Securing Web Applications by HTTP Basic Authentication

SDN Community Contribution

(This is not an official SAP document.)

Disclaimer & Liability Notice

This document may discuss sample coding or other information that does not include SAP official interfaces and therefore is not supported by SAP. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing the information, code or methods suggested in this document, and anyone using these methods does so at his/her own risk.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of this technical article or code sample, including any liability resulting from incompatibility between the content within this document and the materials and services offered by SAP. You agree that you will not hold, or seek to hold, SAP responsible or liable with respect to the content of this document.

Securing Web Applications by HTTP Basic Authentication

Applies To:

SAP J2EE Engine 6.40

Summary

Authentication is a mechanism for securing web applications by determining a user's identity before granting that user access to application resources. The J2EE specification defines four compulsory schemes for web application user's authentication. This article describes the step-by-step approach for using the basic authentication scheme in the web application.

By: Manish Chaitanya

Title: Consultant, International Consulting Group, SAP India

Date: 05 Apr 2005

Table of Contents

Introduction

Authentication is a mechanism for securing web applications by determining a user's identity before granting that user access to application resources. The J2EE specification defines four compulsory schemes for web application user authentication:

a. BASIC – Done by entering a username and password in the browser-generated input screen.
b. FORM – Username and password-based authentication. The application must provide the form page that requires the user's input.
c. DIGEST – Similar to the BASIC scheme; this does not send the username and password as is, but rather uses a checksum.
d. CLIENT-CERT – Authentication is performed using digital certificates.

We can use each of these standard authentication schemes to protect our web applications. They are part of the J2EE engine implementation. This article outlines the steps required for configuring the web applications to make use of the BASIC authentication mechanism. For the example in this article I assume that the application uses the **UME User Store** for authentication.

There are two major parts to the configurations to be followed:

a. Configurations required in the web application.
b. Configurations required in the J2EE engine.

Required Web Application Configuration

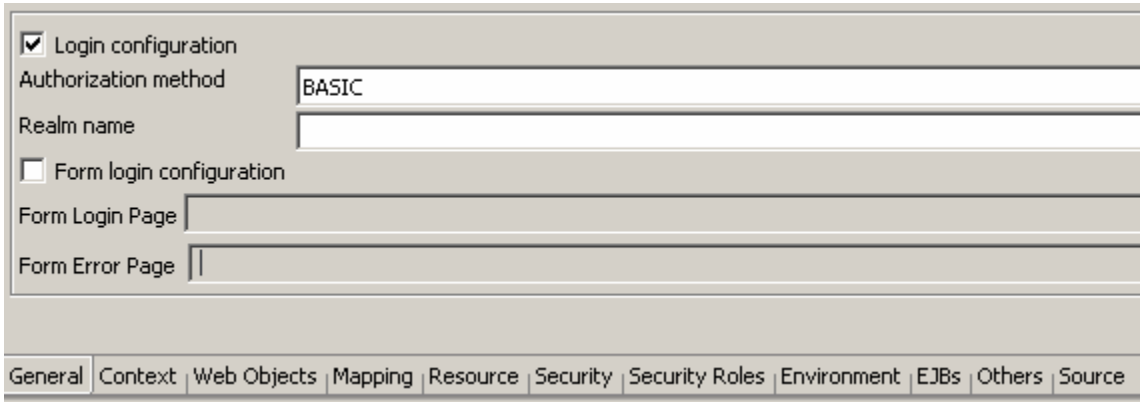
Configuring the web application requires changes in the two XML files web.xml and web-j2ee-engine.xml.

Changes to "web.xml"

Open the web application project in the SAP NetWeaver Developer Studio (NWDS) and double-click on the web.xml file.

