Preface

The guide walks you through an installation of Oracle Entitlements Server and demonstrates how it can be used to secure an application.

Note: Oracle Entitlements Server was previously known as BEA Aqualogic Enterprise Security. Some items, such as schema objects, paths, and so on may still use the term “ALES."

The document is organized as follows:

- “Overview” on page 1-1 gives an overview of the tutorials, describes the use-case scenario, and lists preliminary requirements.
- “Tutorial 1: Installing Oracle Entitlements Server” on page 2-1 describes how to install the Oracle Entitlements Server and launch the Entitlements Administration Application.
- “Tutorial 2: Defining an Organization and Identities” on page 3-1 shows how to create an organization to represent a business entity. It also shows how to create identities (users and groups) belonging to the organization.
- “Tutorial 3: Creating an Application and Resources” on page 4-1 demonstrates how to define an application that represents the actual application to be secured. It also shows how to define elements used in policy definitions, including resources, actions, and application roles.
- “Tutorial 4: Creating Authorization Policies” on page 5-1 leads you through the creation of two authorization policies that grant access to application resources.

- "Tutorial 5: Creating a Role Policy" on page 6-1 shows how to create a policy that assigns a role to a group of users.
- "Tutorial 6: Generating Policy Reports" on page 7-1 shows how to generate policy reports to audit and verify the policies in place.

CHAPTER 1

Overview

- This section contains the following topics:
- “Scenario” on page 1-1
- “Requirements” on page 1-1

Scenario

This document provides six tutorials that collectively demonstrate some of the basic steps involved in securing applications using Oracle Entitlements Server.

The tutorials address a simple, yet realistic use-case scenario. The Admissions Department at Parker Hospital maintains a web-based patient roster that provides information about currently admitted patients. The patient roster will be secured by policies that control who may access it, under what conditions, and what rights they have when they do so.

In successive steps the tutorials demonstrate how to install the Administration Server, launch the Entitlements Administration Application, and use it to define the security policies that secure the patient roster.

Requirements

In order to follow the tutorials, you must first install a supported servlet container and database.

Servlet Containers:

– WebLogic Server 10.0 MP1 or 9.2 MP2

- Apache Tomcat 5.5.23

Databases:

- Oracle 9.2.0.5, 10.1.2, 10.2.0.2, 11.1.06
- Sybase 12.5.3, 15
- MS-SQL 2000 & 2005 (with MS-SQL 2005 driver)

  Note: MS-SQL 2000 driver is not supported.
- PointBase 5.1
- IBM DB2 Universal DB Enterprise Server 9.1

For detailed information about supported products, see the Administration Server Installation Guide.

Tutorial 1: Installing Oracle Entitlements Server

This section contains the following topics:

Overview

This tutorial walks you through installation of the OES Administration Server. At the completion of this task, you'll be able to start the server and launch the Entitlements Administration Application.

Note: In order to follow the steps in this tutorial, you must have already installed the application server and the database.

After installing the database used as the policy store, you must add a user account that is needed to run the Administration Server installation program. This is performed with tool that is downloadable from the OTN site.

Run the Database Configuration Tool

After obtaining the tool, perform the following steps:

1. Unzip the file.

   The script file name is `OES10gR3_DBConfigTool_win32.zip` (Windows) or `OES10gR3_DBConfigTool_unix.zip` (UNIX and Linux).

2. Open `DBConfig.bat|sh` in an editor and set the following properties:
   - JAVA-HOME — specify the fully-qualified path to a JDK.
   - INSTALL_HOME — specify the fully-qualified path to the directory where you unzipped the file.
   - DB_JDBC_DRIVER_LOC — For Pointbase and MSSQL, specify the fully-qualified path to the JDBC driver. (This is not required for Oracle or Sybase databases.) Examples:

     (Pointbase) `C:\bea\weblogic92\common\eval\pointbase\lib\pbclient.jar`

     (MS-SQL) `C:\Program Files\Microsoft SQL Server 2005 JDBC Driver\sqljdbc_1.2\enu\sqljdbc.jar`

3. Enter `dbconfig.bat` or `dbconfig.sh` on a command line. The program issues a number of prompts to answer.

4. Respond to the prompts as described in the table below:

Prompt	Description
Please input DB type<oracle|sybase|mssql|pointbase>	Enter one of the database names listed.
Please input JDBC URL	Enter the JDBC URL for the database server. Oracle—jdbc:oracle:thin:@<**server**>:<**port**>:<**sid**> Sybase— jdbc:sybase:Tds:<**server**>:<**port**> Sql Server— jdbc:sqlserver://<**server**>:<**port**> Pointbase—jdbc:pointbase:server://<**server**>/ales <**server**>—name or IP address of database machine <**port**>—port where the database listener is running <**sid**>—database SID of Oracle database

Please input JDBC Driver	Enter the JDBC driver used to connect to the database. Oracle—oracle.jdbc.driver.OracleDriver Sybase—com.sybase.jdbc3.jdbc.SybDriver Sql—com.microsoft.jdbc.sqlserver.SQLServerDriver Pointbase—com.pointbase.jdbc.jdbcUniversalDriver
Enter new database user name	Enter a username for the account being created.
Enter new database user password Confirm new database user password	Enter and confirm a password for the new user.
Please input database admin username (not required for Pointbase)	Enter the database administrator user name.
Please input database admin password (not required for Pointbase)	Enter the database administrator password.

