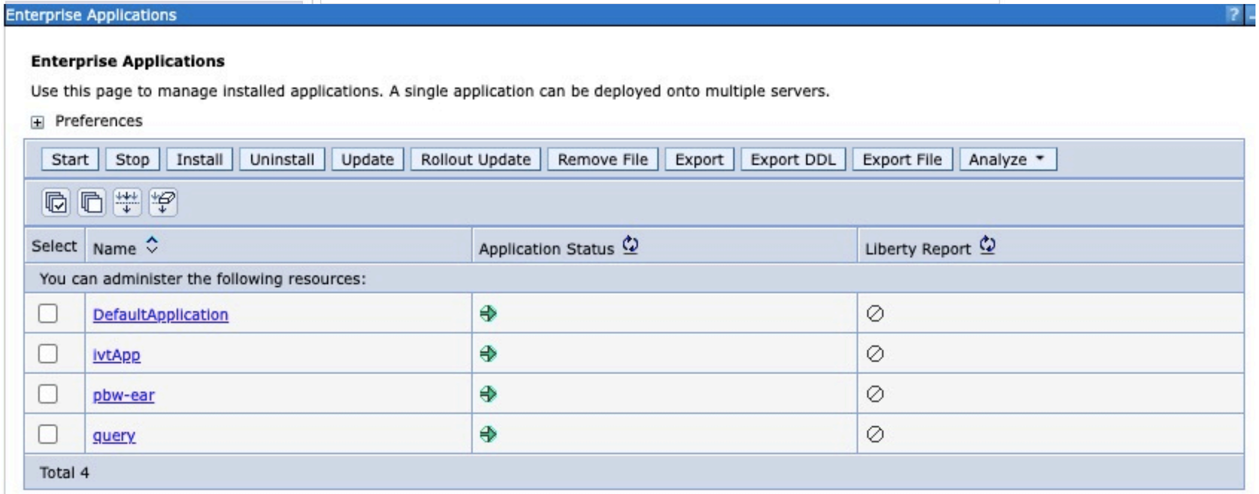
In this part of the exercise, access to the administrative console is granted only to correctly mapped users. Depending on the role to which they are mapped, the administrative console allows those users to complete only certain functions.



Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.20

Integrated Solutions Console, 8.5.5.20
Build Number: cf202127.02
Build Date: 7/8/21
LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89, 5724-L29, 5655-N02, 5733-W70

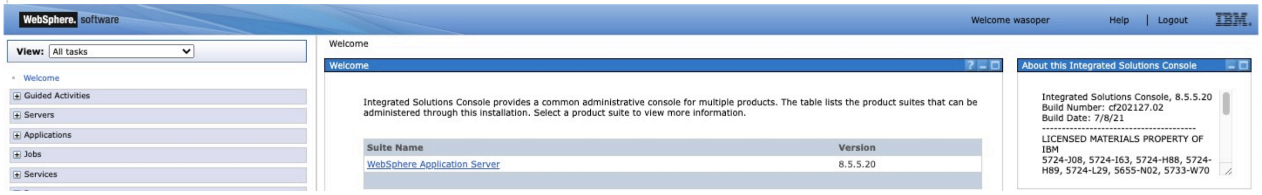


Enterprise Applications

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

Select	Name	Application Status	Liberty Report
You can administer the following resources:			
□	DefaultApplication	➔	⊘
□	ivtApp	➔	⊘
□	pbw-ear	➔	⊘
□	query	➔	⊘

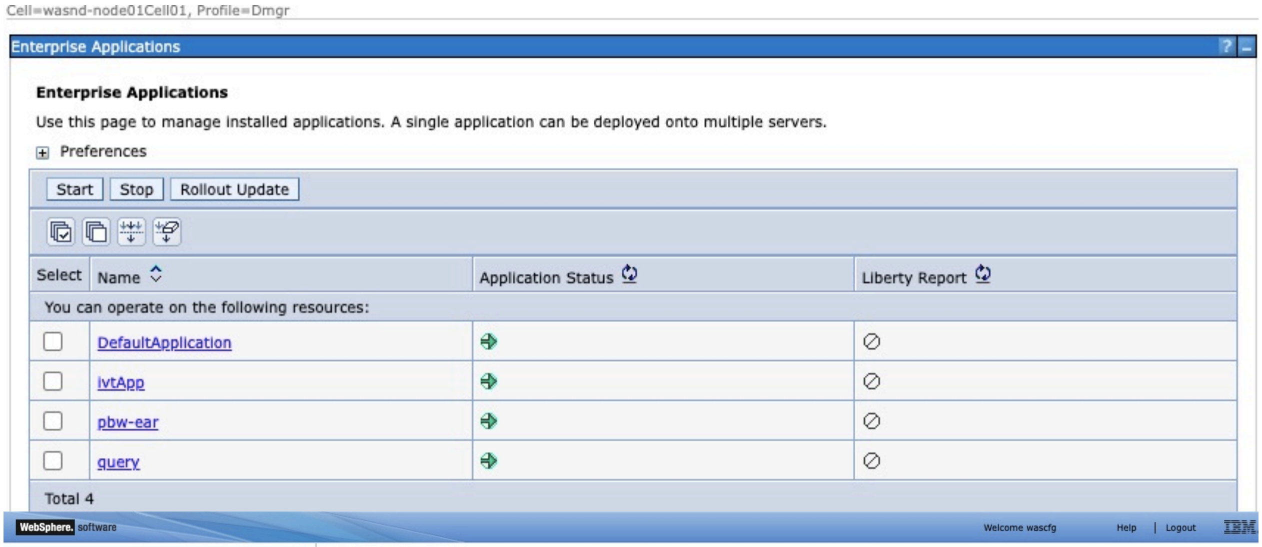
Total 4



Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.20

Integrated Solutions Console, 8.5.5.20
Build Number: cf202127.02
Build Date: 7/8/21
LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89, 5724-L29, 5655-N02, 5733-W70



Cell=wasnd-node01Cell01, Profile=Dmgr

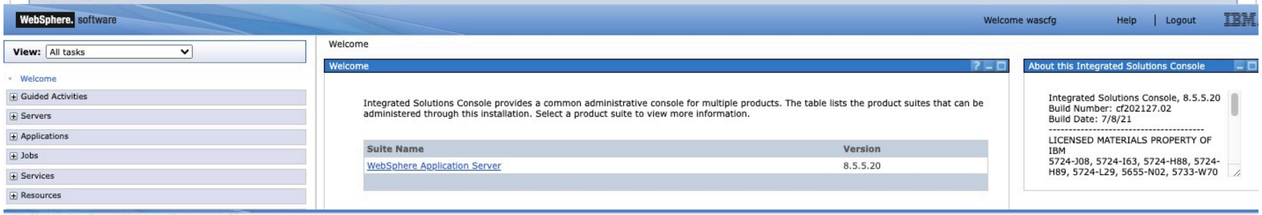
Enterprise Applications

Enterprise Applications

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

⊞ Preferences

Select	Name	Application Status	Liberty Report
You can operate on the following resources:			
□	DefaultApplication	➜	⊘
□	ivtApp	➜	⊘
□	pbw-ear	➜	⊘
□	query	➜	⊘
Total 4			



Welcome

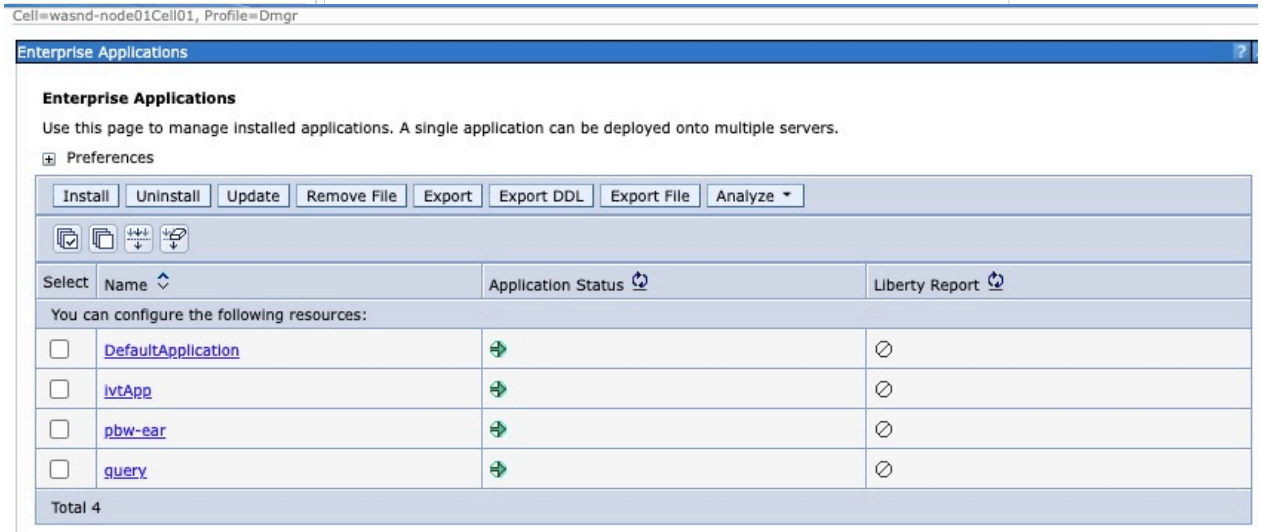
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.20

About this Integrated Solutions Console

Integrated Solutions Console, 8.5.5.20
Build Number: cf202127.02
Build Date: 7/8/21

LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89, 5724-L29, 5655-N02, 5733-W70