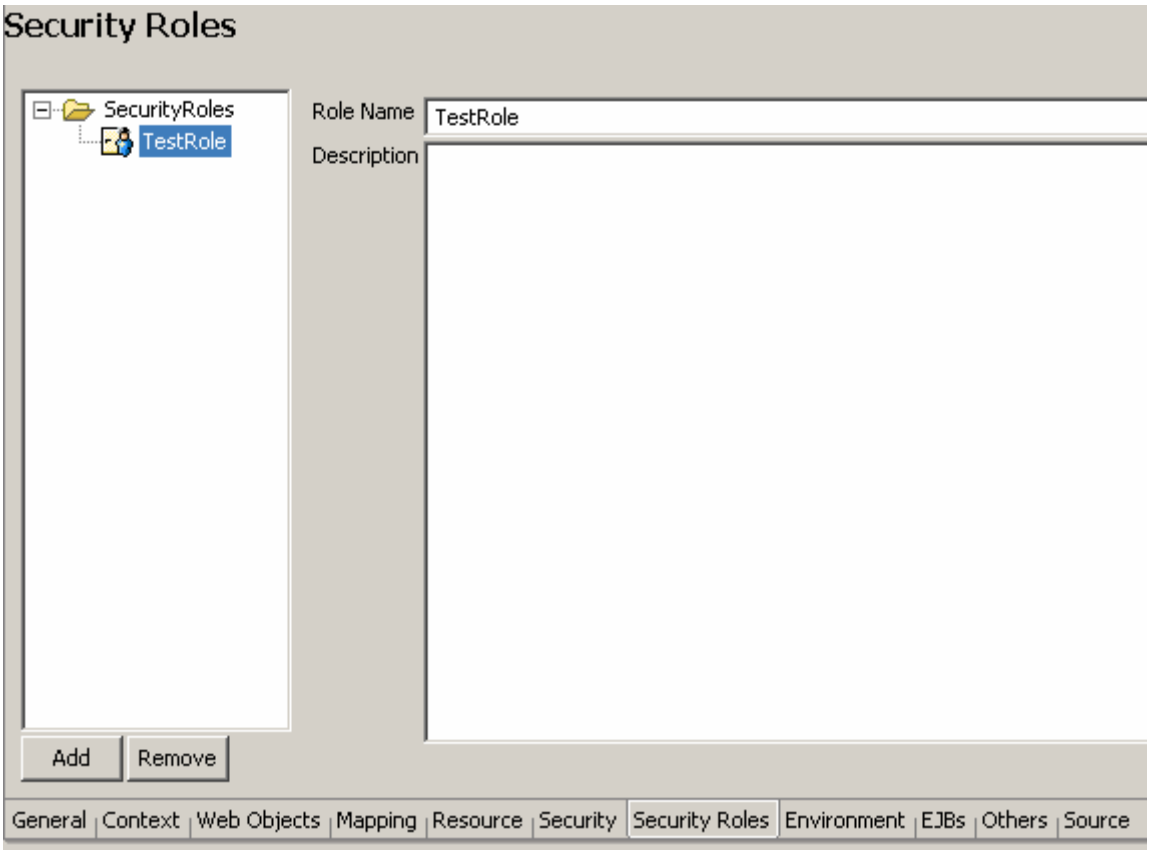
Select the BASIC Authentication Mechanism

In the General tab check the "Login Configuration" checkbox and select BASIC from the drop-down for "Authorization method" field.



Defining a Security Role for the Web Application

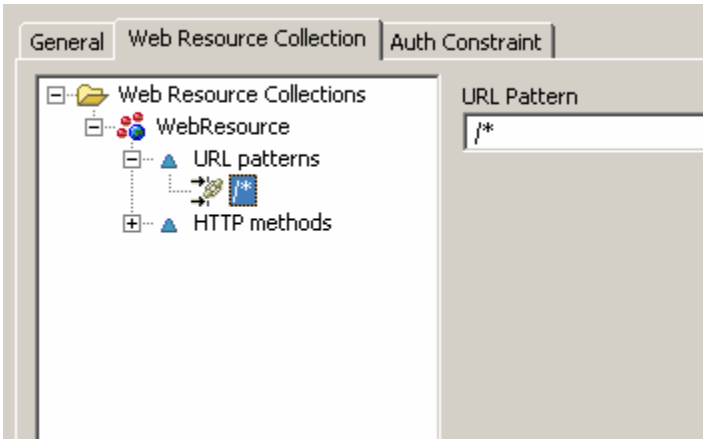
Click on the Security Roles tab and enter a security role name that will be mapped to a role created on the UME User Store.