5. The script runs and displays messages like the following:

```
-- Configuring table space [ales_oracle]
** Tablespace [ales_oracle] exists in DB server. Continuing with
the same.
-- Creating new user [ales_db_admin] .......Done
-- Configuring ALES role [asi_role]
-- Assigning privs to ALES role .......Done
-- Assigning privs to new user [ales_db_admin].......Done
-- Closing down connection
-- Successfully created ALES Database Account --
```

At the completion of these steps, you may install the Administration Server. See the next section for instructions.

Install the Administration Server

1. Start the installation program using one of the options described below:

Platform	Command
Windows	`OES10gR3_admin_win32.exe`

Sun Solaris	1. Change the protection on the install file by entering: `chmod u+x oes10gR3_admin_solaris32.bin` 2. Enter: `./oes10gR3_admin_solaris32.bin`
Red Hat	1. Change the protection on the install file by entering: `chmod u+x oes10gR3_admin_linux32.bin` 2. Enter: `./oes10gR3_admin_linux32.bin`

2. On the **Welcome** window, click **Next**.
3. On the **Choose BEA Home Directory**, select the directory containing the application server and click **Next**.
4. On the **Choose Product Installation Directories**, accept the default and click **Next**.
5. On the **Choose Service Control Manager Directory**, accept the default and click **Next**.
6. On the **Choose Application Server**, select the application server you are using (WebLogic or Tomcat) and then specify the web server directory and click **Next**.

   WARNING: When using Tomcat, the directory name cannot contain spaces.
7. On the **Choose Network Interfaces** window, accept the default and click **Next**.
8. On the **Configure Administration Application** window, accept the default and click **Next**.
9. On the **Configure Database Connection**, select your database type from the **Database client** dropdown list. Then complete the following fields and click **Next**.

   JDBC URL—Replace the bracketed values. These vary by database type:

   <SERVER>—name/IP address of the database machine
   <PORT>—port number where the database listener is running
   <INSTANCE>—instance name to connect to on <server>
   <SID>—database SID of Oracle database

   JDBC driver—Accept the default

   Driver location—If required, browse to and select the driver location.

   Login ID—user created using the database setup script described in "Run the Database Configuration Tool" on page 2-1.

   Install Schema—make sure the checkbox is selected.

10. On the **Key Protection Password Selection** window, select **Generate Random Password** and click **Next**.

    The program takes several minutes to install the files and displays a status bar showing progress.

11. On the **Choose JDK** window, select the default and click **Next**.

12. On the **Installation Complete** window, click **Done**. This page indicates the Administration Server completed successfully.

    A command window will open and notices about server starts and the schema addition will appear. This may take 5 minutes or more.

13. When prompted, press **Enter** to close the window.

    The Administration Server should now be running.

Starting the Server

If you just finished installing the server as described above, the server should already be running and you can launch the Entitlements Administration Application as described in the next section. Otherwise, to start the server on Windows:

1. From the Windows Start Menu, select **Programs** > Oracle Entitlements Server > **Administration Server** > **Start Server**.

   This opens a DOS box that gives information about the start process, which can take several minutes. When the server starts, a message like the following appears:

   ```
   The OES WLS.<server_name> service was started successfully.
   ```

Launch the Entitlements Administration Application

To launch the Entitlements Administration Application:

1. Open Internet Explorer and go to `https://<servername>:7010/entitlementsadministration` where `<servername>` is the server name.

   When you see a message about the security certificate being used, click **Yes** to display the the log on window.

2. Complete the **Username** and **Password** field and click **Login** to access the Entitlements Administration Application's main window.

Note: The default admin username and password is *admin* and *password* respectively.

Summary

This tutorial walked you through a basic installation of the Administration Server and showed how to start the server and launch the Entitlements Administration Application.

CHAPTER 3

Tutorial 2: Defining an Organization and Identities

This section contains the following topics:

Overview

The first steps in defining policies are to (1) create an organization under which the application to be secured will be defined and (2) define identities (users and groups) to represent application users. Once users and groups are created, they be granted access to application resources.

Scenario

This section walks you through the steps of creating the organization and identities needed to represent employees of Parker Hospital who use the Admissions System's patient roster. These are described in Table 3-1.