Cell=wasnd-node01Cell01, Profile=Dmgr

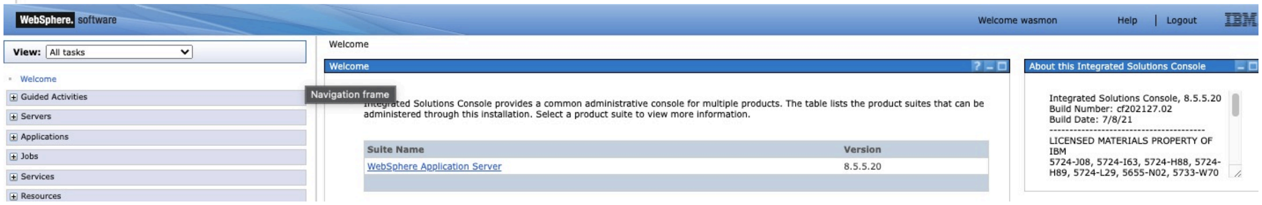
Enterprise Applications

Enterprise Applications

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

⊞ Preferences

Select	Name	Application Status	Liberty Report
You can configure the following resources:			
□	DefaultApplication	➜	⊘
□	ivtApp	➜	⊘
□	pbw-ear	➜	⊘
□	query	➜	⊘
Total 4			



Welcome

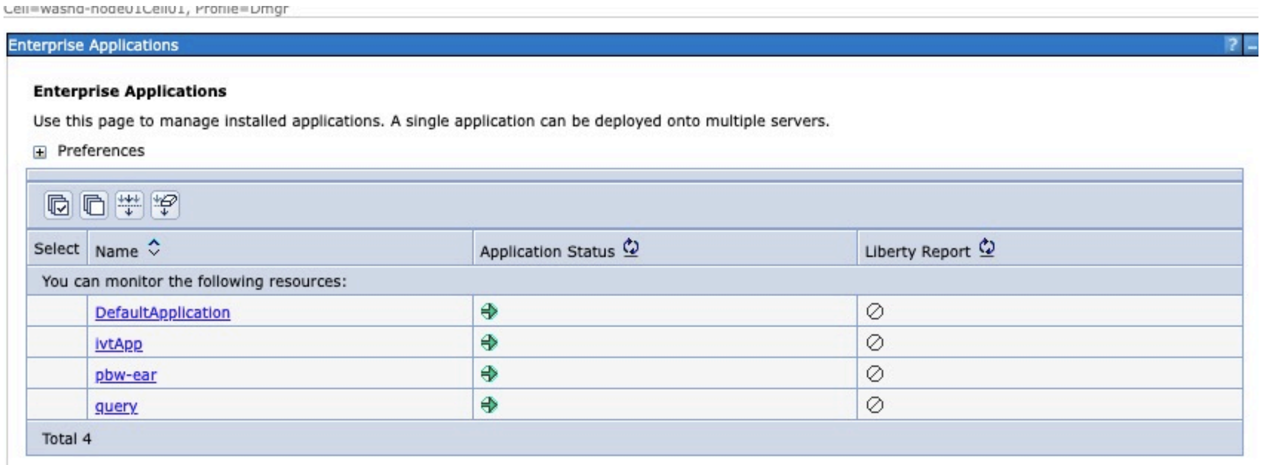
Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.20

About this Integrated Solutions Console

Integrated Solutions Console, 8.5.5.20
Build Number: cf202127.02
Build Date: 7/8/21

LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89, 5724-L29, 5655-N02, 5733-W70



Cell=wasnd-node01Cell01, Profile=Dmgr

Enterprise Applications

Enterprise Applications

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

⊞ Preferences

Select	Name	Application Status	Liberty Report
You can monitor the following resources:			
	DefaultApplication	➔	⊘
	ivtApp	➔	⊘
	pbw-ear	➔	⊘
	query	➔	⊘
Total 4			

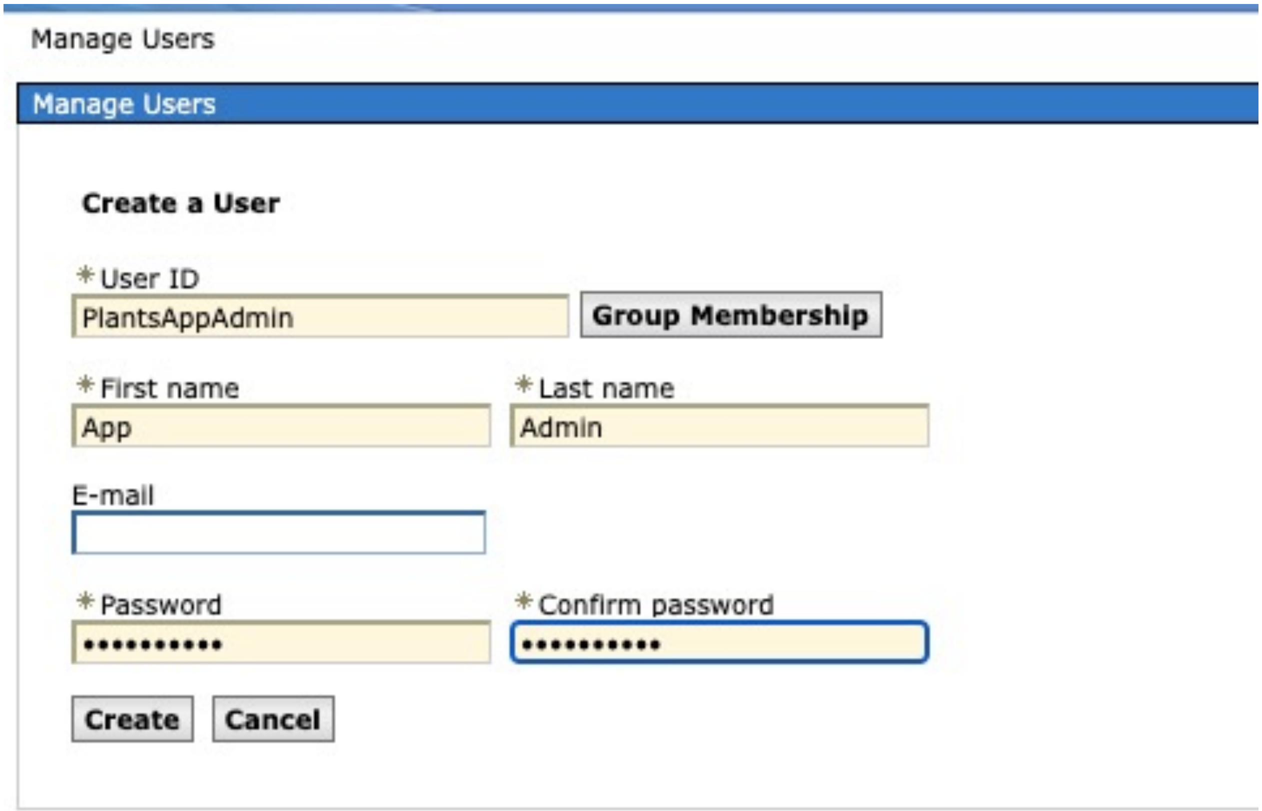
Section 4: Enabling fine-grained control

Now that users with different types of access to the administrative console exist, it might be interesting to control the access more specifically. For example, in the following example the exercise creates two new administrative users. The first, PlantsAppAdmin, is configured to have rights only on the PlantsByWebSphere application. The second, DefaultAppAdmin, is configured to have rights only on the DefaultApplication.

By creating this setup, the exercise demonstrates how fine-grained access controls can be granted to administrative users. These types of controls can be granted on many different types of objects, not just applications.

The fine-grained access is defined by mapping administrative authorization groups to administrative console users. The administrative authorization groups point at specific scopes or objects. When an administrative user attempts to access an object and does not have global access, the access that the administrative authorization groups define for the object is checked.

The user with fine-grained administrative access requires a minimum of global Monitor access.



Manage Users

Manage Users

Create a User

*User ID: PlantsAppAdmin

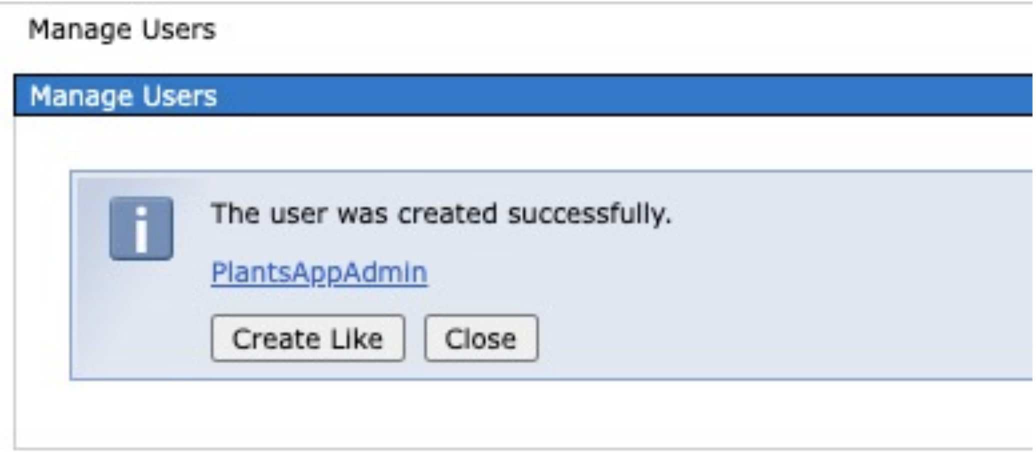
*First name: App

*Last name: Admin

E-mail:

*Password: •••••••••••

*Confirm password: •••••••••••

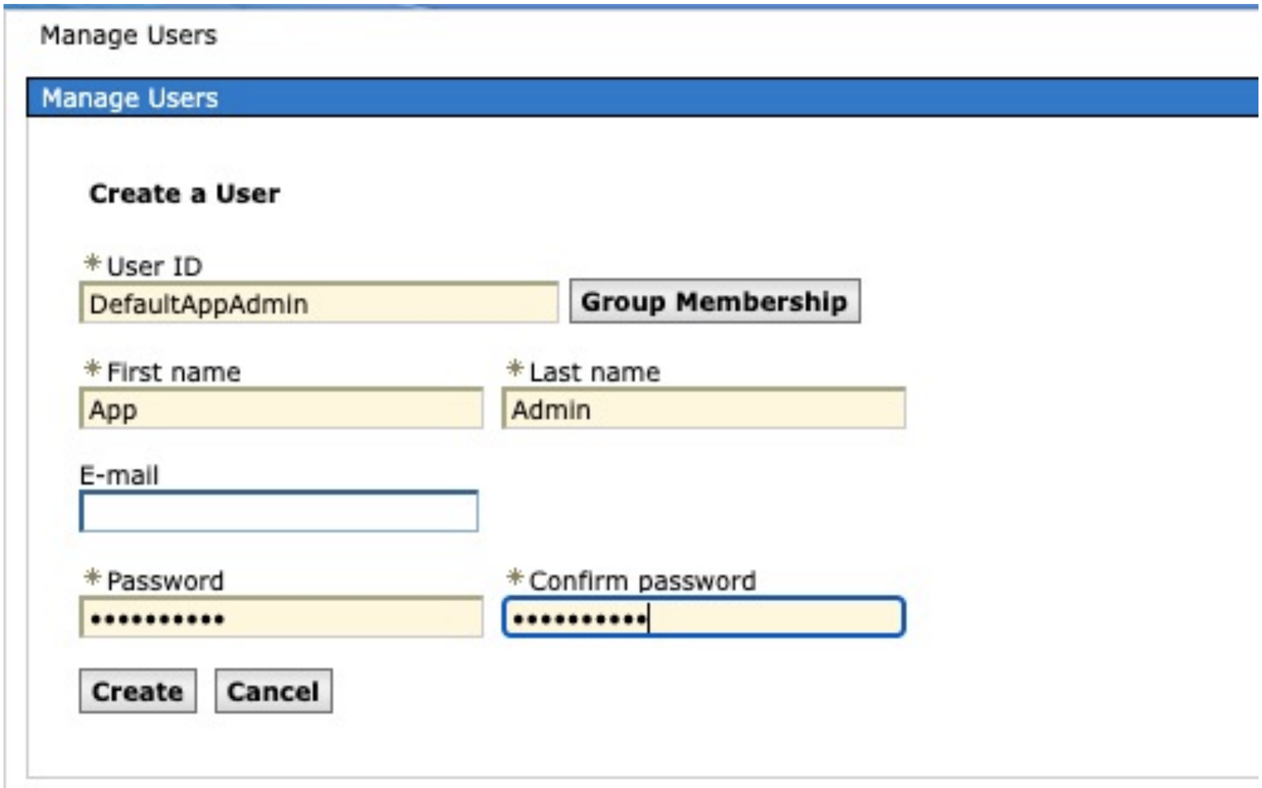


Manage Users

Manage Users

The user was created successfully.

PlantsAppAdmin



Manage Users

Manage Users

Create a User

* User ID: DefaultAppAdmin

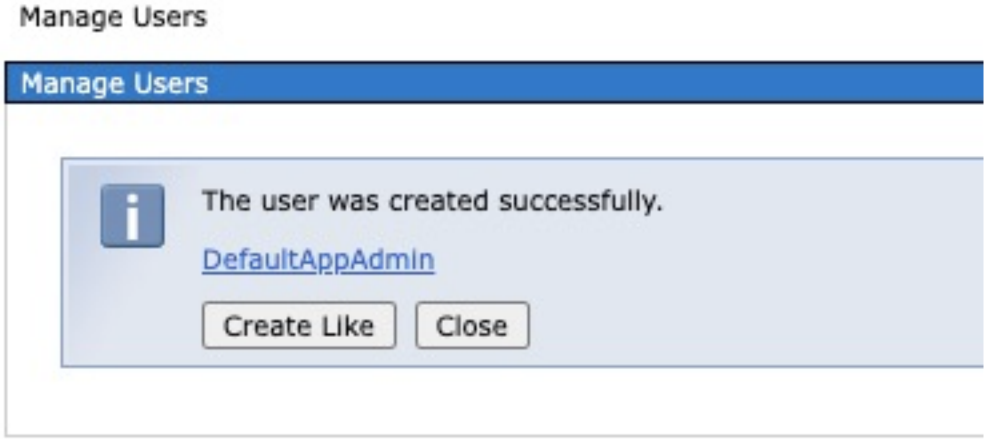
* First name: App

* Last name: Admin

E-mail:

* Password: •••••••••••

* Confirm password: •••••••••••

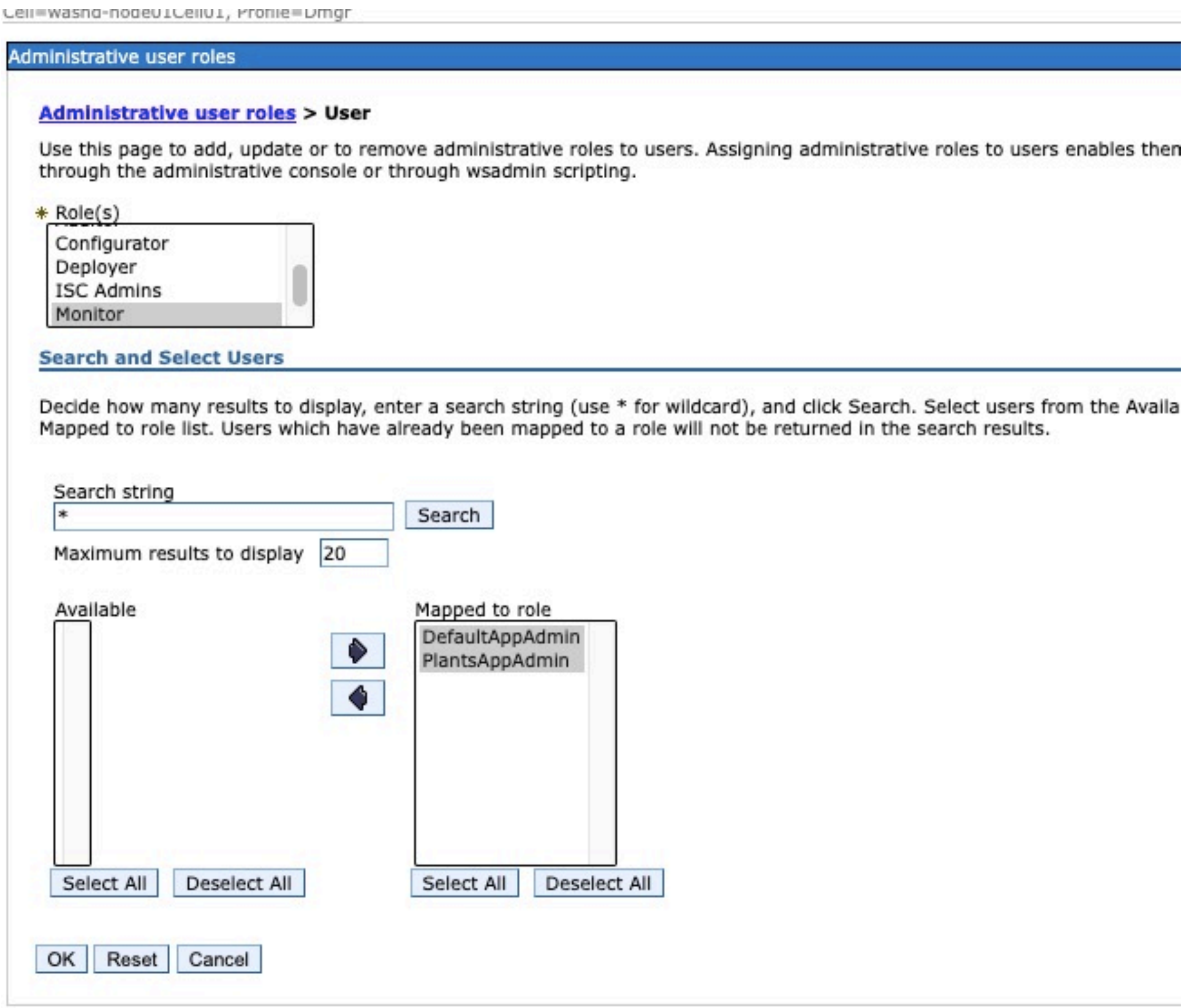


Manage Users

Manage Users

The user was created successfully.

DefaultAppAdmin


Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative user roles

Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables then
through the administrative console or through wsadmin scripting.

* Role(s)

- Configurator
- Deployer
- ISC Admins
- Monitor

Search and Select Users

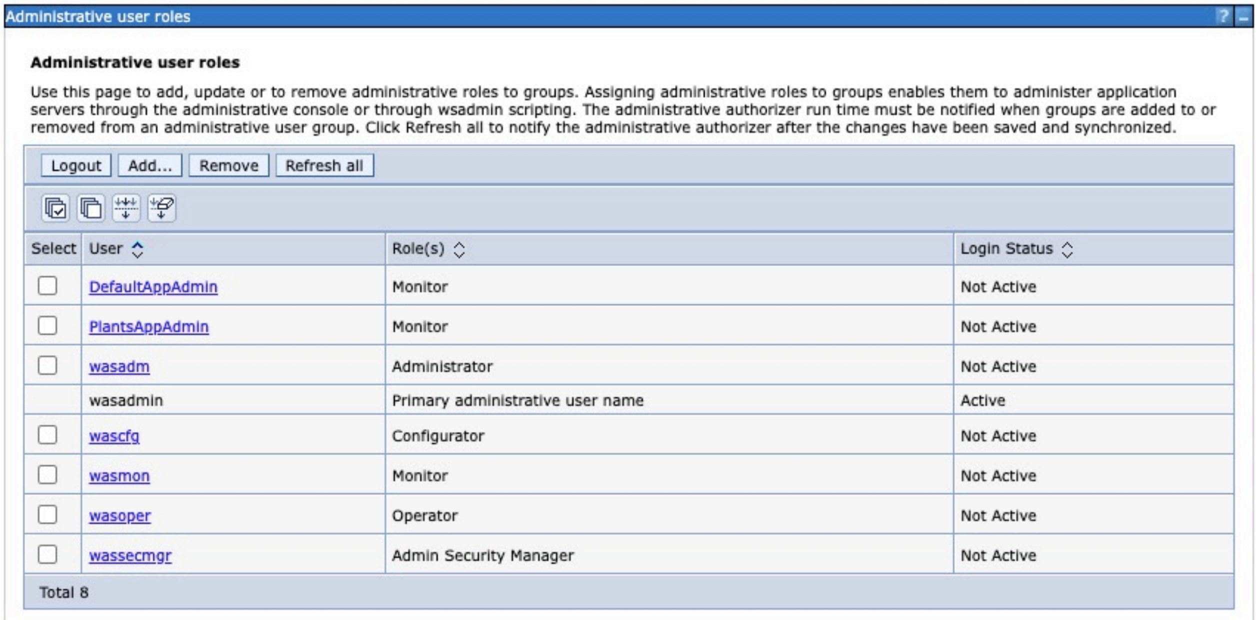
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Availa
Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: *

