18

Security Concepts and Configuration

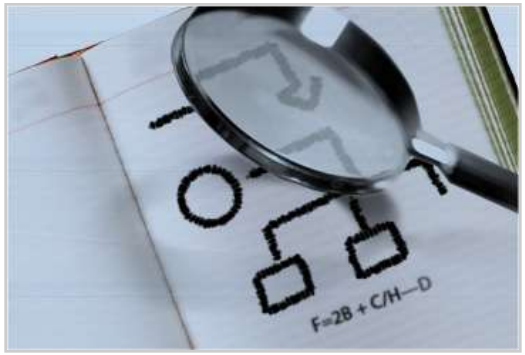
Objectives

After completing this lesson, you should be able to do the following:

- Use the WLS security architecture
- Configure security realms
- Configure users and groups
- Configure roles
- Configure policies
- Configure protection for:
  - Web application resources
  - EJBs

Road Map

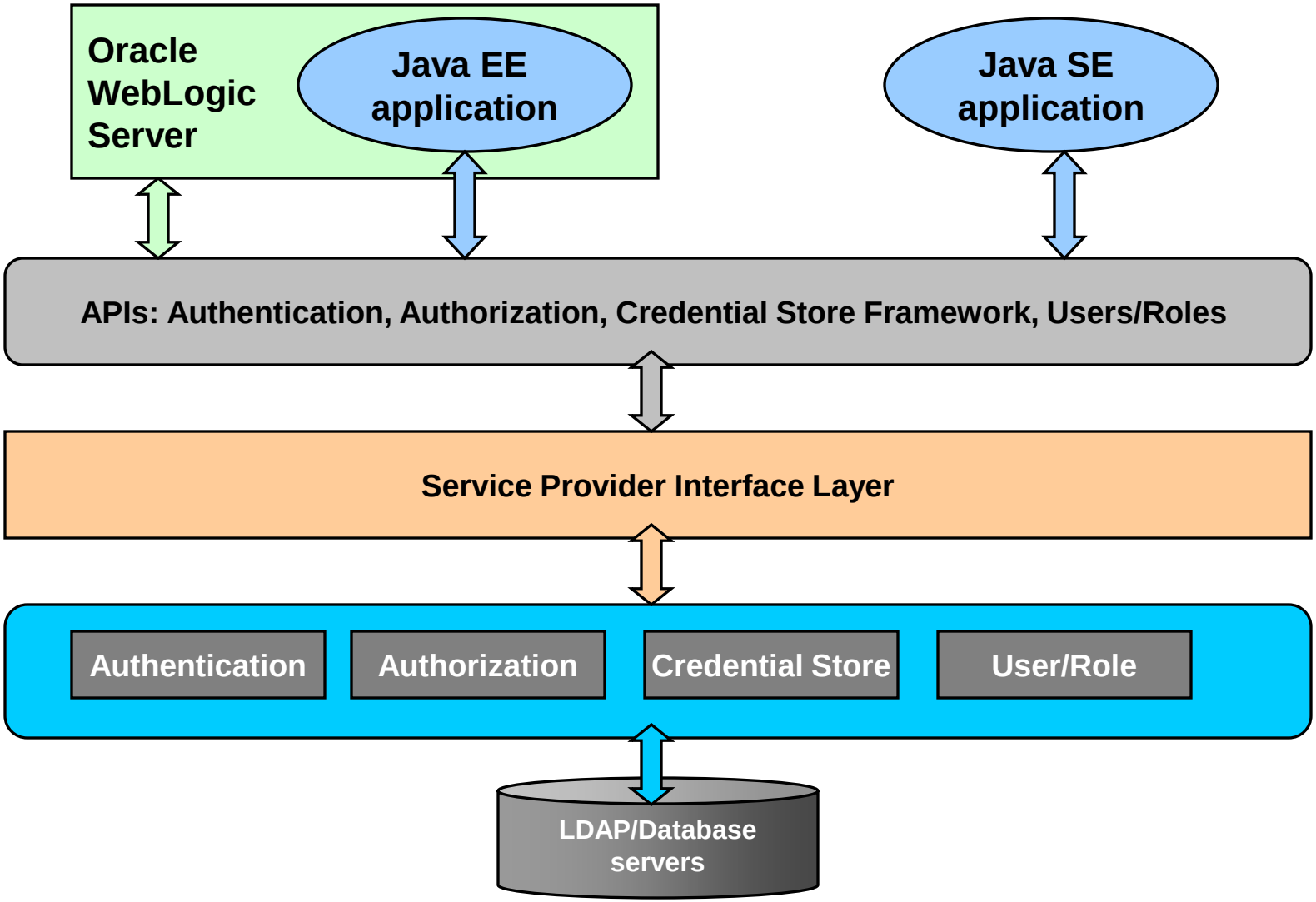
- Security overview
  - Oracle Platform Security Services
  - Oracle WLS Security
  - Oracle WLS Security Models
  - Introduction to WLS Security components
- Users and groups
- Protecting application resources



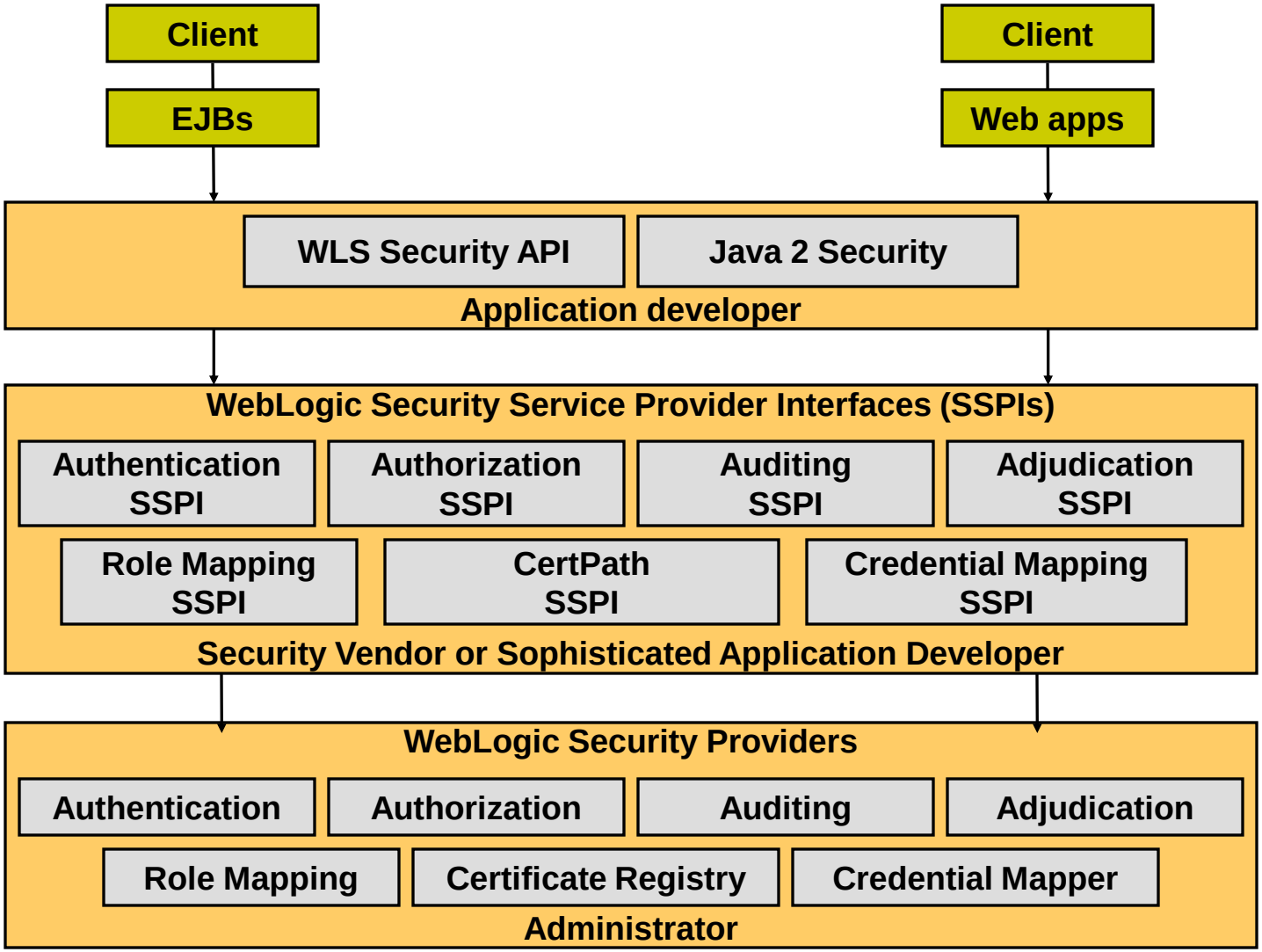
Introduction to Oracle WebLogic Security Service