Table 3-1 Organization and Identities

Object	Description
Organization	**ParkerHospital** is created to hold all Parker Hospital identities and applications.
Identity Directory	The **Parker_Identities** directory is created to contain all Parker Hospital employees (users) as well as any groups needed to define user collections.
Users	**John Kildaire** — A doctor who requires *view* access to the Admissions System's patient roster. **Harry Hopkins** — An Admissions System operator who manages the patient roster. He requires *view* and *edit* access.
Groups	**Doctors** — a group to contain all doctors at Parker Hospital. **AdmissionsOperators** — a group to contain all Admissions System operators.

Create the Organization

1. If you have not already done so, start the Oracle Entitlements Server and launch the Entitlements Administration Application as described inthe previous chapter.
2. In the left pane of the console window, select the **RootOrg** organization and click **New Organization** at the bottom of the pane.

Tip: When you expand **RootOrg**, you will see two out-of-box entities: the **EntitlementUI** application and a child organization named **DefaultOrg**. The **EntitlementUI** application represents the Entitlements Administration Application itself and the **DefaultOrg** organization contains a number of out-of-box resources and any resources created in previous versions of this product. For further information about these objects, see Entitlements Administration Application help system.

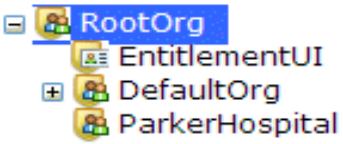
---

3. On the **New Organization** dialog, enter `ParkerHospital` in the **Name** field and click **OK**.

   Note that spaces are not allowed in organization names.

   As shown in Figure 3-1, the **ParkerHospital** organization will appear in the navigation tree under **RootOrg**.

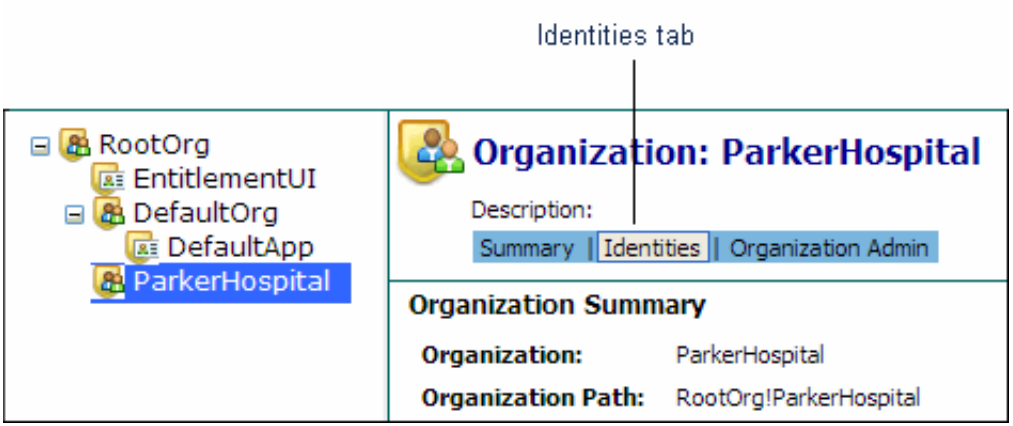
Figure 3-1 ParkerHospital Organization



Create the Identity Directory

1. In the left pane, select the **ParkerHospital** organization. Then click the **Identities** tab in the right pane as shown in Figure 3-2.

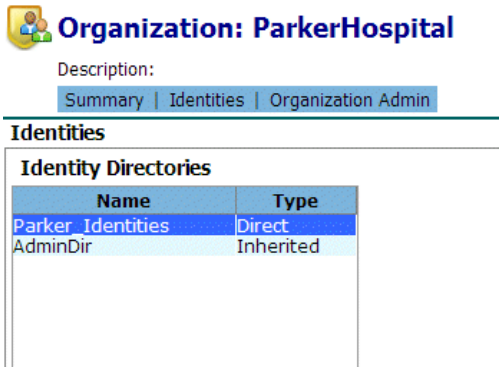
Figure 3-2 Identities tab



2. Click **New** at the bottom of the right pane. When the **New Identity Directory** dialog appears, enter `Parker_Identities` and click **OK**.

As shown in Figure 3-3, the identity directory will appear in the **Identities Directory** list and the **Type** column will indicate it is a direct child of the ParkerHospital organization.

Figure 3-3 Creating Identities

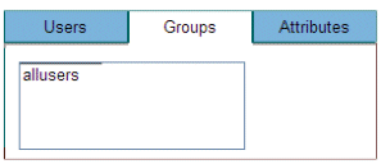


Create the Groups

1. With the **Parker_Identities** directory selected in the Identities Directories list, select the **Groups** tab on the right.