Maximum results to display: 20

Available:

Mapped to role:
- DefaultAppAdmin
- PlantsAppAdmin

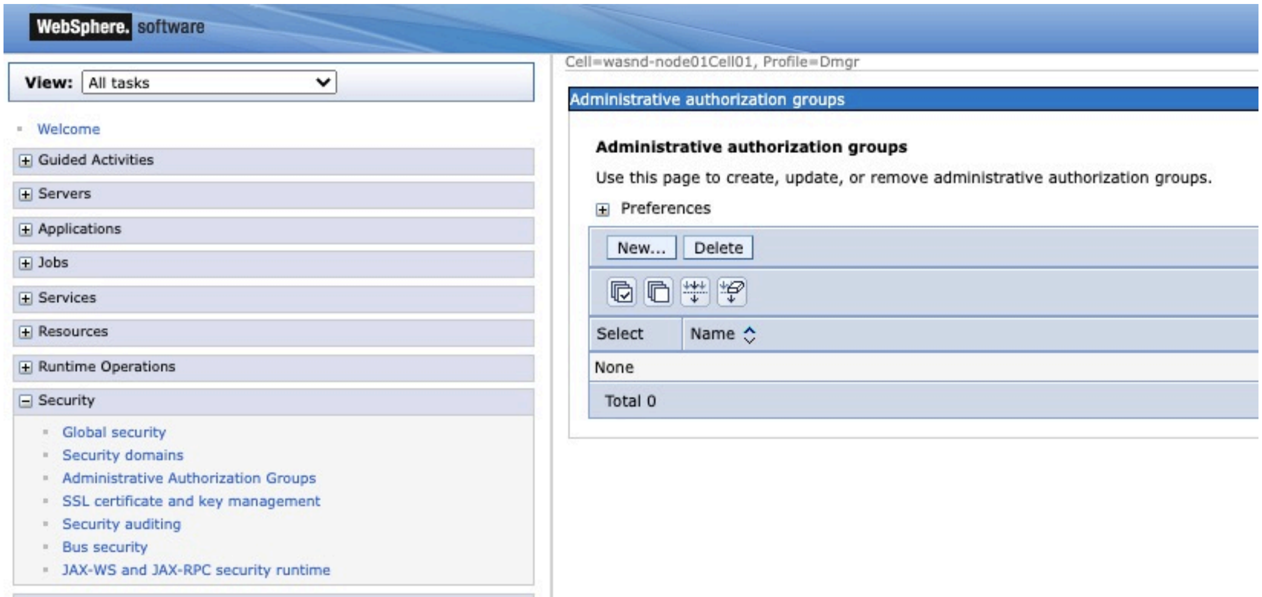

Administrative user roles

Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Select	User	Role(s)	Login Status
□	DefaultAppAdmin	Monitor	Not Active
□	PlantsAppAdmin	Monitor	Not Active
□	wasadm	Administrator	Not Active
	wasadmin	Primary administrative user name	Active
□	wascfg	Configurator	Not Active
□	wasmon	Monitor	Not Active
□	wasoper	Operator	Not Active
□	wassecmgr	Admin Security Manager	Not Active

Total 8



WebSphere. software

View: All tasks

- Welcome
- ⊞ Guided Activities
- ⊞ Servers
- ⊞ Applications
- ⊞ Jobs
- ⊞ Services
- ⊞ Resources
- ⊞ Runtime Operations
- ⊟ Security
  - Global security
  - Security domains
  - Administrative Authorization Groups
  - SSL certificate and key management
  - Security auditing
  - Bus security
  - JAX-WS and JAX-RPC security runtime

Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative authorization groups

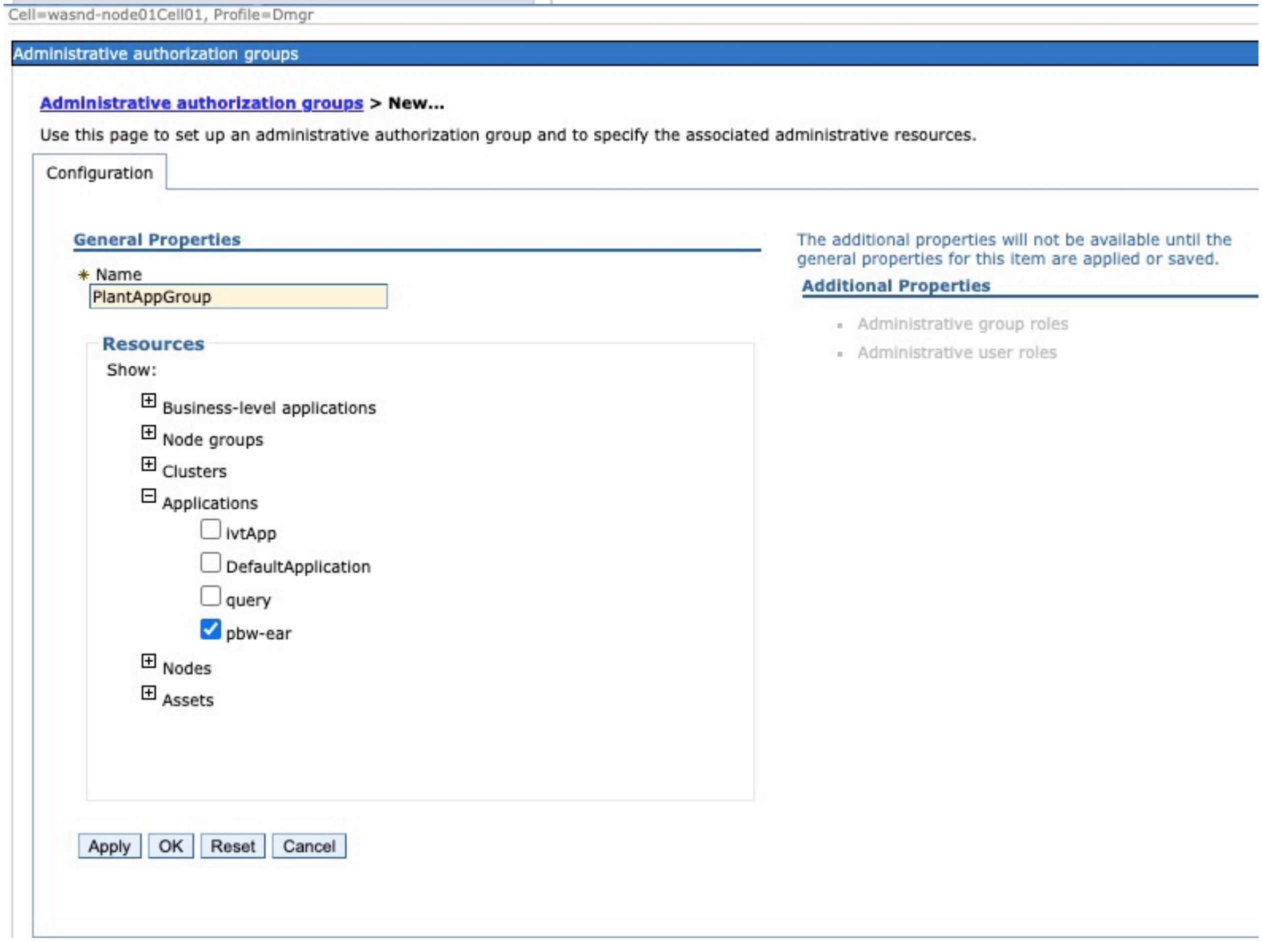
Administrative authorization groups

Use this page to create, update, or remove administrative authorization groups.

⊞ Preferences

New... Delete

Select	Name ⇕
None	
Total 0	



Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative authorization groups

Administrative authorization groups > New...

Use this page to set up an administrative authorization group and to specify the associated administrative resources.

Configuration

General Properties

* Name: PlantAppGroup

Resources

Show:

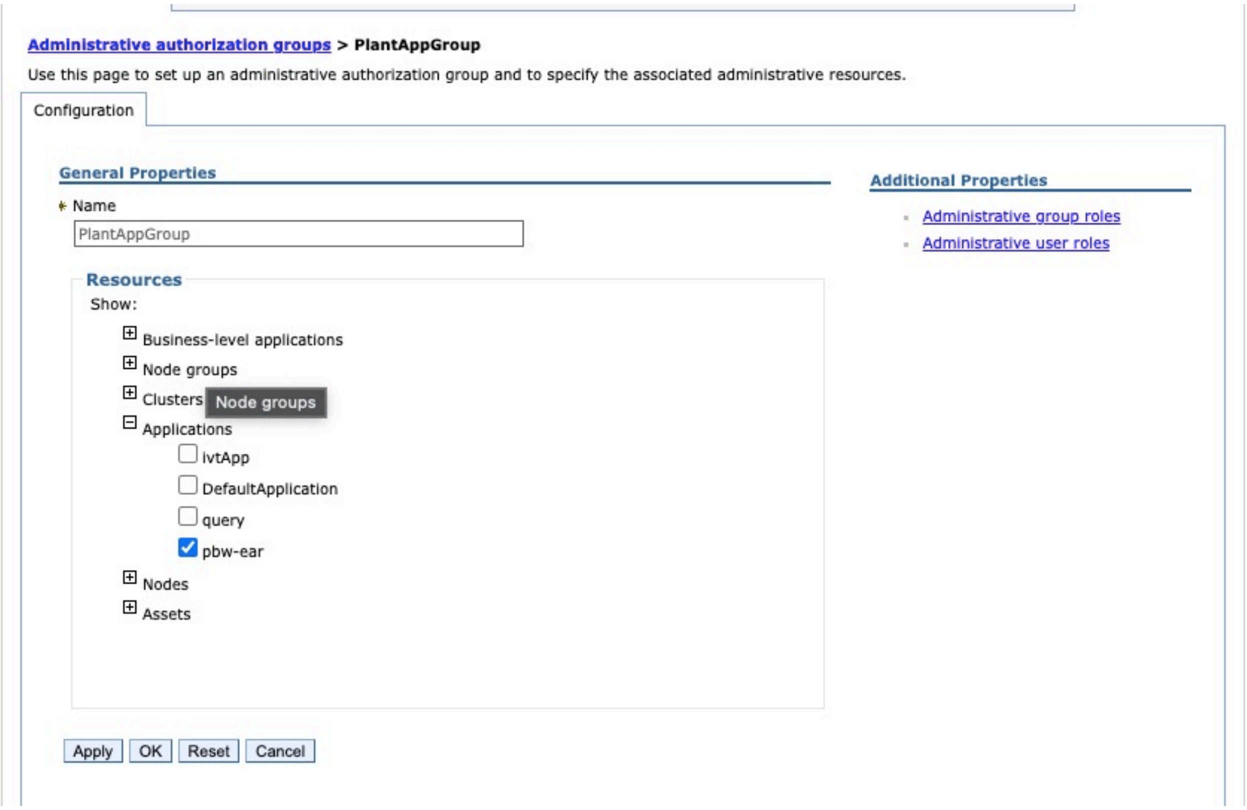
- ⊞ Business-level applications
- ⊞ Node groups
- ⊞ Clusters
- ⊟ Applications
  - ☐ ivtApp
  - ☐ DefaultApplication
  - ☐ query
  - ☑ pbw-ear
- ⊞ Nodes
- ⊞ Assets