- Security is a challenge in environments with diverse applications and Web-based services.
- This requires established and well-communicated security policies and procedures.
- You can use Oracle WebLogic Server as a comprehensive and flexible security infrastructure to protect applications.

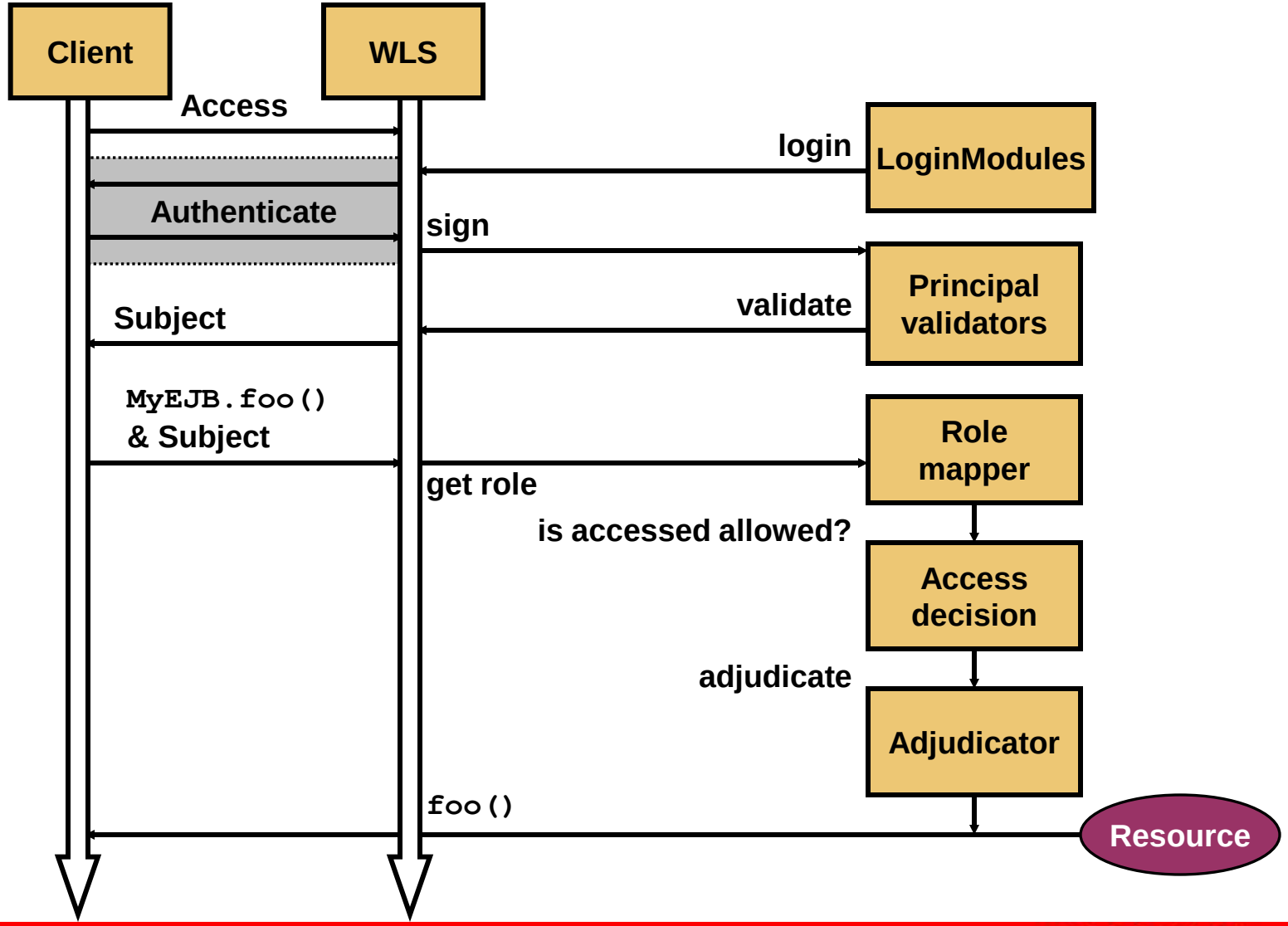
Oracle Platform Security Services



Oracle WLS Security Architecture



Security Services



Overview of Security Concepts

- Authentication providers handle identity information and make it possible to associate with users, groups, or roles.
- Identity assertion providers map a valid token to an Oracle WebLogic Server user.
- An authorization provider is a process that is used to control the interactions between users and resources based on user identity.
- The adjudication provider weighs the results that multiple access decisions return to determine the final decision.
- The credential mapping process is initiated when application components access the authentication mechanism of a legacy system to obtain a set of credentials.
- Auditing provides a trail of activity. The auditing provider is used to log activity before and after security operations.

Confidentiality

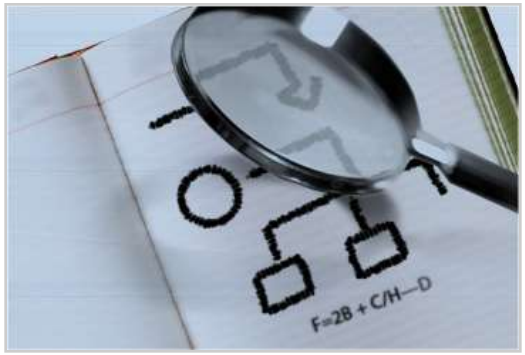
- Oracle WebLogic Server supports the Secure Sockets Layer (SSL) protocol to secure the communication between the clients and the server.
- The SSL client authentication allows a server to confirm a user's identity by verifying that a client's certificate and public ID are valid and are issued by a Certificate Authority (CA).
- The SSL server authentication allows a user to confirm a server's identity by verifying that the server's certificate and public ID are valid and are issued by a CA.