   As shown in Figure 3-4, the **Groups** tab lists the **allusers** group, which is an automatically provided group that contains all users in the Parker_Identities directory.

Figure 3-4 Groups Tab



2. To create the **Doctors** group, select **New** at the bottom of the tab. Then enter `Doctors` in the **Group Name** field and click **OK**.
3. Repeat step 2 to create a group named **AdmissionsOperators**.

   After both groups are created, they will appear in groups list as shown in Figure 3-5.

Figure 3-5 Groups in Parker_Identities Directory

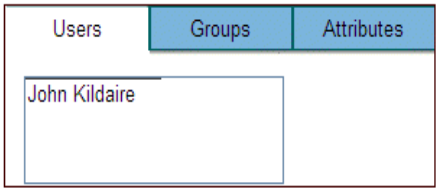
Create the Users

1. With the **Parker_Identities** directory selected in the Identities Directories list, select the **Users** tab on the right and click **New** at the bottom of the tab.
2. When the **New User** dialog appears, enter `John Kildaire` in the **User Name** field and complete the two password fields using any string of at least six characters and click **OK**.

   Note: The password value is unimportant; it will not be used in these tutorials.

   John Kildaire will appear in the **Users** list as shown in Figure 3-6.

Figure 3-6 User John Kildaire



3. Add John Kildaire to the **Doctors** group.
4. Repeat steps to create a user named **Harry Hopkins** and assign it to the **AdmissionsOperators** group.

Save Your Work

After creating the organization and identities, save your changes as follows:

1. In the top right part of the console window, click **Save & Distribute** as shown in Figure 3-7.

Figure 3-7 Save Changes

2. On the **Save and Distribute** window, make sure **No, just save changes** is selected and click **OK**.

   Note: The **Yes, save changes and distribute** option is used when you have made changes to policy definitions. Selecting it will save your changes and also distribute the policies to the SSM that is securing the application.

3. To turn on autosave so that changes will be automatically saved, click the **Auto Save** checkbox on the main menu as shown in Figure 3-8.

Figure 3-8 Autosave

Summary

This tutorial showed how to create the following objects:

- Organization — ParkerHospital was created to hold all employees at Parker Hospital.
- Identity Directory — Parker_Identities was created to hold all Parker Hospital users and groups.
- Groups — The Doctors and AdmissionsOperators groups were created to contain all doctors and operators who access the patient roster.
- Users — John Kildaire was created and added to the Doctors group. Harry Hopkins was created and added to the AdmissionsOperators group. These users access the Admissions System's patient roster.

CHAPTER 4

Tutorial 3: Creating an Application and Resources

This section contains the following sections:

Overview

In order to secure an application using Oracle Entitlements Server, the application must be defined using the Entitlements Administration Application. Once the application is defined, you can specify the application resources to which you want to assign policies, actions that may be performed on these resources, application roles that may be granted access to the resources, and policy definitions that are enforced when users access the secured application.

Scenario

This tutorial leads you through the steps of creating an application named AdmissionsSystem and the resources, actions, and roles as described in Table 4-1.

Table 4-1 Application Objects

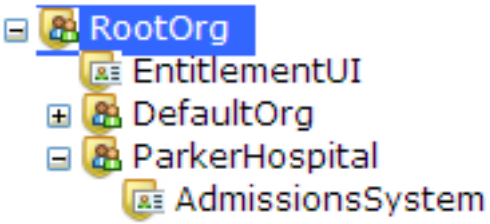
Object	Description
Application	The **AdmisssionsSystem** application contains the web-based patient roster.
Resource	A resource named **url** is created to serve as the parent resource of the patient roster (**roster_index.jsp**).
Resource	A resource named **roster_index.jsp** is created to represent the JSP page in the Admissions System that users access to administer and view the patient roster. In tutorial 4, we will show how to assign policies to this resource so as to determine who may access the roster.
Actions	The following actions that correspond to web-based requests are defined: **GET**, **POST** After defining these actions, they may be used in policy definitions.
Application Role	A application role name **HealthProviders** is created. In tutorial 4, a role policy is used to assign this role to John Kildaire.

Create the Application

1. If you have not already done so, start the Administration Server and launch the Entitlements Administration Application.
2. In the left pane, select the **ParkerHospital** organization and click **New Application** at the bottom of the pane.
3. On the **New Application** dialog, enter `AdmissionsSystem` in the **Name** field and click **OK**. The **AdmissionsSystem** application appears as a child of the **ParkerHospital** organization as shown in Figure 4-1.

   Note: The **SSM Bound** field is not used in these tutorials. This field is used to bind an application to an SSM.