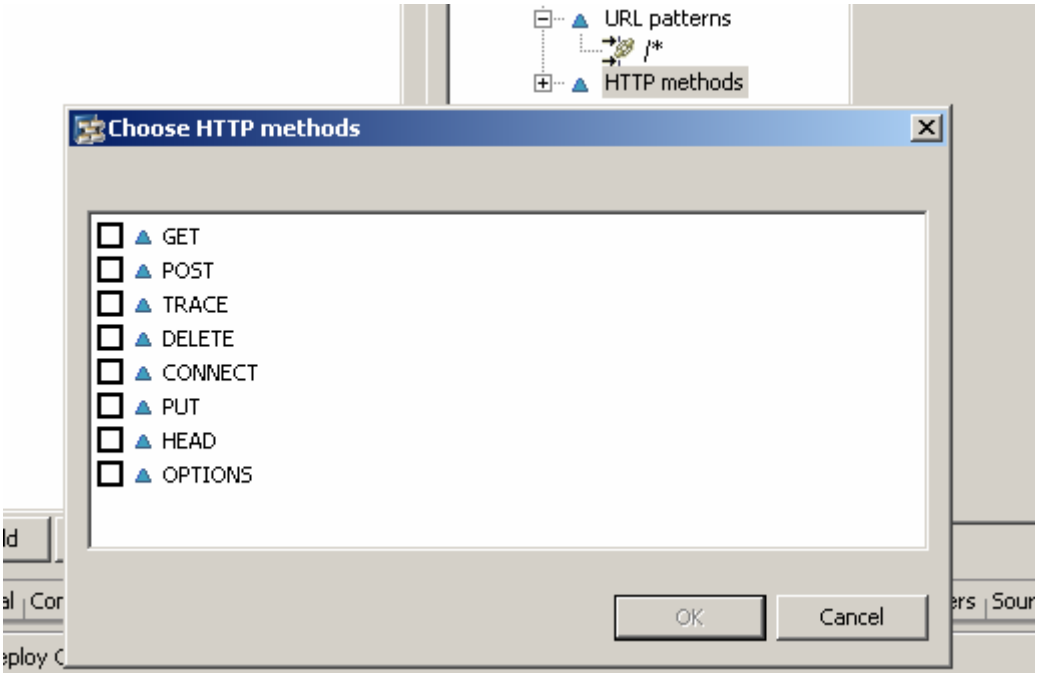
Save the project.

Selecting the URL Patterns and HTTP Methods to Protect

Now, click on the Security tab. Select the Security Constraints node and click on Add. In the General tab on the right-hand side, leave the default Display Name. Under Web Resource Collection select “URL patterns” and click on Add. Change "*" to "/*" to protect the entire application.



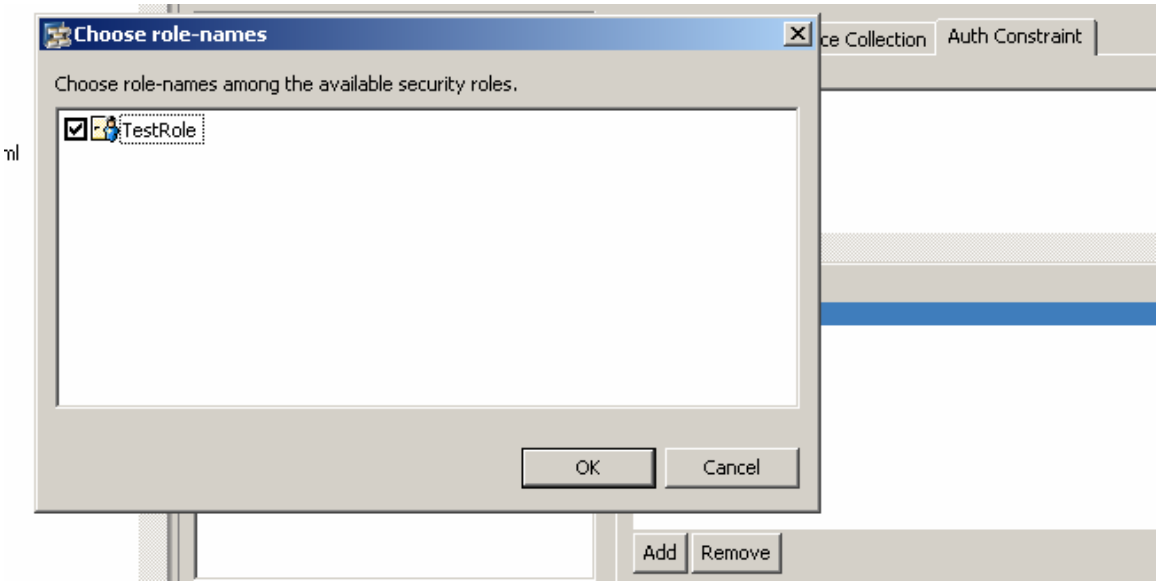
Select “HTTP methods” and click on Add.