Credential Mapping

- The credential mapping process is used when application components access the authentication mechanism of an external system to obtain a set of credentials.
- The requesting application passes the subject as part of the call and information about the type of credentials required.
- Credentials are returned to the security framework, which is then passed to the requesting application component.
- The application component uses the credentials to access the external system.

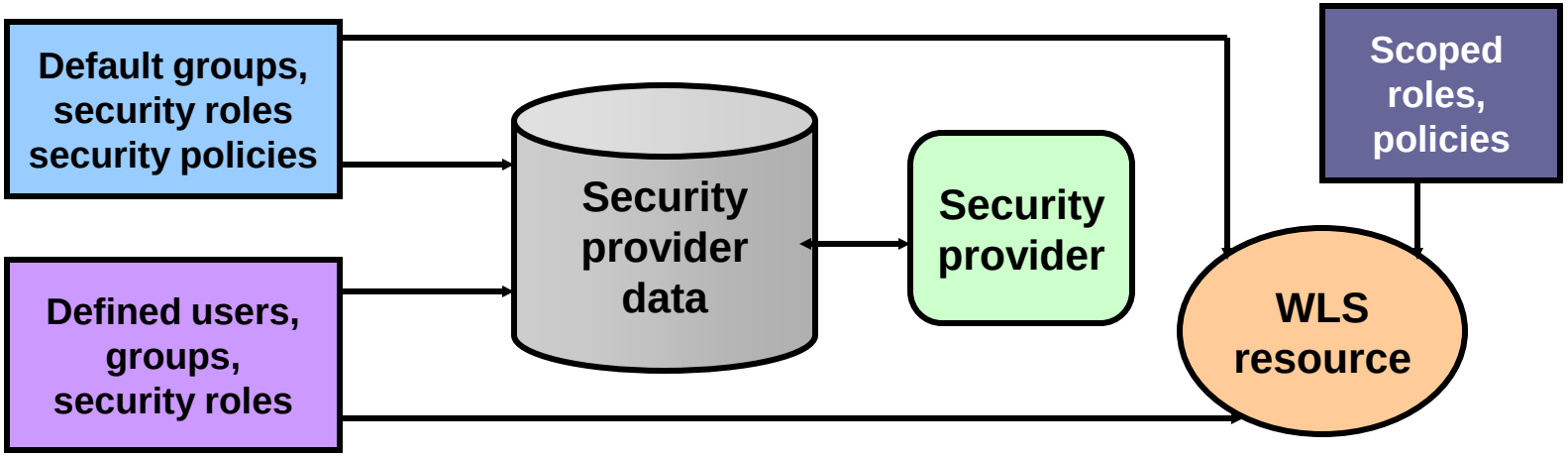
Road Map

- Security overview
- Users and groups
  - Security realms
  - Embedded LDAP
  - Configuring users, groups, and roles
- Protecting application resources



Security Realms

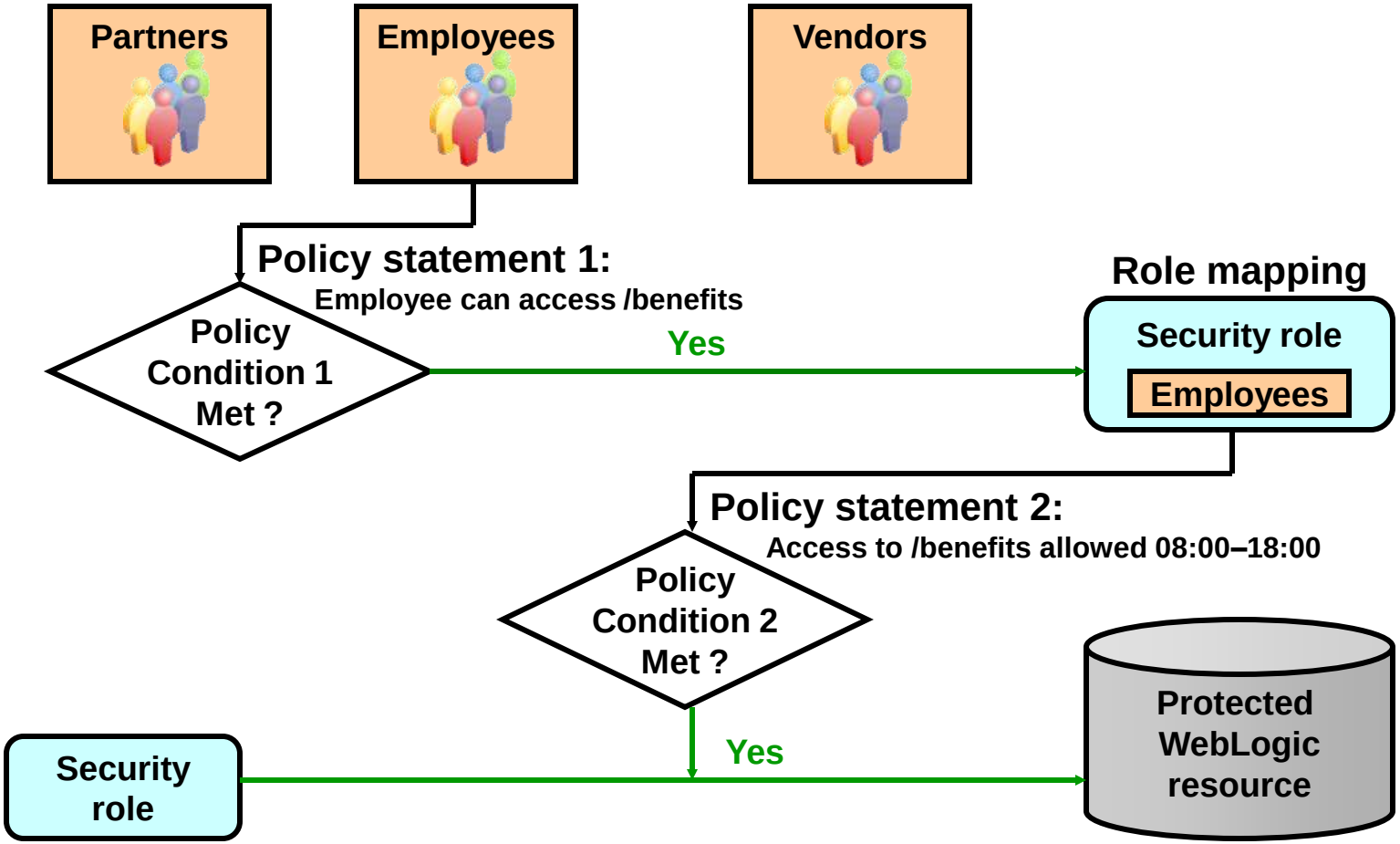
- A security realm is a collection of system resources and security service providers.
- A valid user must be authenticated by the authentication provider in the security realm.
- Only one security realm can be active at a given time.
- A single security policy can be used in any realm.
- Administration tasks include creating security realms.