Apply OK Reset Cancel

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

Additional Properties

- Administrative group roles
- Administrative user roles



Administrative authorization groups > **PlantAppGroup**

Use this page to set up an administrative authorization group and to specify the associated administrative resources.

Configuration

General Properties

* Name

PlantAppGroup

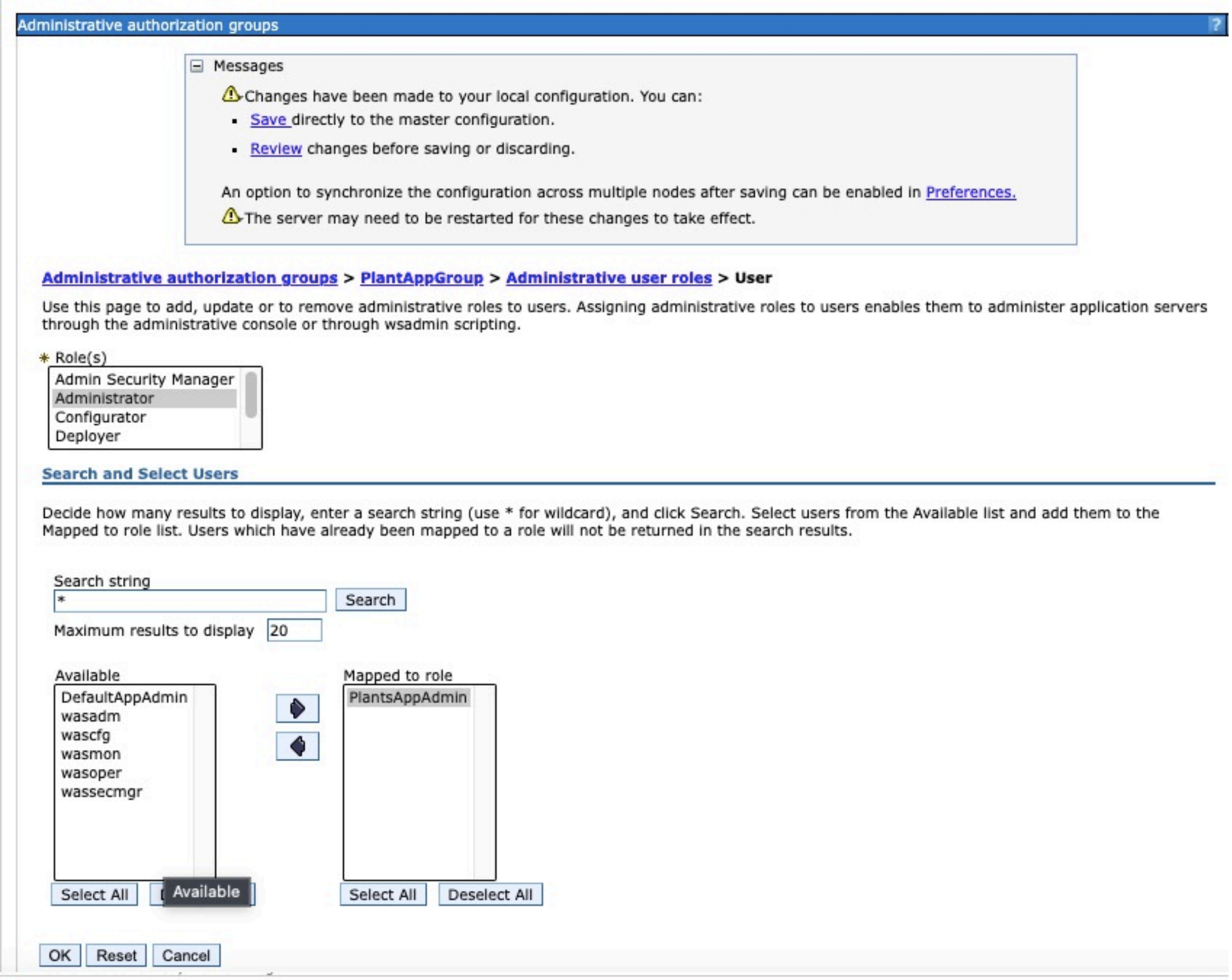
Resources

Show:

- ⊞ Business-level applications
- ⊞ Node groups
- ⊞ Clusters
- ⊟ Applications
  - □ ivtApp
  - □ DefaultApplication
  - □ query
  - ☑ pbw-ear
- ⊞ Nodes
- ⊞ Assets

Additional Properties

- Administrative group roles
- Administrative user roles



Administrative authorization groups

⊟ Messages

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

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

An option to synchronize the configuration across multiple nodes after saving can be enabled in Preferences.

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

Administrative authorization groups > PlantAppGroup > Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.

* Role(s)

Admin Security Manager
Administrator
Configurator
Deployer

Search and Select Users

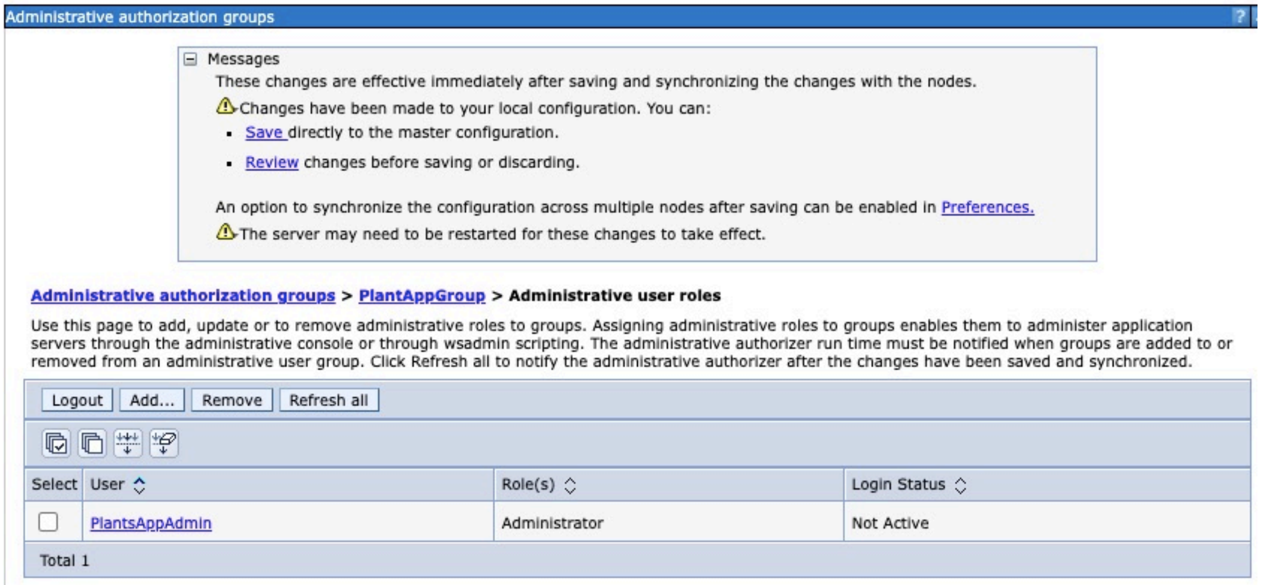
Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: *

Maximum results to display: 20

Available:
DefaultAppAdmin
wasadm
wascfg
wasmon
wasoper
wassecmgr

Mapped to role:
PlantsAppAdmin



Administrative authorization groups

⊟ Messages

These changes are effective immediately after saving and synchronizing the changes with the nodes.

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

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

An option to synchronize the configuration across multiple nodes after saving can be enabled in Preferences.