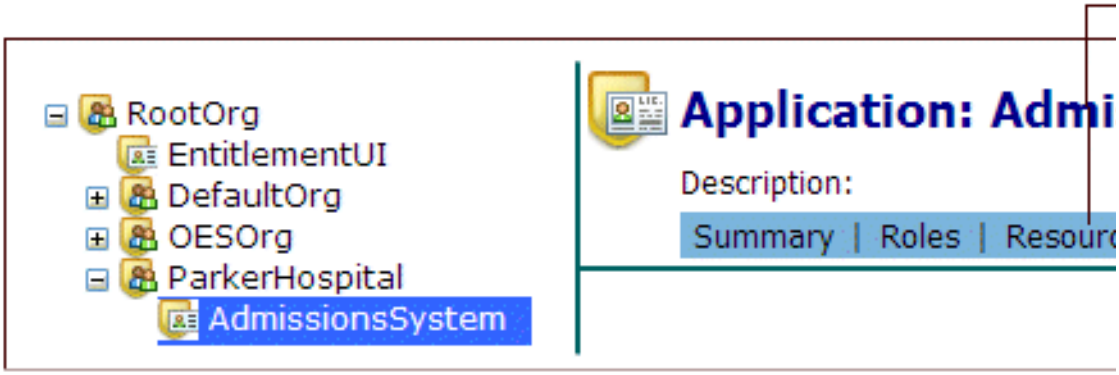
Figure 4-1 AdmissionsSystem Application



Create the Resources

1. Select the **AdmissionsSystem** application in the left pane. Then click on **Resources** in the right pane as shown in Figure 4-2.

Figure 4-2 Selecting Resources

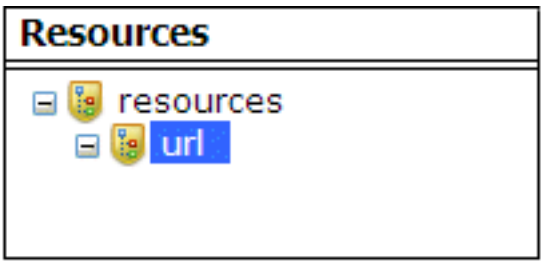


2. On the Resources page, click **New** at the bottom.
3. On the **New Resource** dialog, enter `url` in the **Name** field and click **OK**.

   When you select a resource's **Allow Virtual Resource** field, any policies applied to the resource will also apply to any child resources in the actual application. This dispenses with the need to define these child resources in the Entitlements Administration Application.

   When you click **OK** the **url** resource displays in the resources list as shown in Figure 4-3.

Figure 4-3 URL Resource



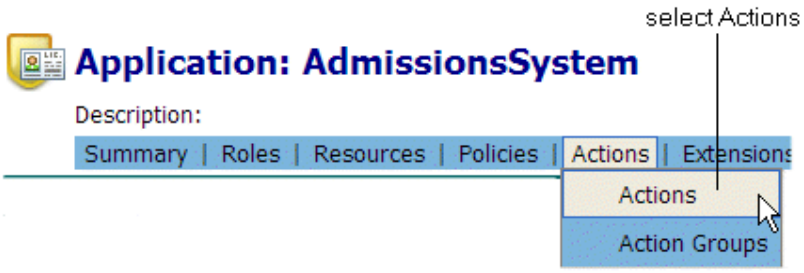
4. Select the **url** resource and click **New** at the bottom of the list.
5. On the **New Resource** dialog, enter `roster_index.jsp` in the **Name** field and click **OK**.

Note: The resource name must be the same as the name of actual application resource.

Create the Actions

1. With the **AdmissionsSystem** application selected in the left pane, click on the **Actions** tab and select the **Actions** sub-menu as shown in Figure 4-4.

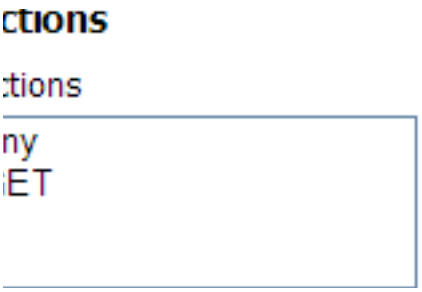
Figure 4-4 Selecting Actions



Tip: You will notice that the **any** action is automatically provided.

2. On the **Actions** page, click **New** at the bottom of the page.
3. On the **New Action** dialog, enter `GET` in the **Name** field and click **OK**. The **GET** action then appears in the list of existing actions as shown in Figure 4-5.

Figure 4-5 Actions List



4. Repeat step 2 to create the **POST** action.

Notes:

- In real situations, many actions could be required to cover the full range of requests made on the secured application. In these cases, it can be useful to manage actions under different action groups. For example, you could create an action group to contain all HTTP-based actions.

Create an Application Role

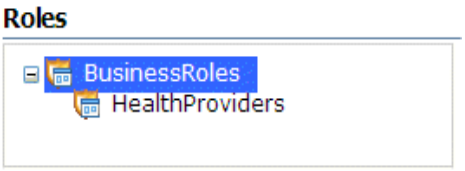
Application roles are distinct from admin roles, which are not covered in this tutorial. For more information, see the Entitlements Administration Application help system.