Choose the HTTP methods you want to protect and click OK.

Defining Which Roles Have Access to this Application

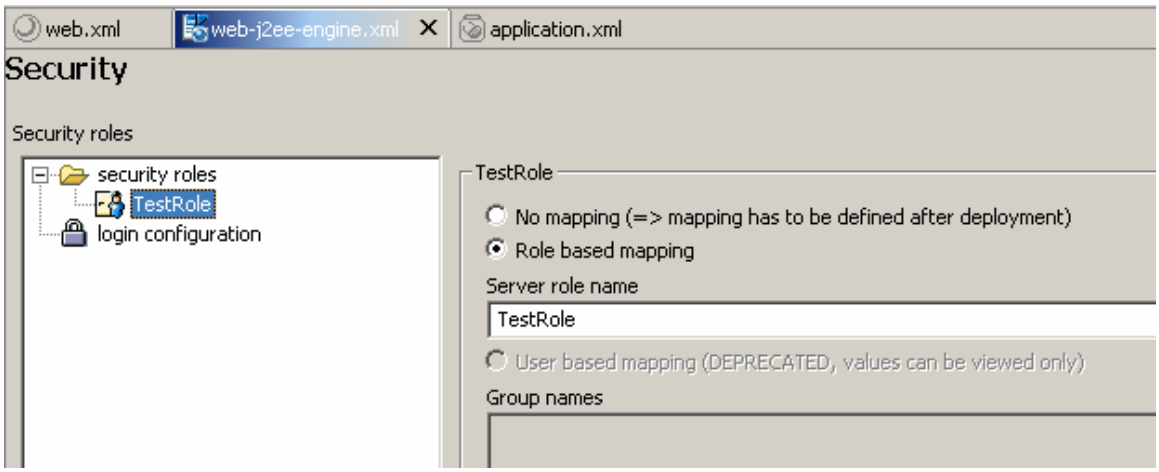
Go to the Auth Constraint tab and click on Add. From the list select the role(s) that you want to be able to access this application and select OK.



Save the project.

Changes to "web-j2ee-engine.xml"

Open the web-j2ee-engine.xml file by double clicking on it in the J2EE Explorer and click on the Security tab. Expand the “security roles” and select the role that was created in the above step.



Choose “Role based mapping” and provide a name for a server role. This name can be different from the name that was created above in the web application.