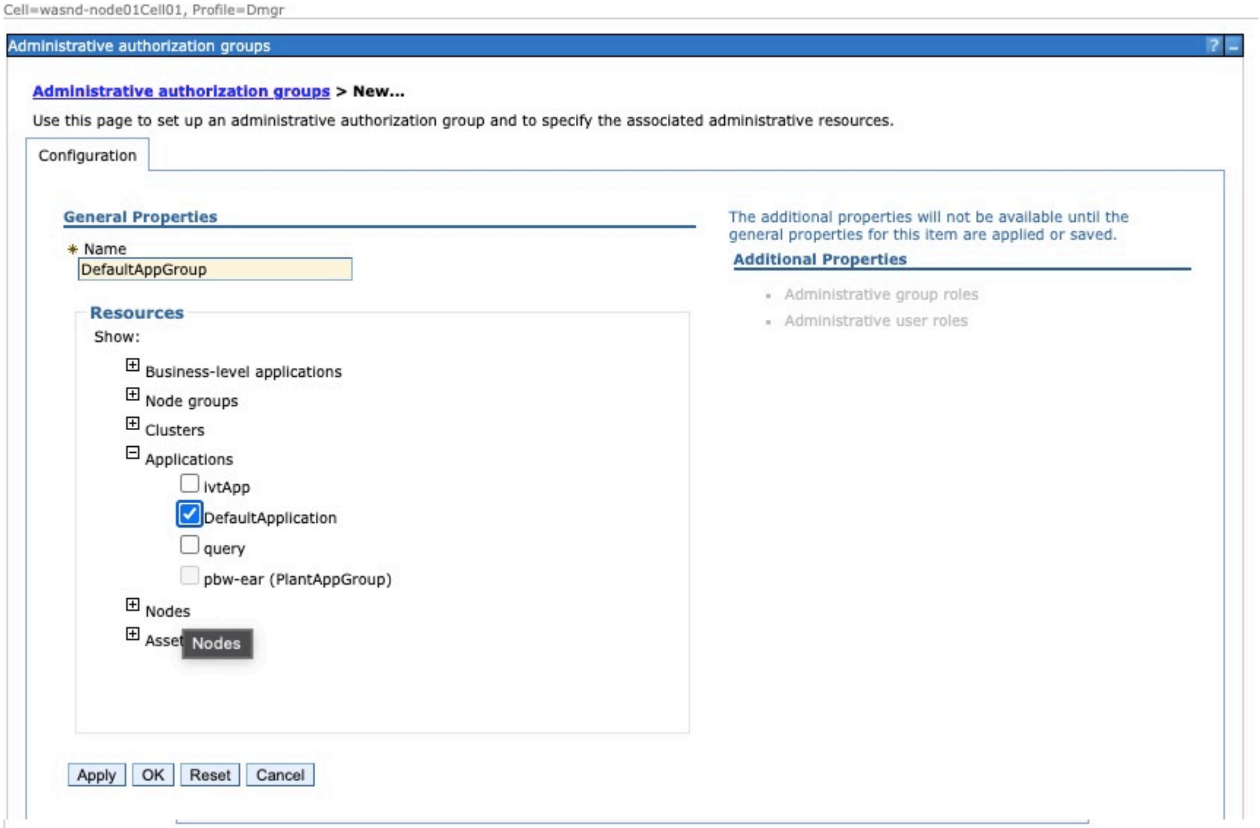
⚠ The server may need to be restarted for these changes to take effect.

Administrative authorization groups > PlantAppGroup > Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Select	User	Role(s)	Login Status
☐	PlantsAppAdmin	Administrator	Not Active

Total 1



Cell=wasnd-node01Cell01, Profile=Dmgr

Administrative authorization groups

Administrative authorization groups > New...

Use this page to set up an administrative authorization group and to specify the associated administrative resources.

General Properties

* Name: DefaultAppGroup

Resources

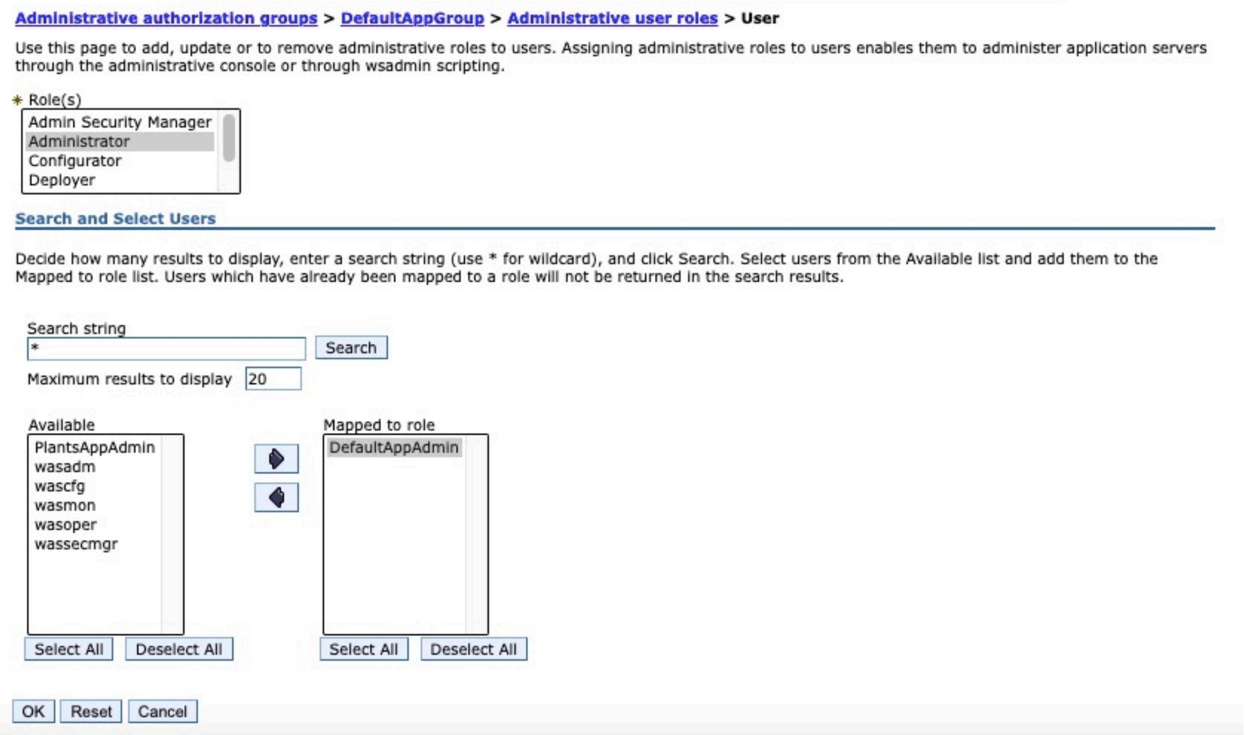
Show:

- ⊞ Business-level applications
- ⊞ Node groups
- ⊞ Clusters
- ⊟ Applications
  - □ ivtApp
  - ☑ DefaultApplication
  - □ query
  - □ pbw-ear (PlantAppGroup)
- ⊞ Nodes
- ⊞ Asset

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

Additional Properties

- Administrative group roles
- Administrative user roles



Administrative authorization groups > DefaultAppGroup > Administrative user roles > User

Use this page to add, update or to remove administrative roles to users. Assigning administrative roles to users enables them to administer application servers through the administrative console or through wsadmin scripting.

* Role(s)

- Admin Security Manager
- Administrator
- Configurator
- Deployer

Search and Select Users

Decide how many results to display, enter a search string (use * for wildcard), and click Search. Select users from the Available list and add them to the Mapped to role list. Users which have already been mapped to a role will not be returned in the search results.

Search string: *

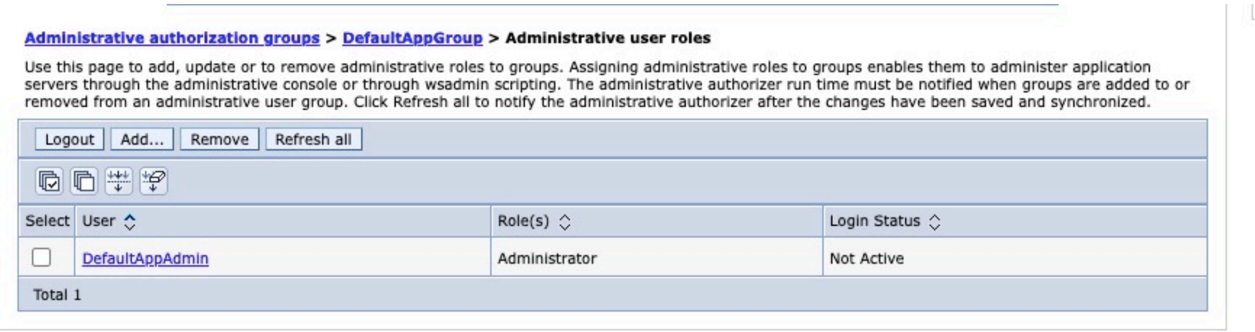
Maximum results to display: 20

Available:

- PlantsAppAdmin
- wasadm
- wascfg
- wasmon
- wasoper
- wassecmgr

Mapped to role:

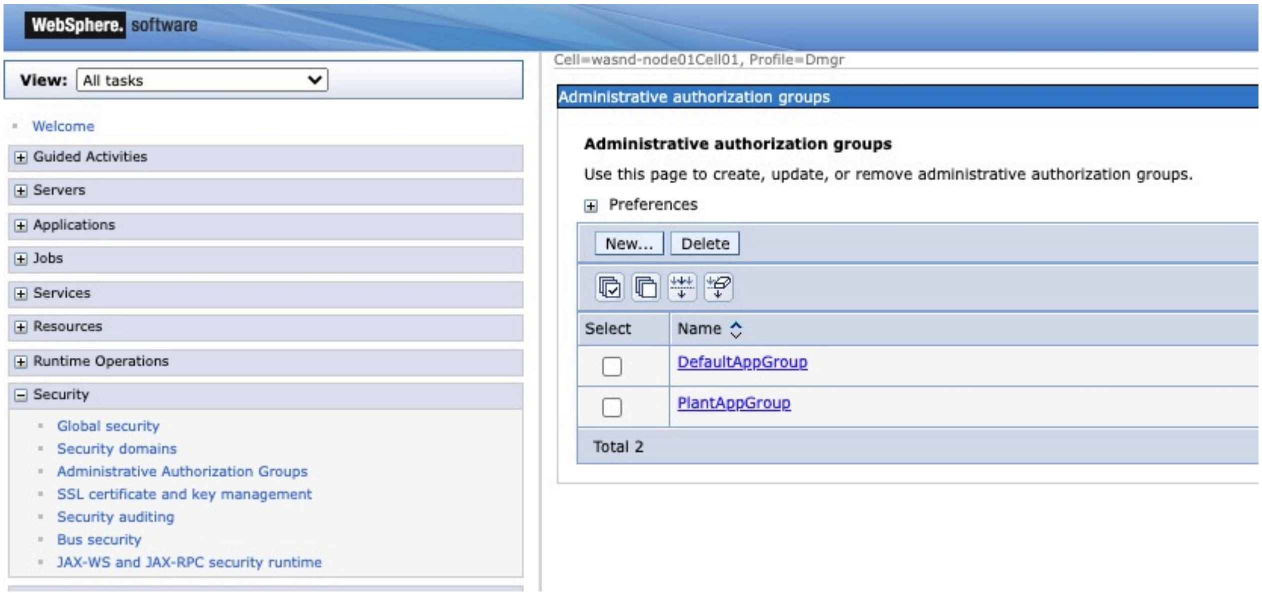
- DefaultAppAdmin



Administrative authorization groups > DefaultAppGroup > Administrative user roles

Use this page to add, update or to remove administrative roles to groups. Assigning administrative roles to groups enables them to administer application servers through the administrative console or through wsadmin scripting. The administrative authorizer run time must be notified when groups are added to or removed from an administrative user group. Click Refresh all to notify the administrative authorizer after the changes have been saved and synchronized.