Security Model Options for Applications

Security Model	Location of Users, Roles, and Policies	Security Checks Performed
Deployment Descriptor Only (Java EE standard)	Deployment descriptors: • `web.xml and weblogic.xml` • `ejb-jar.xml and weblogic-ejb-jar.xml`	Only when clients request URLs or EJB methods that are protected by a policy in the deployment descriptor
Custom Roles	Role mappings from a role mapping provider that you configure for the security realm Policies are defined in the `web.xml` and `ejb-jar.xml` deployment descriptors.	Only when clients request URLs or EJB methods that are protected by a policy in the deployment descriptor.
Custom Roles and Policies	Role mappings and authorization from providers that you configure for the security realm	For all URLs and EJB methods in the application
Advanced	This model is fully flexible. You can import security data from deployment descriptors into the security provider databases to provide a baseline.	Configurable

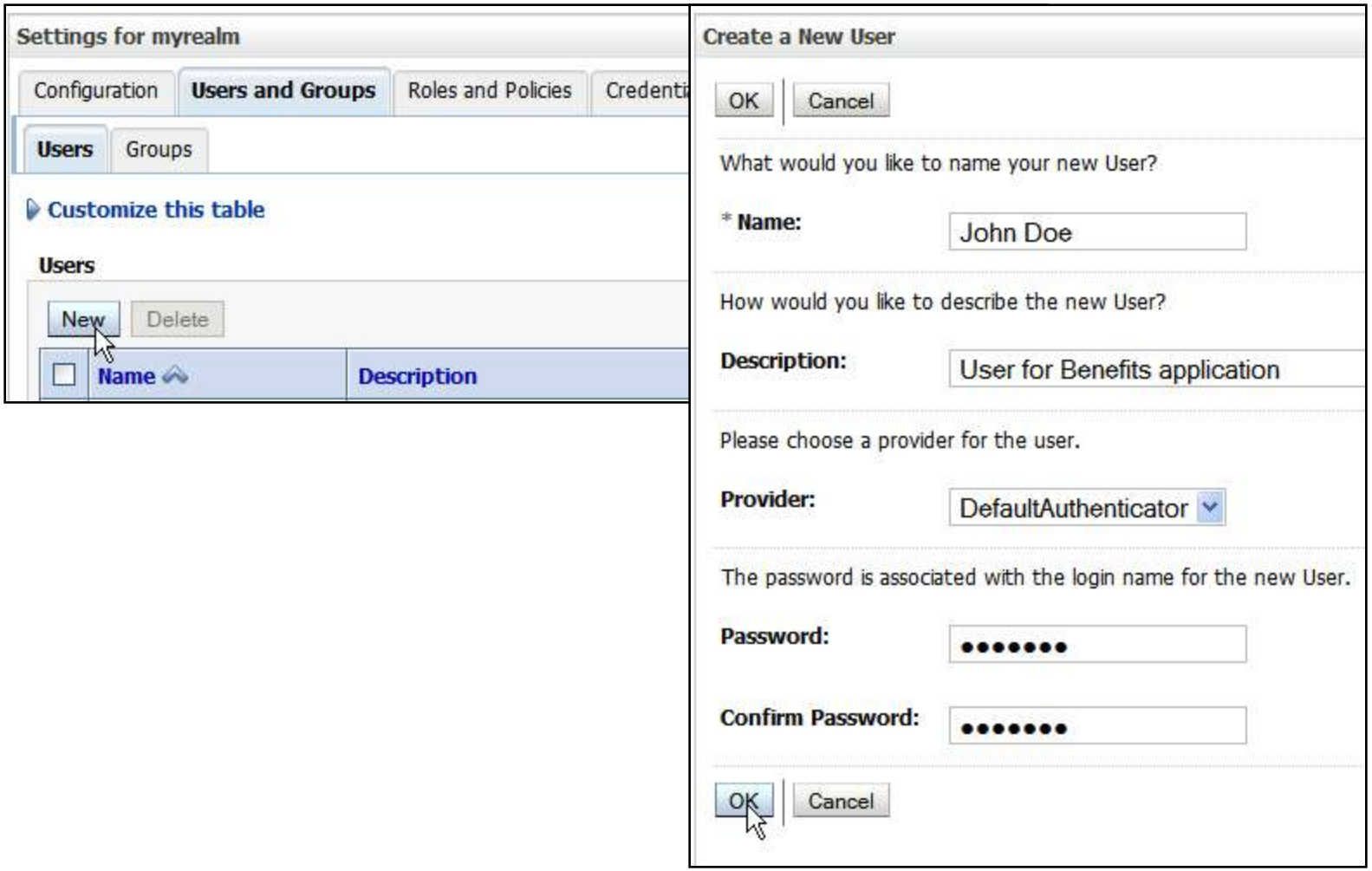
How WLS Resources Are Protected



Users and Groups

- Users are entities that use WLS, such as:
  - Application end users
  - Client applications
  - Other Oracle WebLogic Servers
- Groups are:
  - Logical sets of users
  - More efficient for managing a large number of users