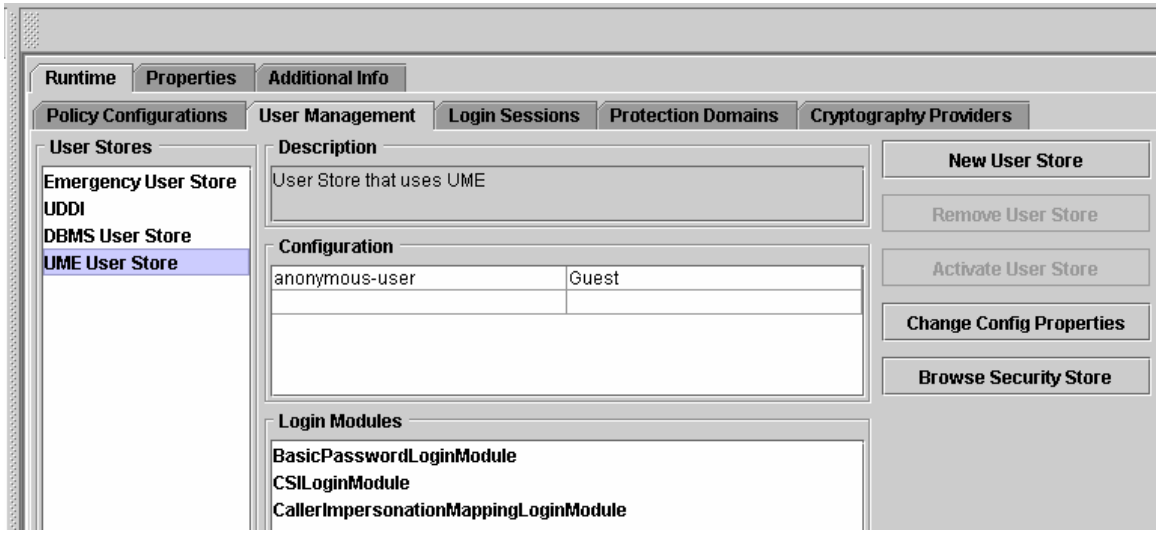
Save project, create the web and enterprise archives, and deploy the application on the SAP J2EE Engine.

Required J2EE Engine Configuration

Roles and users can be created in the UME User Store using the Visual Administrator for the SAP J2EE Engine. For this example we will assume that no users and roles are already created so we’ll create the users and roles using the visual admin.

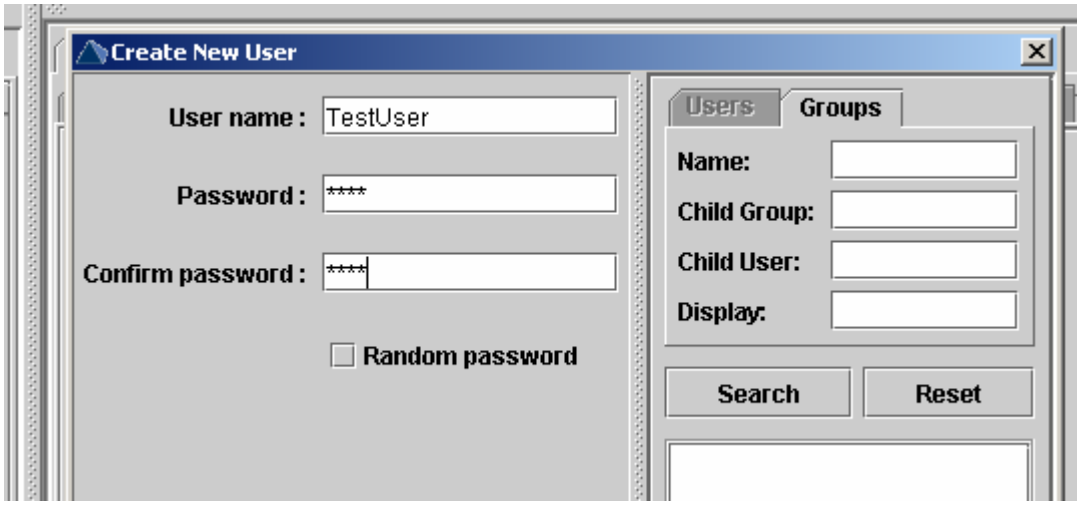
Creating the User

In the Visual Admin go to Cluster -> Services -> Security Provider service and click on Runtime -> User Management tab. The following screen appears:



Select UME User Store and click on Browse Security Store.