Select	User	Role(s)	Login Status
□	DefaultAppAdmin	Administrator	Not Active
Total 1			



Cell=wasnd-node01Cell01, Profile=Dmgr

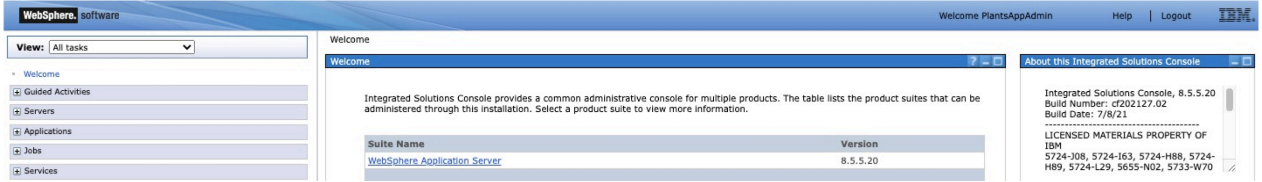
Administrative authorization groups

Use this page to create, update, or remove administrative authorization groups.

Select	Name
□	DefaultAppGroup
□	PlantAppGroup
Total 2	

Section 5: Test the fine-grained access

Now that the new administrative console users are created, and the administrative authorization groups are added and mapped to the applications, access by the users to the applications must be verified.

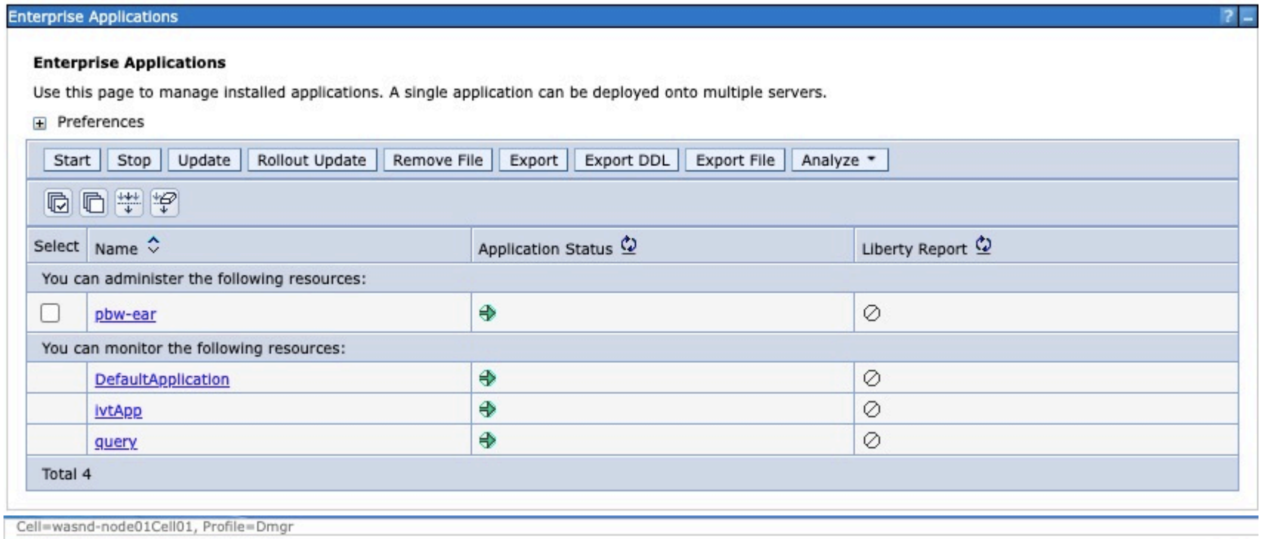


Integrated Solutions Console provides a common administrative console for multiple products. The table lists the product suites that can be administered through this installation. Select a product suite to view more information.

Suite Name	Version
WebSphere Application Server	8.5.5.20

Integrated Solutions Console, 8.5.5.20
Build Number: cf202127.02
Build Date: 7/8/21

LICENSED MATERIALS PROPERTY OF IBM
5724-J08, 5724-I63, 5724-H88, 5724-H89, 5724-L29, 5655-N02, 5733-W70

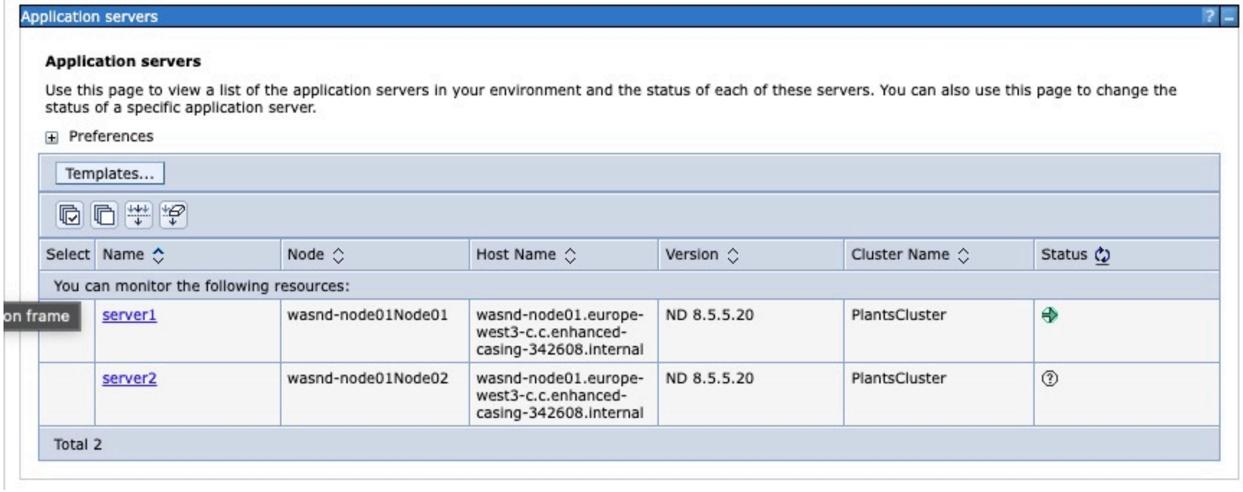


Enterprise Applications

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

Select	Name	Application Status	Liberty Report
You can administer the following resources:			
□	pbw-ear	➡	⊘
You can monitor the following resources:			
	DefaultApplication	➡	⊘
	ivtApp	➡	⊘
	query	➡	⊘
Total 4			

Cell=wasnd-node01Cell01, Profile=Dmgr



Application servers

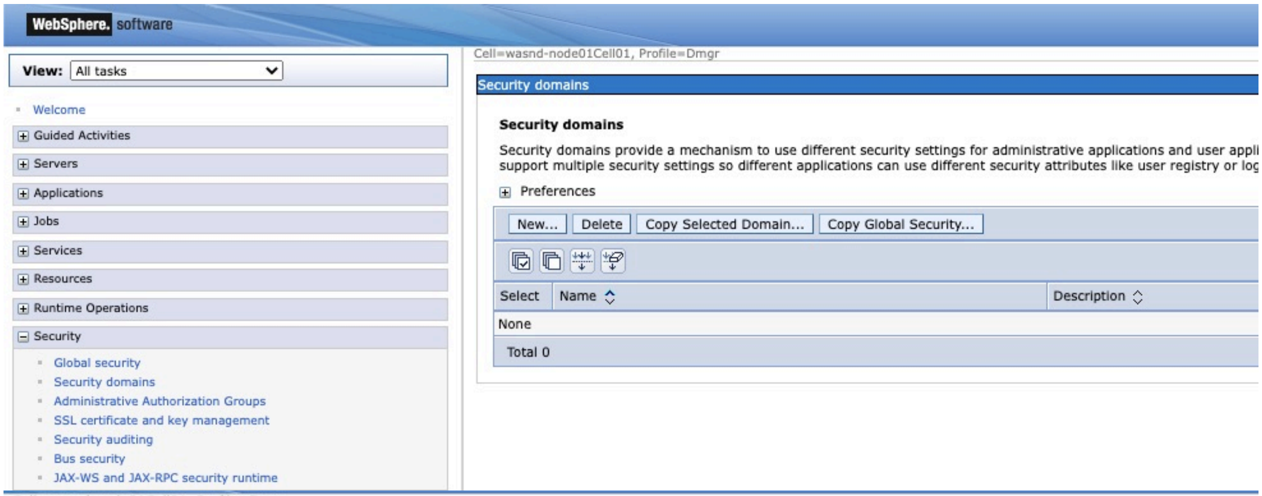
Use this page to view a list of the application servers in your environment and the status of each of these servers. You can also use this page to change the status of a specific application server.

Select	Name	Node	Host Name	Version	Cluster Name	Status
You can monitor the following resources:						
	server1	wasnd-node01Node01	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	PlantsCluster	➡
	server2	wasnd-node01Node02	wasnd-node01.europe-west3-c.c.enhanced-casing-342608.internal	ND 8.5.5.20	PlantsCluster	?
Total 2						

Section 6: Examine security domains

In the previous section, fine-grained access control was configured, thus allowing administrators the ability to have better control over which administrators have access to which portions of a cell.

Security domains allow an administrator to define alternative security configurations for a cell. Historically, security configurations were defined only at a cell level, which meant that if something such as a user registry was defined within a cell, it applied to the whole cell. There was no ability to define an alternative configuration for specific sections of a cell.