1. With the **AdmissionsSystem** application selected in the left pane, click on the **Roles** tab.
2. On the **Roles** page, click **New** at the bottom.
3. On the **New Role** dialog, enter `HealthProviders` and click **OK**.

   The **HealthProviders** role appears in the list as shown in Figure 4-6.

Tip: You could assign users or groups to the HealthProviders role by selecting it and clicking New under the list of Role Policies. We also show a different method of accomplishing the same thing in "Tutorial 5: Creating a Role Policy" on page 6-1.

Figure 4-6 HealthProviders Role



Save Your Work

If autosave is not enabled, save your work as follows:

1. Click **Save & Distribute** as shown in Figure 4-7.

Figure 4-7 Save Changes

2. On the **Save and Distribute** window, make sure **No, just save changes** is selected and click **OK**.

   Note: The **Yes, save changes and distribute** option is used when you have made changes to policy definitions. Selecting it saves your changes and also distributes the policies to the SSM securing the application.

Summary

This tutorial showed how to create the following objects:

- Application — The **AdmissionsSystem** application was created to hold the resources, actions, and application roles used to secure access to the patient roster.
- Resources — The **url** and **roster_index.jsp** resources where created so that policies could be applied to **roster_index.jsp**. In the next tutorial, an authorization policy will be used to secure access to **roster_index.jsp**.
- Actions — The **GET** and **POST** actions were created, because these request types are submitted when users access **roster_index.jsp**.
- Application Role — The **HealthProviders** roles was created. In the next tutorial, an authorization policy will grant access to roster_index.jsp to anyone in the **HealthProviders** role. In addition, a role policy in tutorial 5 will assign this role to certain users.

Tutorial 4: Creating Authorization Policies

This section contains the following sections:

Overview

Once the necessary application resources, identities, application roles, and actions are defined, you can make use of them in authorization policies. An authorization policy specifies who can access a resource and what rights (actions) they have when they do so.

Scenario

This tutorial shows how to define two authorization policies that secure access to the patient roster. The policy details are provided in Table 5-1.

Table 5-1 Authorization Policies

Policy	Description
Authorization Policy 1	This policy will allow any user in the **AdmissionsOperators** group to view and edit the patient roster. Since the roster is a JSP page, the required access rights (actions) are *POST* and *GET*. Effect: Grant Actions: GET, POST Subjects: AdmissionsOperators Resources: roster_index.jsp
Authorization Policy 2	This policy allows any user in the **HealthProviders** role to view the roster. Any user assigned to this role will have *view* access. Effect: Grant Actions: GET Subjects: HealthProviders role Resources: roster_index.jsp

Create Authorization Policy 1

This policy will allow any user in the **AdmissionsOperators** group to view and edit the patient roster. Since **Harry Hopkins** is a member of this group, he will be able to manage the roster.

1. Select the **AdmissionsSystem** application in the left pane. Then click on the **Resources** tab as shown in Figure 5-1.

Figure 5-1 Selecting Resource Tab

2. Select the **roster_index.jsp** resource. Then click **New** in the lower right part of the **Authorization Policies** tab.
3. On the **New Authorization Policy** dialog, select the **Grant** radio button and do the following:
   a. On the **Actions** tab, make sure All is selected in the **Select Action Group** field. Then select **POST** and **GET** in the list of **Available Actions** and transfer them to the **Selected Actions** list.
   b. On the **Resources** tab, clear the **resources** checkbox and expand the resources tree. Then select and transfer **roster_index.jsp** to the **Selected Resources** list.
   c. On the **Subjects** tab, select the **Group** radio button and make sure `ParkerIdentities` displays in the **Identity Directories** field. Then select `AdmissionsOperators` in the **Available Subjects** list and transfer it to the **Selected Subjects** list.
4. Click **OK**. The resulting policy will display in the Policies list as shown in Figure 5-2.

Figure 5-2 Authorization Policy 1

Effect	Actions	Resources	Subjects
grant	GET POST	//resources/url/roster_index.jsp	AdmissionsOperators

Create Authorization Policy 2

This policy will allow the **HealthProviders** role to view the patient roster.

1. Picking up from step two in the previous section, make sure the **roster_index.jsp** resource is selected and click **New** to open the **New Authorization Policy** dialog.
2. On the **New Authorization Policy** dialog, select the **Grant** radio button and do the following:
   a. On the **Actions** tab, make sure All is selected in the **Select Action Group** field. Then select **GET** in the list of **Available Actions** and transfer it to the **Selected Actions** list.
   b. On the **Resources** tab, clear the **resources** checkbox and expand the resources tree. Then select and transfer **roster_index.jsp** to the **Selected Resources** list.
   c. On the **Subjects** tab, select the **Role** radio button. Then select the **HealthProviders** role and transfer it to the **Selected Subjects** list.
3. Click **OK**. The resulting policy will display in the **Policies** list as shown in Figure 5-3.