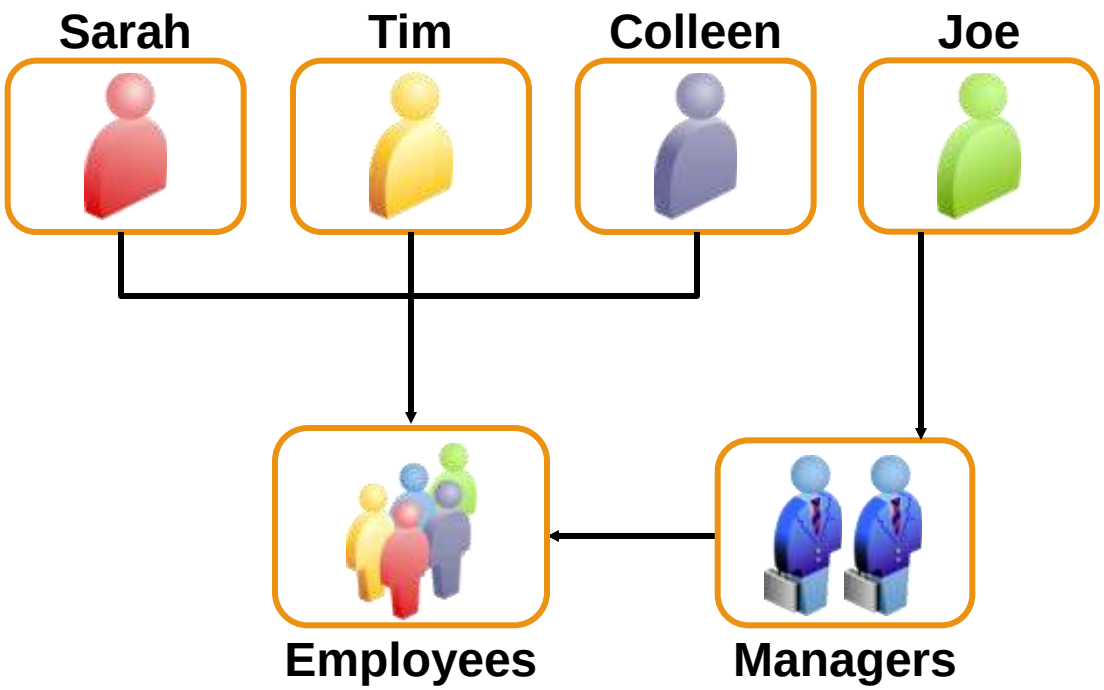
Configuring New Users



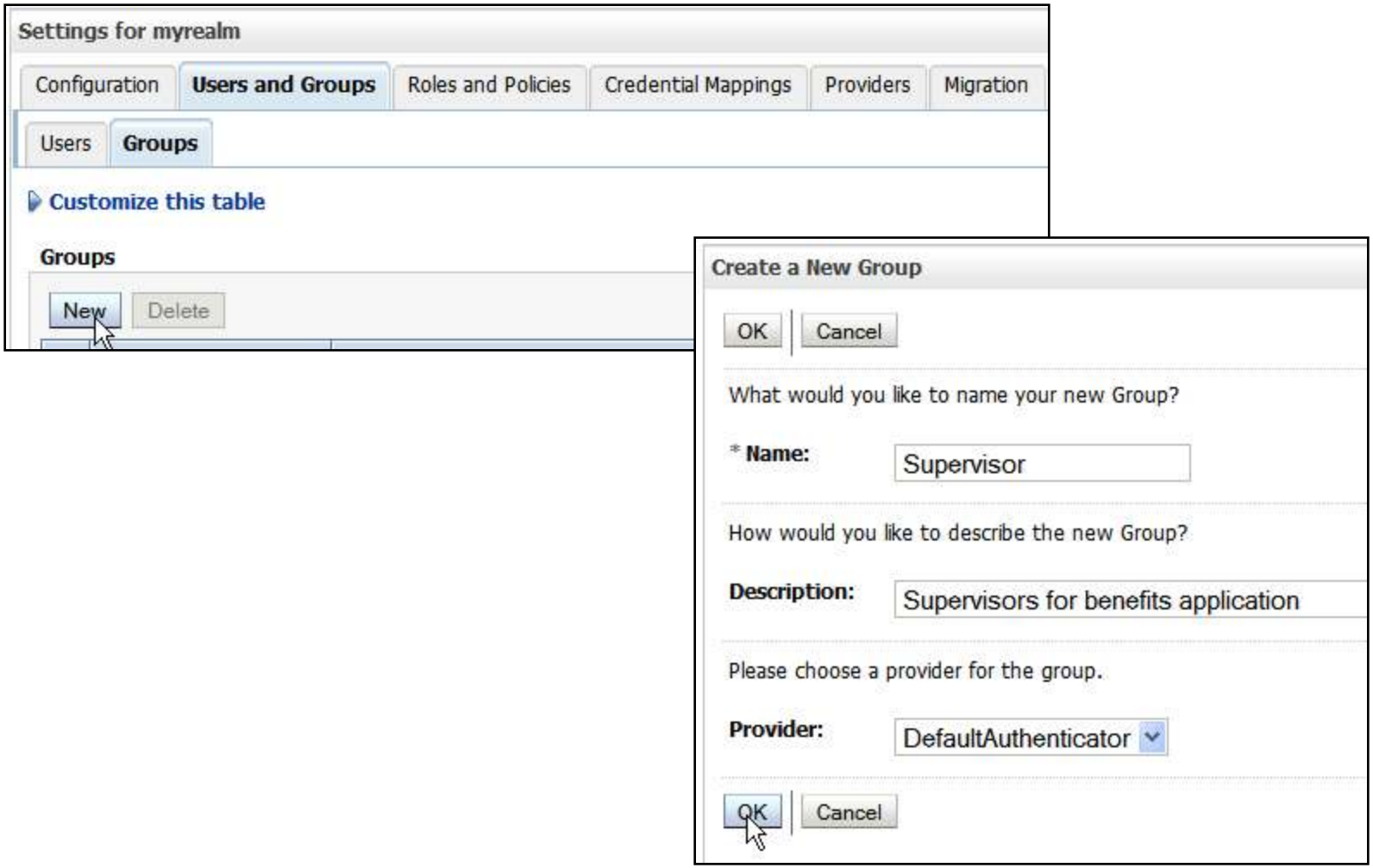
Groups

WLS provides the flexibility to organize groups in various ways:

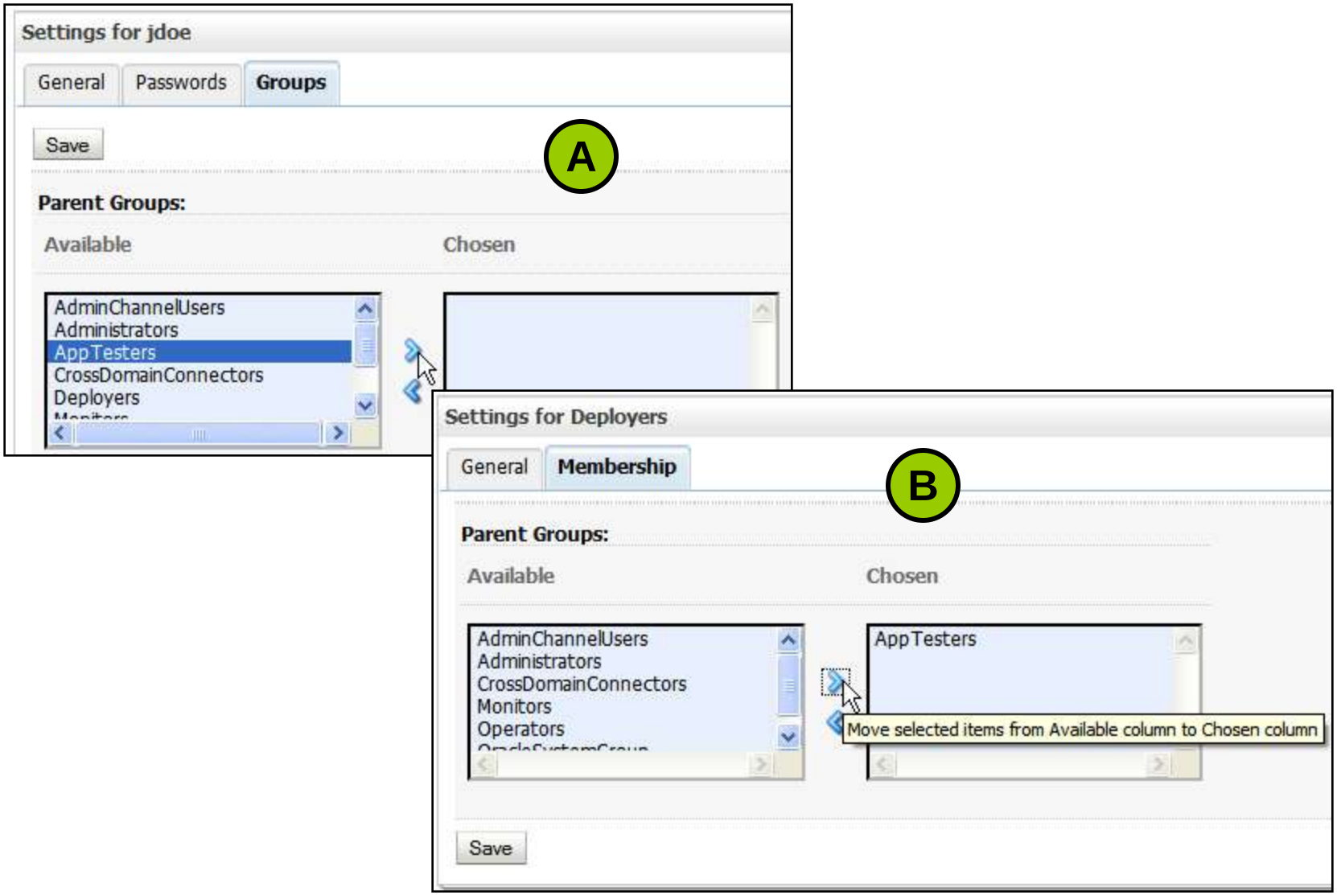
- Groups can contain users.
- Groups can contain other groups.