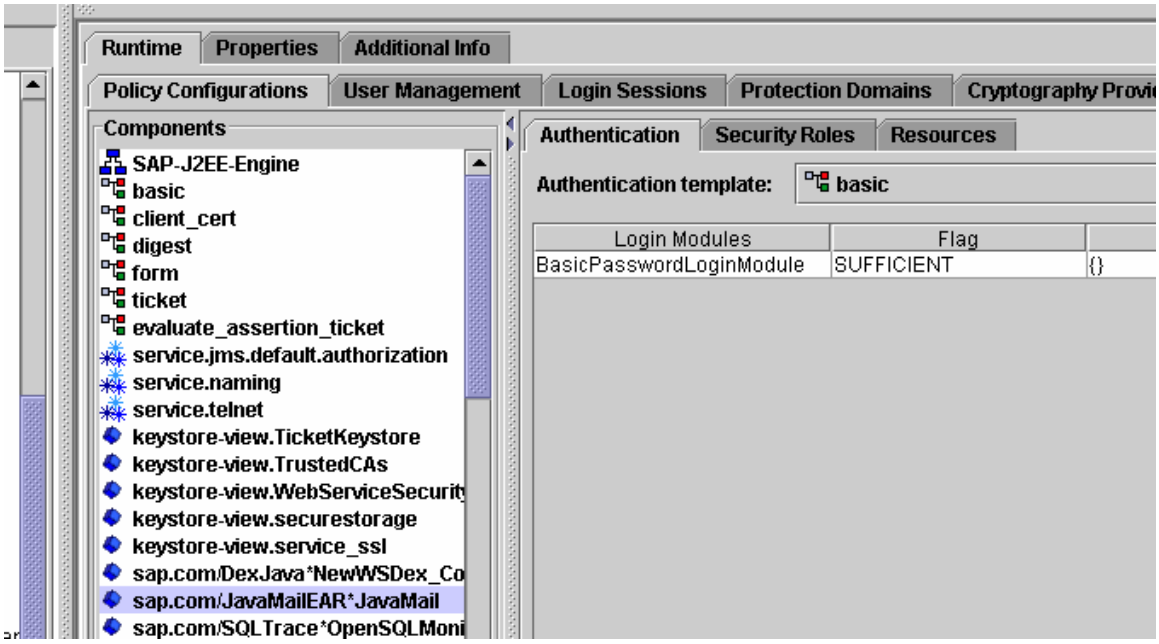
Click on Create User and enter a username and password for the new user.



We have created a user; however, we haven't yet attached the user to a role.

Adding BasicPasswordLoginModule to the Deployed Application

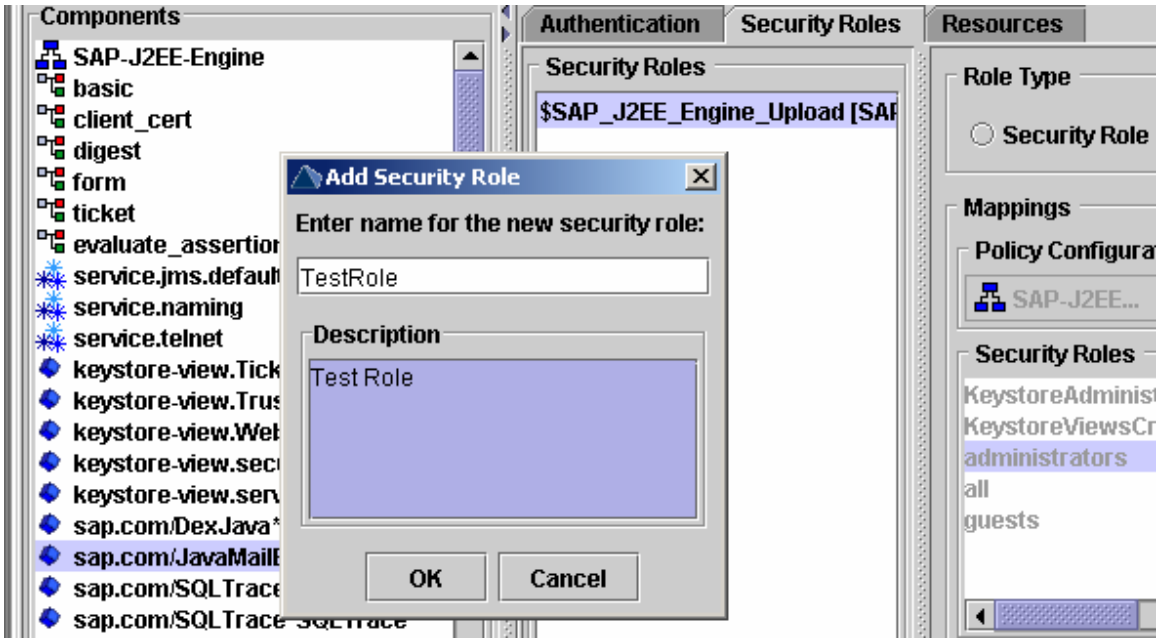
Next go to the Runtime -> Policy Configurations tab. In Components select the application that was deployed.