Figure 5-3 Authorization Policy 2

Effect	Actions	Resources	Subjects
grant	GET POST	//resources/url/roster_index.jsp	ROLE:HealthProviders

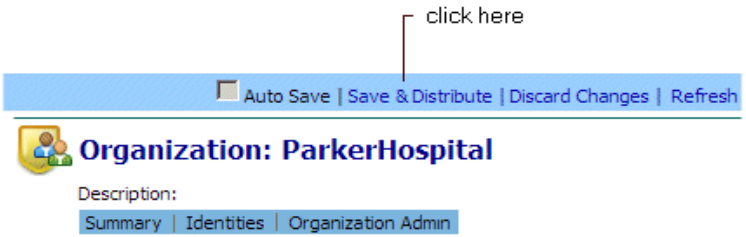
Tip: Note that, by itself, authorization policy 2 does not allow any particular users, because as yet the HealthProviders roles is not assigned to any users or groups. In the next tutorial, this will be accomplished using a role policy.

Save Your Work

If autosave is not enabled, save your work as follows:

1. Click **Save & Distribute** as shown in Figure 5-4.

Figure 5-4 Save Changes



2. On the **Save and Distribute** window, make sure **No, just save changes** is selected and click **OK**.

   Note: In an actual deployment, you could select the **Yes, save changes and distribute** option to both save the role policy and distribute it to the SSM for immediate enforcement in the secured application.

Summary

In this tutorial we defined two authorization policies that restrict access to the patient roster.

- Authorization Policy 1 allows users in the **AdmissionsOperators** group to view and edit the roster. Since Harry Hopkins is a member of this group, he may view and edit the roster.
- Authorization Policy 2 allows the **HealthcareProviders** role to view the roster. Any user assigned to this role will have *view* access.

Tutorial 5: Creating a Role Policy

This section contains the following sections:

Overview

A role policy is essentially a collection of permissions that are granted to users and/or groups who are assigned to the role. It also defines how, when, and under what constraints the role is assigned.

Granting a role to a user or a group confers the defined access privileges as long as the user or group is assigned to the role. Roles are computed and granted to users or groups dynamically at runtime.

Roles can be managed in hierarchies so a user assigned to a parent role also inherits any child roles (so long as this is not prohibited by other policies).

Scenario

This section walks you through the steps of defining a role policy that assigns the **HealthProviders** role to the **Doctors** group for the purpose of granting view access to the

Admissions System's patient roster. All users in the **Doctors** group will have view access to the roster.

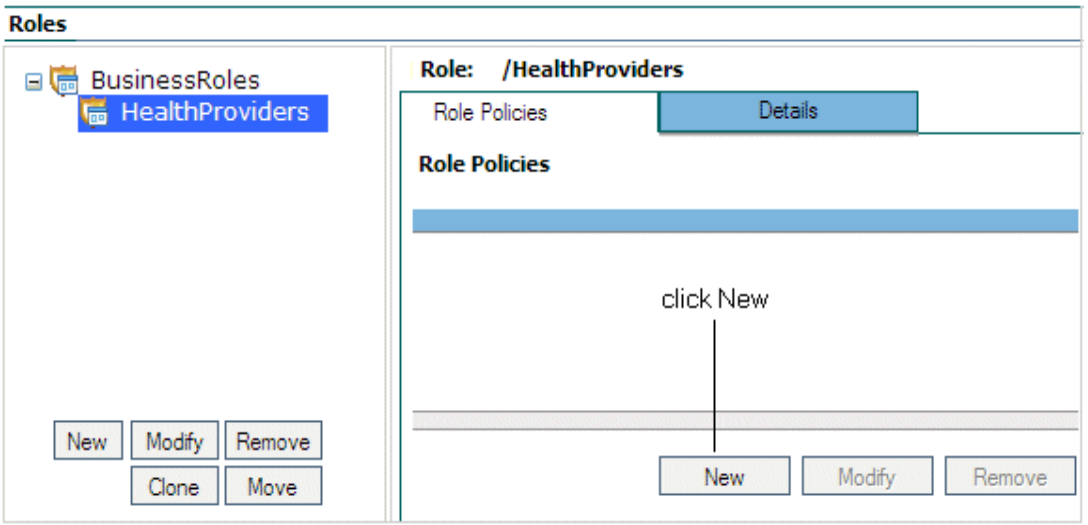
Create the Role Policy

1. With the **AdmissionsSystem** application selected in the left pane, click the **Roles** tab as shown in Figure 6-1.

Figure 6-1 Selecting Role Tab

2. Click **New** at the bottom of the **Role Policies** tab as shown in figure

Figure 6-2 Role Policies Tab



3. On the **New Role Policy** dialog, select the **Grant** radio button and do the following:

   a. On the **Roles** tab, select **HealthProviders** under **Available Roles** and transfer it to the **Select Roles** list.