Configuring New Groups



Configuring Group Memberships



Road Map

- Security overview
- Users and groups
- Roles and policies
  - Security roles
  - Security policies
  - Defining policies and roles
  - Protecting Web resources
  - Protecting other resources

Security Roles

- A role refers to a set of permissions granted to a user or group.
- A role differs from a group; a group has static membership, whereas a role is conditional.
- A user and group can be granted multiple roles.
- The two types of roles are global-scoped roles and resource-scoped roles.
- The global roles that are available by default are Admin, Operator, Deployer, Monitor, AppTester, and Anonymous.
- Roles defined in deployment descriptors can be inherited.
- You can manage role definitions and assignments without editing deployment descriptors or redeploying the application.

Configuring the Global Security Role

Lock & Edit

Release Configuration

Domain Structure

MedRecDomain
- Environment
- Deployments
- Services
- Security Realms
- Interoperability
- Diagnostics

How do I...
- Manage security roles
- Create scoped roles for JNDI resources
- Create scoped roles for WorkContext resources

System Status

Configuration | Users and Groups | Roles and Policies | Credential Mappings | Providers

Realm Roles | Realm Policies

Use this table to view, add, modify or remove global or scoped security roles for this security rea
Name column under the Global Roles node. Scoped roles are listed in the Name column under th
secure.

Notes:
- This table does n
view the Security
- If you imported s
Application Assis

Roles

Edit Role

Name
Deployments
Domain
Global Roles
Roles

Create a New Role for this Realm

OK | Cancel

Role Properties

The following properties will be used to identify your new role.

* Indicates required fields

What would you like to name your new role?

* Name: MyTest

Which role mapper would you like to use with this role?

Provider Name: XACMLRoleMapper

OK | Cancel

Security Policies

- Security policies implement parameterized authorization.
- Security policies comprise rules and conditions.
- Users and groups that adhere to the security policy are granted access to resources protected by the policy.
- Security policies follow a hierarchy. The policy of a narrower scope overrides that of a broader scope.
- When you install Oracle WebLogic Server, some default root-level policies are provided.

Policy Conditions

- Policy conditions are the essential components of a policy.
- The WebLogic Server authorization provides three kinds of built-in policy conditions in the Administration Console:
  - Basic policy conditions
  - Date and Time policy conditions
  - Context Element policy conditions

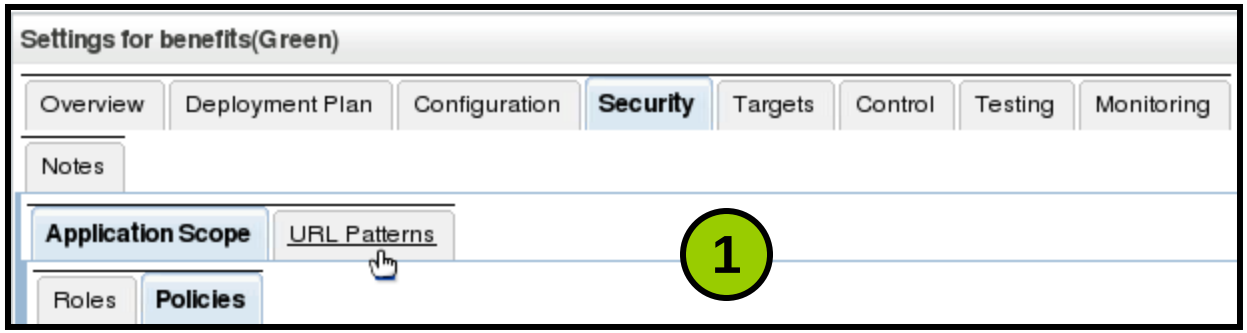
Protecting Web Applications

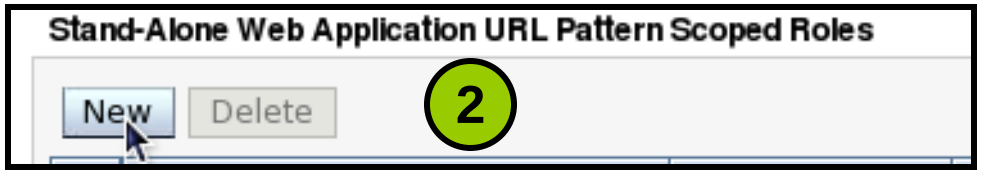
To protect a Web application with declarative security, perform the following steps:

1. Define the roles that should access the protected resources.
2. Determine the Web application resources that must be protected.
3. Map the protected resources to roles that should access them.
4. Map roles to users or groups in the WLS security realm.
5. Set up an authentication mechanism.

Specifying Protected Web Resources

Protection for Web resources are defined based on URL patterns.