On the right hand side under Authentication tab make sure that “BasicPasswordLoginModule” is listed. If it is not, the click on “Add New” and select BasicPasswordLoginModule from the list.

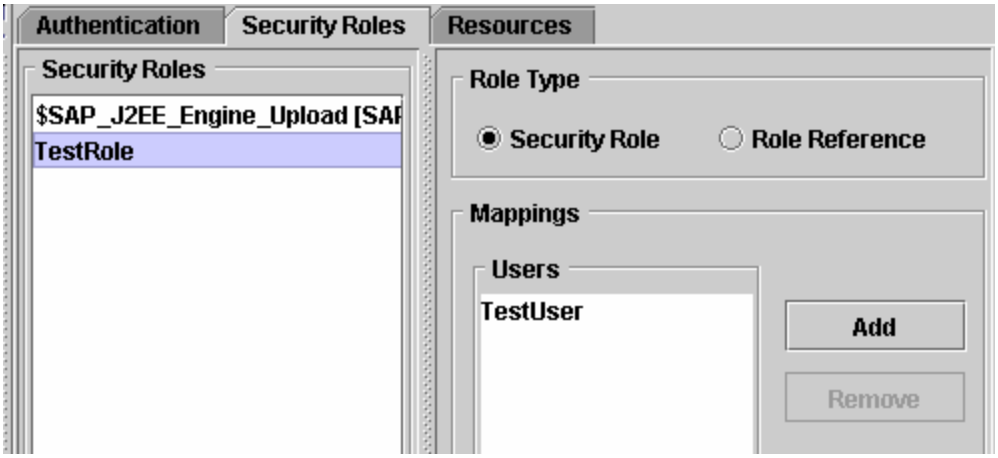
Adding a Role and Attaching Users

Go to the Security Roles tab and under Security Roles click on Add and enter the name of the role to be created. This should be same as the name entered earlier for “Server role name” in web-j2ee-engine.xml.

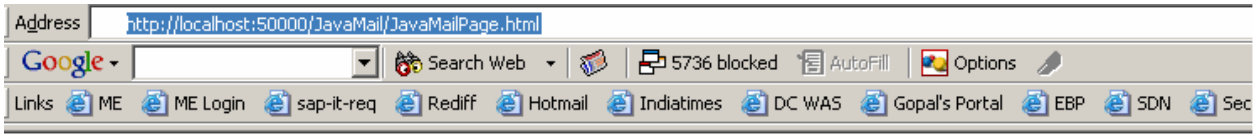


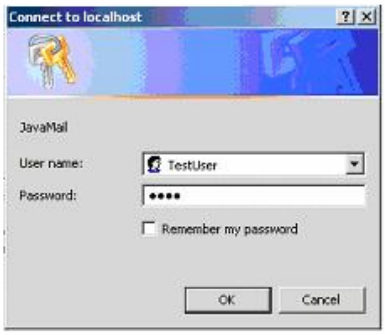
Click OK and select “Security Role” for the “Role Type.”

In Mappings click on Add for users and select the user created above.



All the required settings are done and we are ready to use the application. Open a browser and try to access the application by typing the URL. You will be prompted by the browser to enter a username and password to access the application.





Enter the username and password for the user that was created in the UME User Store earlier and you will be authenticated by the J2EE engine.

Disclaimer & Liability Notice

This document may discuss sample coding, which does not include official interfaces and therefore is not supported. Changes made based on this information are not supported and can be overwritten during an upgrade.

SAP will not be held liable for any damages caused by using or misusing of the code and methods suggested here, and anyone using these methods, is doing it under his/her own responsibility.

SAP offers no guarantees and assumes no responsibility or liability of any type with respect to the content of the technial article, including any liability resulting from incompatibility between the content of the technical article and the materials and services offered by SAP. You agree that you will not hold SAP responsible or liable with respect to the content of the Technical Article or seek to do so.