   b. On the **Resources** tab, clear the **resources** checkbox and expand the resources tree. Then select and transfer **roster_index.jsp** to the **Selected Resources** list.

   c. On the **Subjects** tab, select the **Group** radio button and make sure **Parker_Identities** displays in the **Identity Directories** field. Then select **`Doctors`** in the **Available Subjects** list and transfer it to the **Selected Subjects** list.

4. Click **OK**. The resulting policy will display in the policies list as shown in Figure 6-1.

Figure 6-3 Role Policy

Note: This graphic modified for spacing.

Save Your Work

If autosave is not enabled, save your work as follows:

1. Click **Save & Distribute** as shown in Figure 6-4.

Figure 6-4 Save Changes

2. On the **Save and Distribute** window, make sure **No, just save changes** is selected and click **OK**.

   Note: In an actual deployment, you could select the **Yes, save changes and distribute** option to both save the role policy and distribute it to the SSM for immediate enforcement in the secured application.

Summary

This tutorial showed how to assign a role to a group with the result that all users in the group receive the role.

The next tutorial shows how to build and generate policy reports.

CHAPTER 7

Tutorial 6: Generating Policy Reports

This section contains the following topics:

Overview

This section shows how to generate reports about the policies that were created in tutorials four and five. These reports are described in Table 7-1.

Table 7-1 Policy Reports

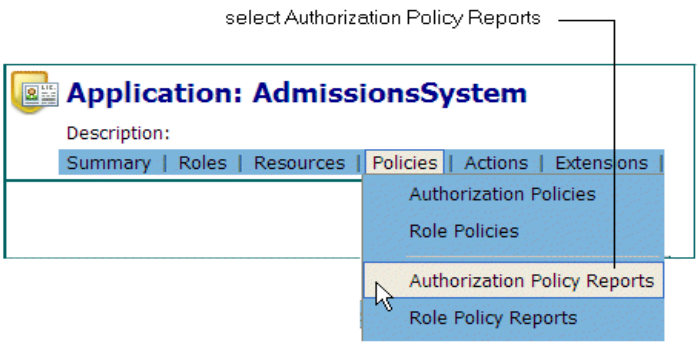
Report Type	Description
Authorization Policy	This report shows rights granted users in the **AdmissionOperators** group. Effect: Grant Subjects: AdmissionsOperators
Role Policy	This report shows John Kildaire's role assignments. Effect: Grant Subjects: John Kildaire

Generate an Authorization Policy Report

This report will show the rights that users in the **AdmissionOperators** group have on any application resource.

1. In the left pane, select the **AdmissionsSystem** application under the **ParkerHospital** organization. Then click on **Policies** in the right pane and select **Authorization Policy Report** in the sub-menu as shown in Figure 7-1.

Figure 7-1 Select Authorization Policy Reports



2. On the **Authorization Policy Report** page, click **Build Query**.
3. On the **Build Authorization Policy Report** dialog:
   a. In the **Effect** field, select the **Grant** radio-button.
   b. On the **Subjects** tab's **Select Policy Subjects From** field, select the **Group** radio-button. Then select the **AdmissionsOperators** group and move it to the **Selected Subjects** field.
   c. Click **OK**.
4. When you are returned to the authorization policy report page, run the report by clicking **Generate Report**.

   The report results show that users in the **AdmissionsOperators** group have both GET and POST rights on the patient roster.

Generate a Role Policy Report

This report will show John Kildaire's assigned roles.

1. In the left pane, select the **AdmissionsSystem** application under the **ParkerHospital** organization. Then click on **Policies** in the right pane and select **Role Policy Reports** in the sub-menu as shown in Figure 7-2.

Figure 7-2 Select Role Policy Reports

2. On the **Role Policy Report** page, click **Build Query**.
3. On the **Query** dialog, make sure the **Grant** radio-button is selected.
4. On the **Subjects** tab, select the **User** radio button. Then select **John Kildaire** in the **Available Subjects** field and transfer it to the **Selected Subjects** field and click **OK**.
5. When you return to the role policy report page, click **Generate Report**.

   As shown in Figure 7-3, the report results show that **HealthProviders** is John Kildaire's only role assignment.

Figure 7-3 Role Policy Report

Effect	Roles	Resources	Subjects
grant	ROLE:HealthProviders	//resources/url/roster_index.jsp	USER:RootOrg!ParkerHospital!Parker_Identities:John Kildaire