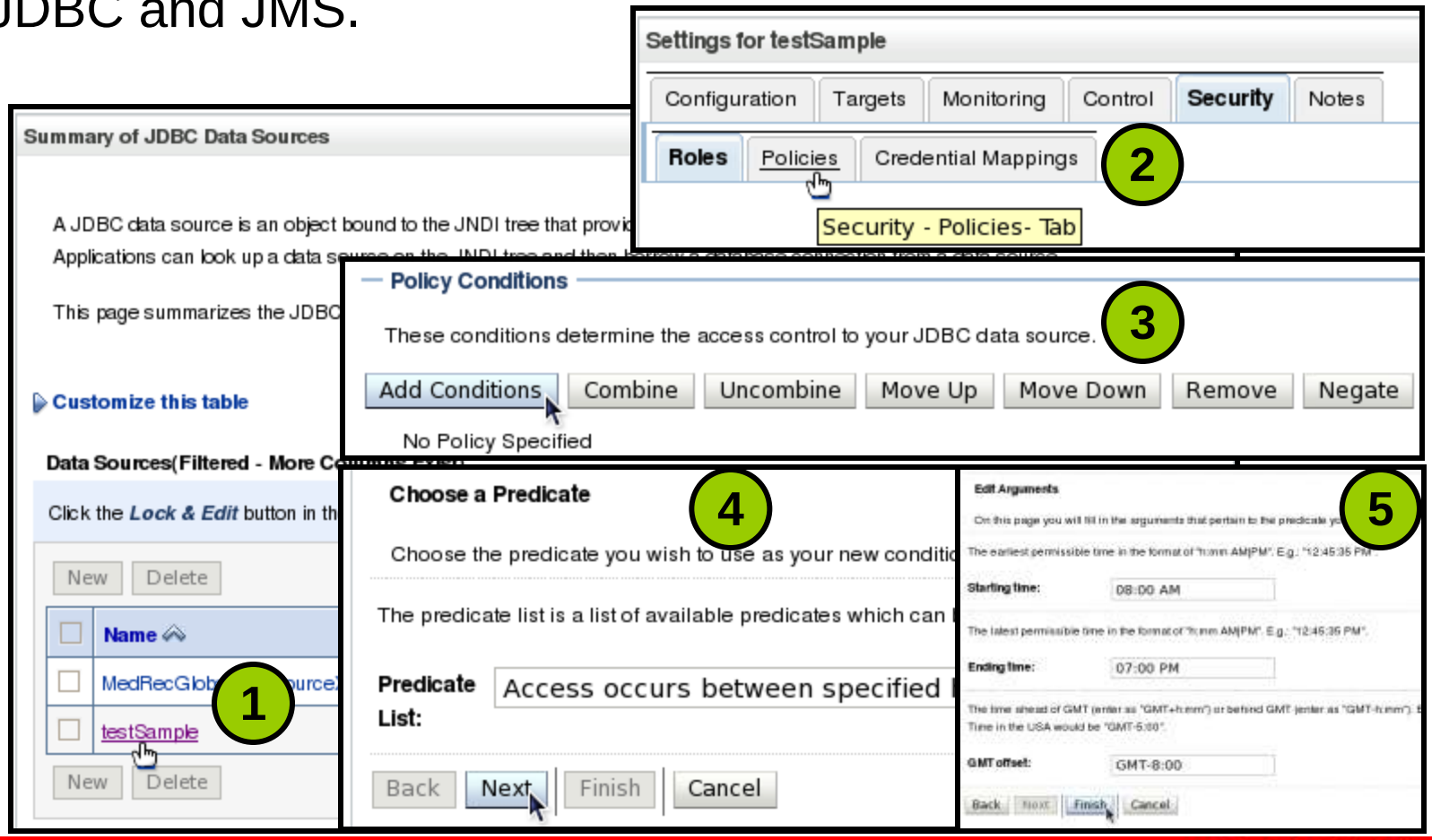


Example URL patterns:

URL Pattern	Role Name
`/*`	Some role name (for example, director)
`/*.jsp`	employee
`/EastCoast/*`	east-coaster

Defining Policies and Roles for Other Resources

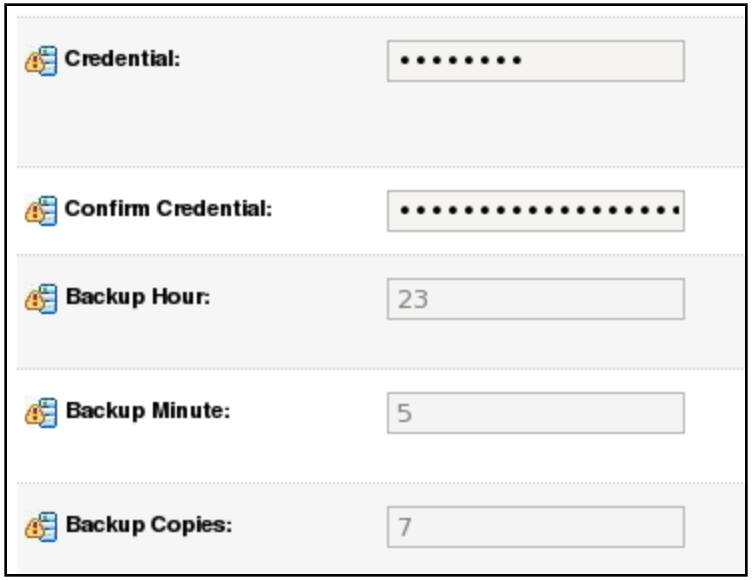
You can define roles and policies for other resources, such as JDBC and JMS.

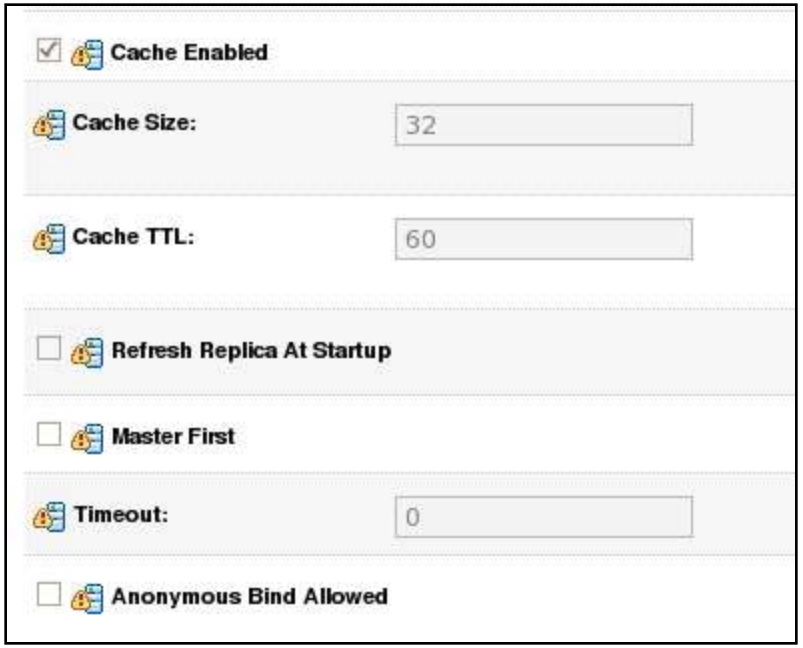


Embedded LDAP Server

- In WLS, users, groups, and authorization information are stored in an embedded LDAP server.
- Several properties can be set to manage the LDAP server, including:
  - Credentials
  - Backup settings
  - Cache settings
  - Replication settings

Configuring an Embedded LDAP





Configuring Authentication

Configure how a Web application determines the security credentials of users:

- `BASIC`: The Web browser displays a dialog box.
- `FORM`: Use a custom HTML form.
- `CLIENT-CERT`: Request a client certificate.