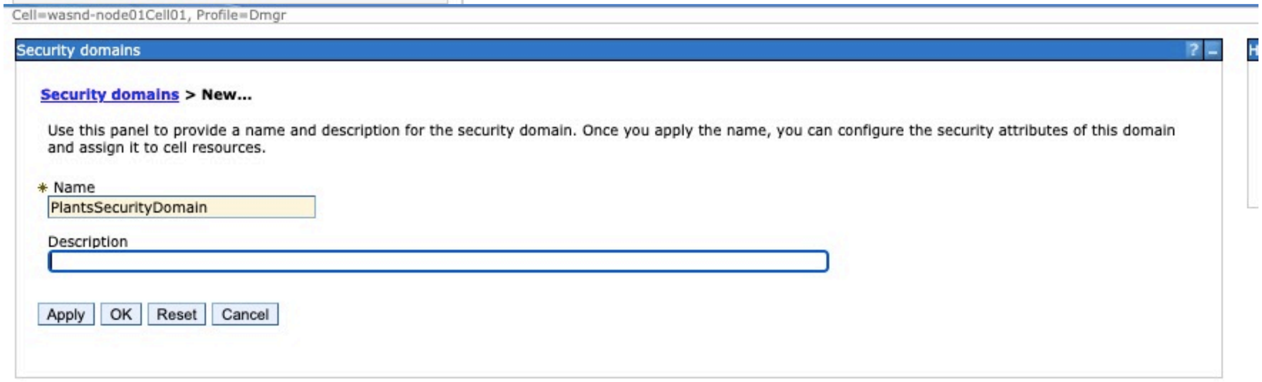
Cell=wasnd-node01Cell01, Profile=Dmgr

Security domains

Security domains

Security domains provide a mechanism to use different security settings for administrative applications and user appli
support multiple security settings so different applications can use different security attributes like user registry or log

Select	Name	Description
None		
Total 0		



Cell=wasnd-node01Cell01, Profile=Dmgr

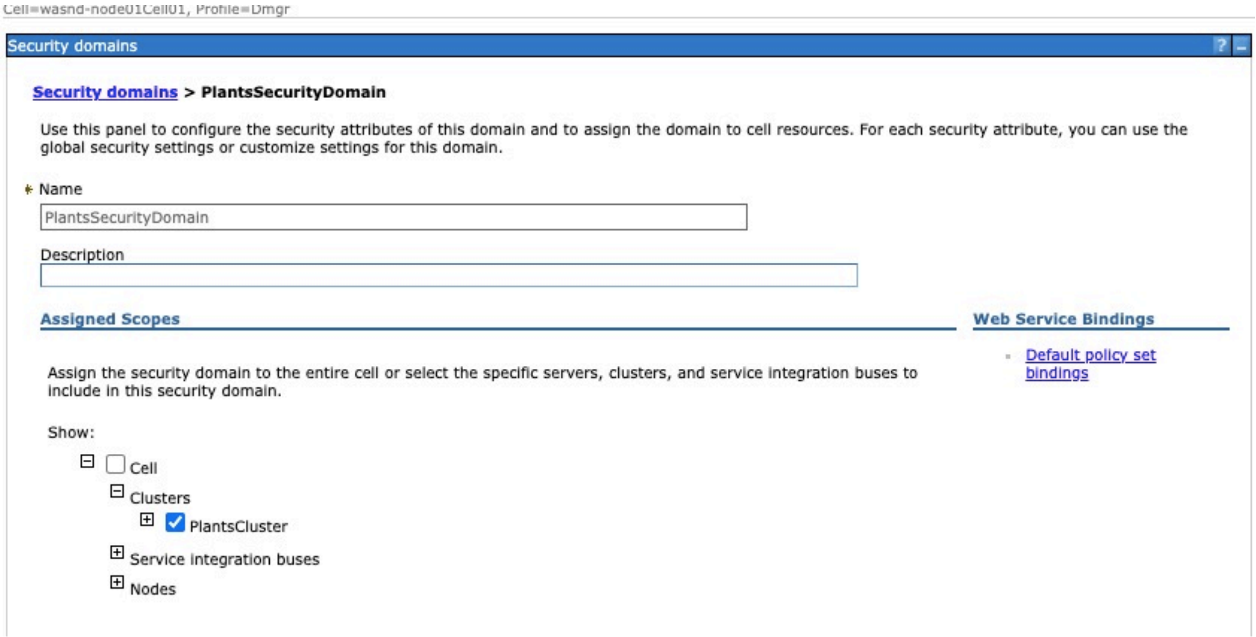
Security domains

Security domains > New...

Use this panel to provide a name and description for the security domain. Once you apply the name, you can configure the security attributes of this domain and assign it to cell resources.

* Name: PlantsSecurityDomain

Description:



Cell=wasnd-node01Cell01, Profile=Dmgr

Security domains

Security domains > PlantsSecurityDomain

Use this panel to configure the security attributes of this domain and to assign the domain to cell resources. For each security attribute, you can use the global security settings or customize settings for this domain.

* Name: PlantsSecurityDomain

Description:

Assigned Scopes

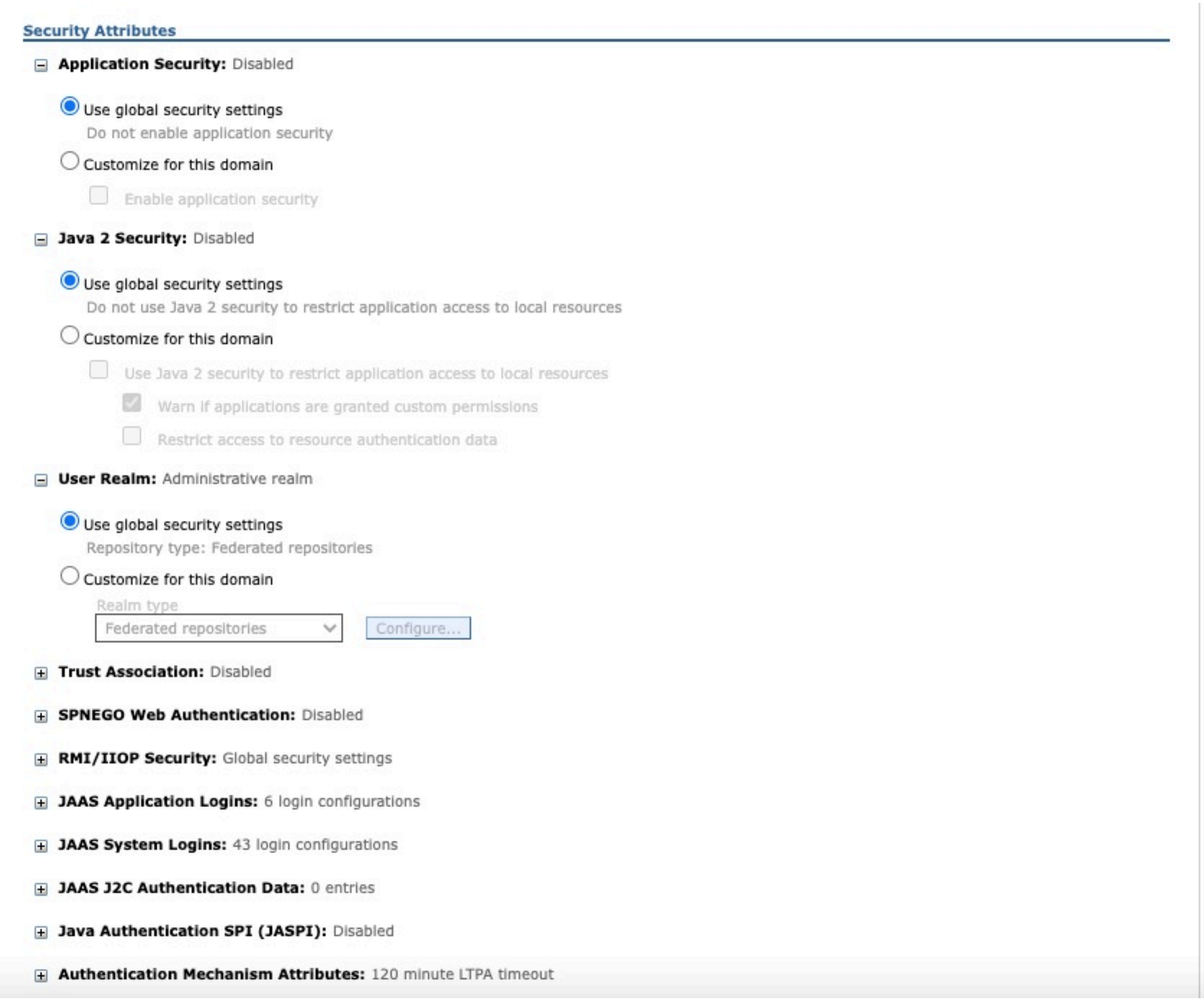
Assign the security domain to the entire cell or select the specific servers, clusters, and service integration buses to include in this security domain.

Show:

- □ Cell
  - Clusters
    - ☑ PlantsCluster
  - Service integration buses
  - Nodes

Web Service Bindings

- Default policy set bindings



Security Attributes

⊟ **Application Security:** Disabled

● Use global security settings
Do not enable application security

○ Customize for this domain

□ Enable application security

⊟ **Java 2 Security:** Disabled

● Use global security settings
Do not use Java 2 security to restrict application access to local resources

○ Customize for this domain

□ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

□ Restrict access to resource authentication data

⊟ **User Realm:** Administrative realm

● Use global security settings
Repository type: Federated repositories

○ Customize for this domain

Realm type
Federated repositories ⌄ Configure...

⊞ **Trust Association:** Disabled

⊞ **SPNEGO Web Authentication:** Disabled

⊞ **RMI/IIOP Security:** Global security settings

⊞ **JAAS Application Logins:** 6 login configurations

⊞ **JAAS System Logins:** 43 login configurations

⊞ **JAAS J2C Authentication Data:** 0 entries

⊞ **Java Authentication SPI (JASPI):** Disabled

⊞ **Authentication Mechanism Attributes:** 120 minute LTPA timeout