Configure the authentication using the `<login-config>` element:

```
<login-config>
   <auth-method>BASIC, FORM, or CLIENT-CERT</auth-method>
<form-login-config>
      <form-login-page>login.jsp</form-login-page>
      <form-error-page>badLogin.jsp</form-error-page>
   </form-login-config>
</login-config>
```

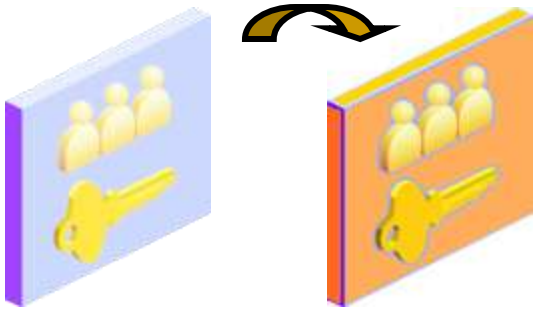
Authentication Examples

BASIC authentication

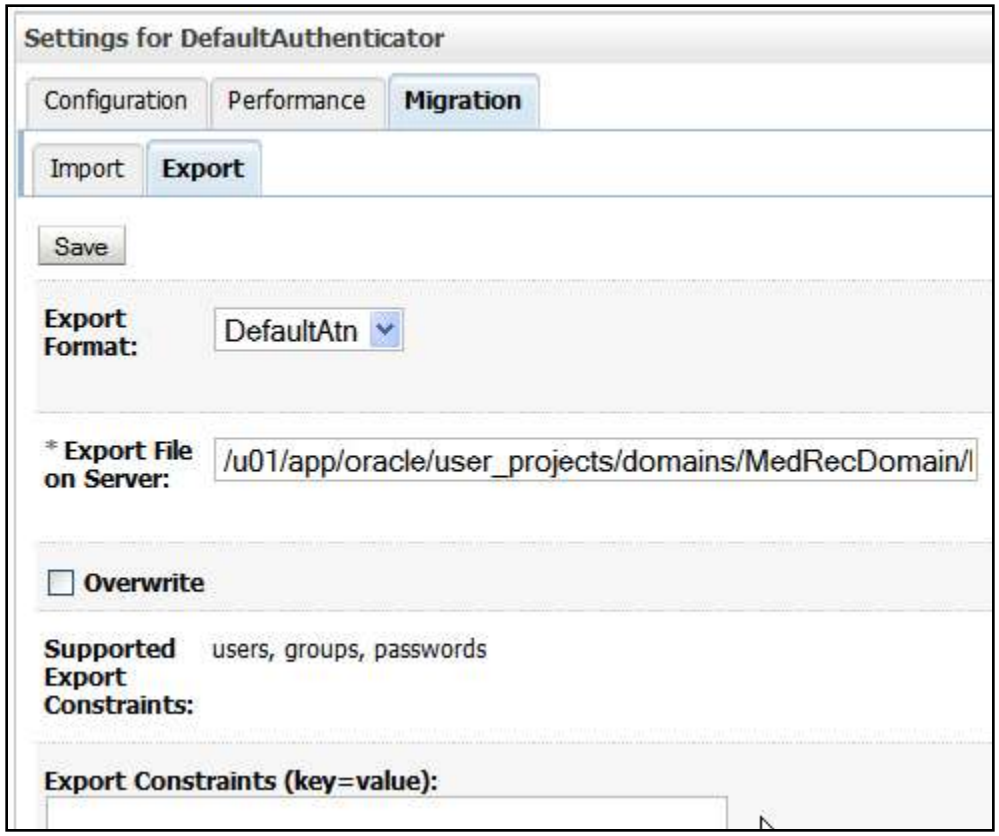
FORM-based authentication

Migrating Security Data

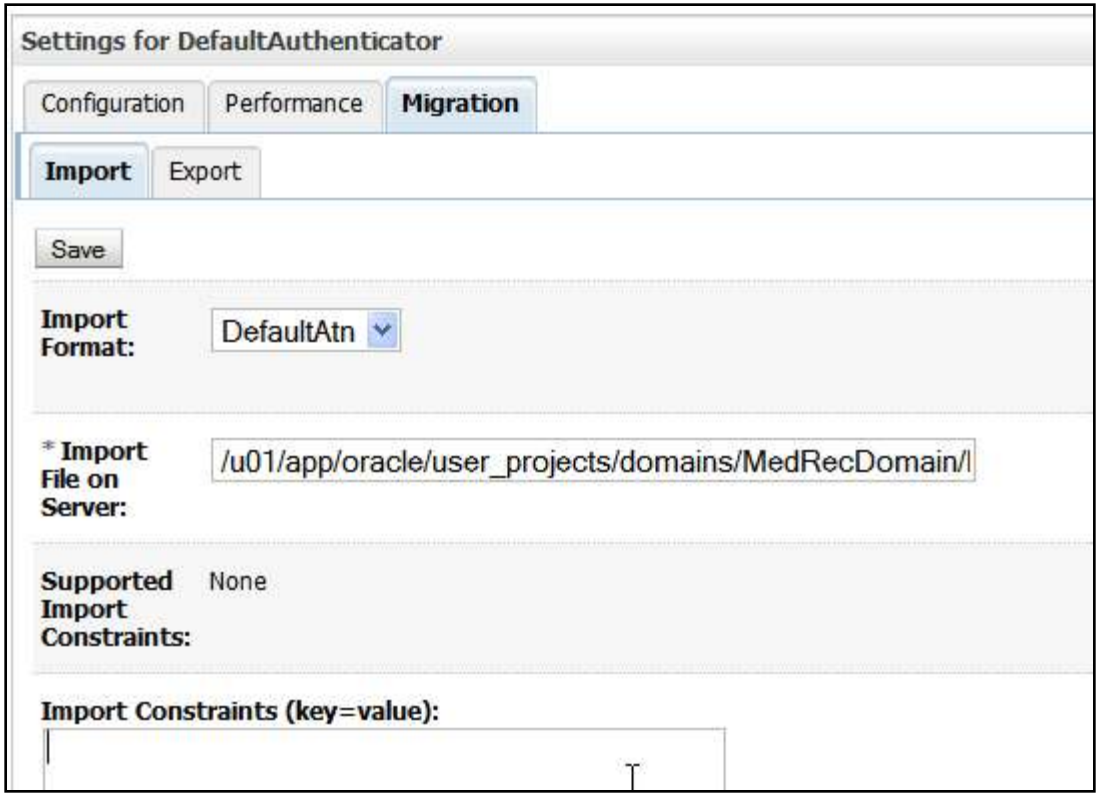
- You can export users and groups, security policies, security roles, or credential maps between security realms or domains.
- It is useful, for example, in transitioning from development to QA to production.
- You can use migration constraints (key/value pairs) to specify the export/import options.
- Currently, the system supports migrating only security data between the WLS security providers.



Exporting the WLS Default Authenticator Provider



Importing into a Different Domain



Summary

In this lesson, you should have learned how to:

- Use the WLS security architecture
- Configure users, groups, and roles
- Configure roles
- Configure policies
- Configure protection for:
  - Web application resources
  - EJBs
- Configure security realms

Practice 18: Overview
Configuring Security for WLS Resources

This practice covers the following topics:

- Creating new users using the Administration Console
- Creating groups of employees and managers
- Assigning groups to users
- Configuring groups-to-role mapping
- Defining resources that are protected by the security you have configured
- Verifying that the security protection that you enabled is working