8 Group Membership Authorization

8.1 Description

This tutorials makes changes to the basic authentication added in ***Tutorial 6 - Basic Authentication*** to add group membership authorization. It also introduces you, in part, to conditional logic in policy.

8.2 Prerequisites

8.2.1 Environment

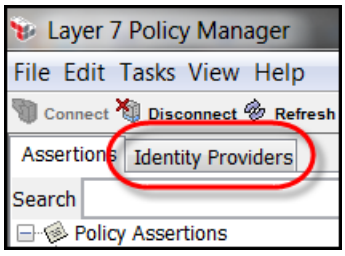
1. Layer 7 SecureSpan Gateway *(this tutorial was designed using a version 7.0 gateway; it may or may not work with earlier versions; it should work with later versions)*
2. Layer 7 Policy Manager *(this tutorial uses the Policy Manager software installation; the software installation version must match the gateway version; alternatively, users can use the Policy Manager browser-based version which always matches the gateway version that is connected to)*
3. soapUI *(this tutorial was designed using the free soapUI version 4.5.1; it may or may not work with other versions of soapUI; other clients can be used for this and other tutorials, but specific steps will not be provided for those other clients)*

8.2.2 Tutorials

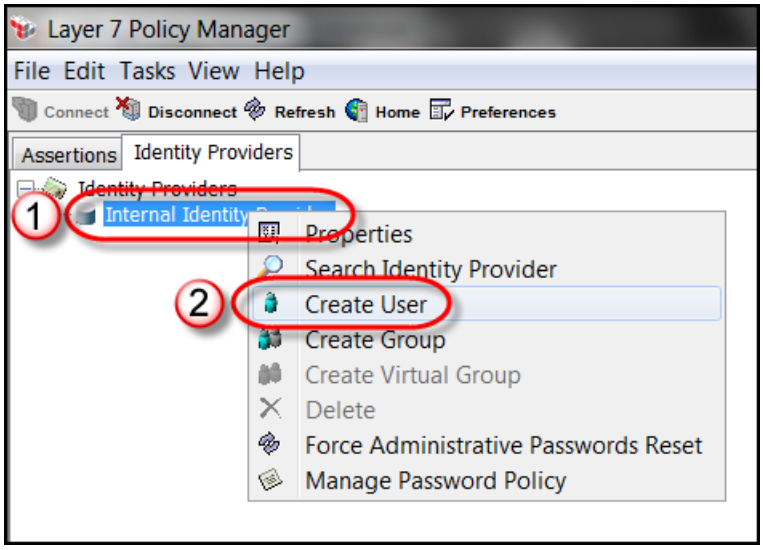
1. Layer 7 Tutorials - Getting Started
2. Tutorial 1 - Deploy Tutorial Services
3. Tutorial 3 - Test Tutorial REST Service
4. Tutorial 5 - Publish REST Service
5. Tutorial 6 - Basic Authentication

8.3 Tutorial Steps

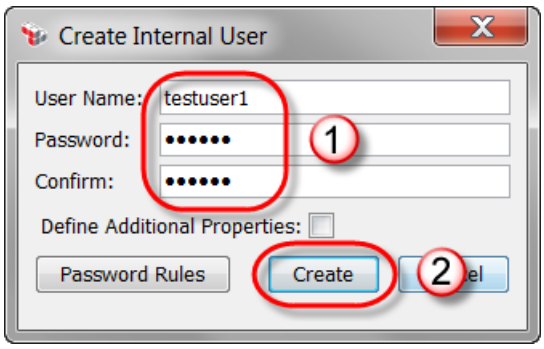
1. Connect to your gateway using Policy Manager (see tutorial ***Layer 7 Tutorials - Getting Started***).
2. Per ***Layer 7 Tutorials - Getting Started/Basic Policy Concepts/Policy Authoring/Policy Revisions***, set the active policy version of the ***Warehouse REST Tutorials*** service to the version that has been commented with, **Tutorial 6 Complete**.
3. In Policy Manager, select the ***Identity Providers*** tab.



4. In the Identity Providers tree, right click on the ***Internal Identity Provider***, and in the context menu, select the ***Create User*** item.



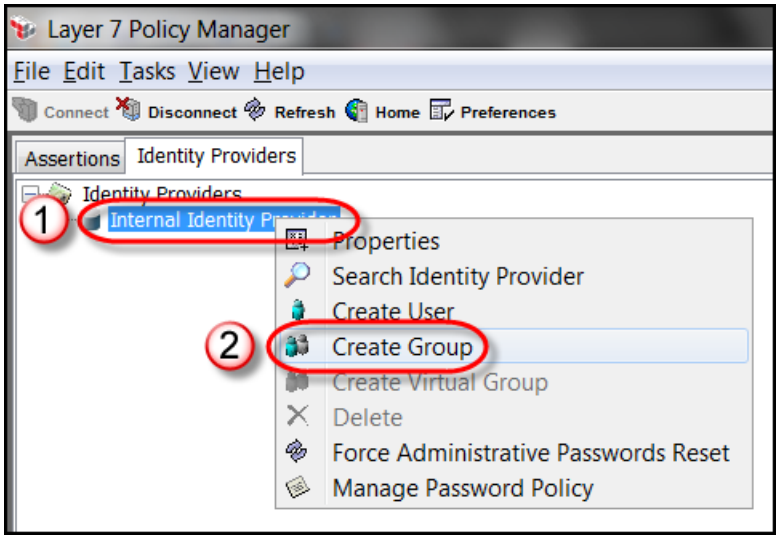
5. In the Create Internal User dialog, in the ***User Name*** field type ***testuser2***, type and confirm a password of your choice, and click the ***Create*** button.



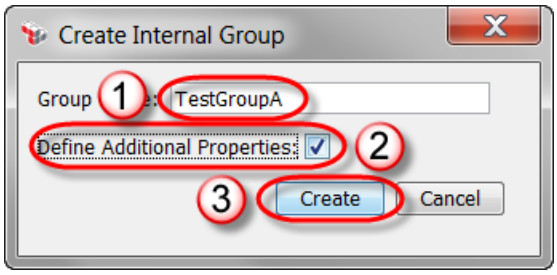
Note: "7layer" is a password that Layer 7 often uses by default. If the Internal Identity Provider's password policy has been relaxed, it's an easy to remember password that many Layer 7 employees will think to try first if they help you with your tutorials. You may also want to use "7layer" for this reason. In any case, remember the password you use for this and later tutorials.

6. Repeat steps 4 and 5 to add another user named ***testuser3***.

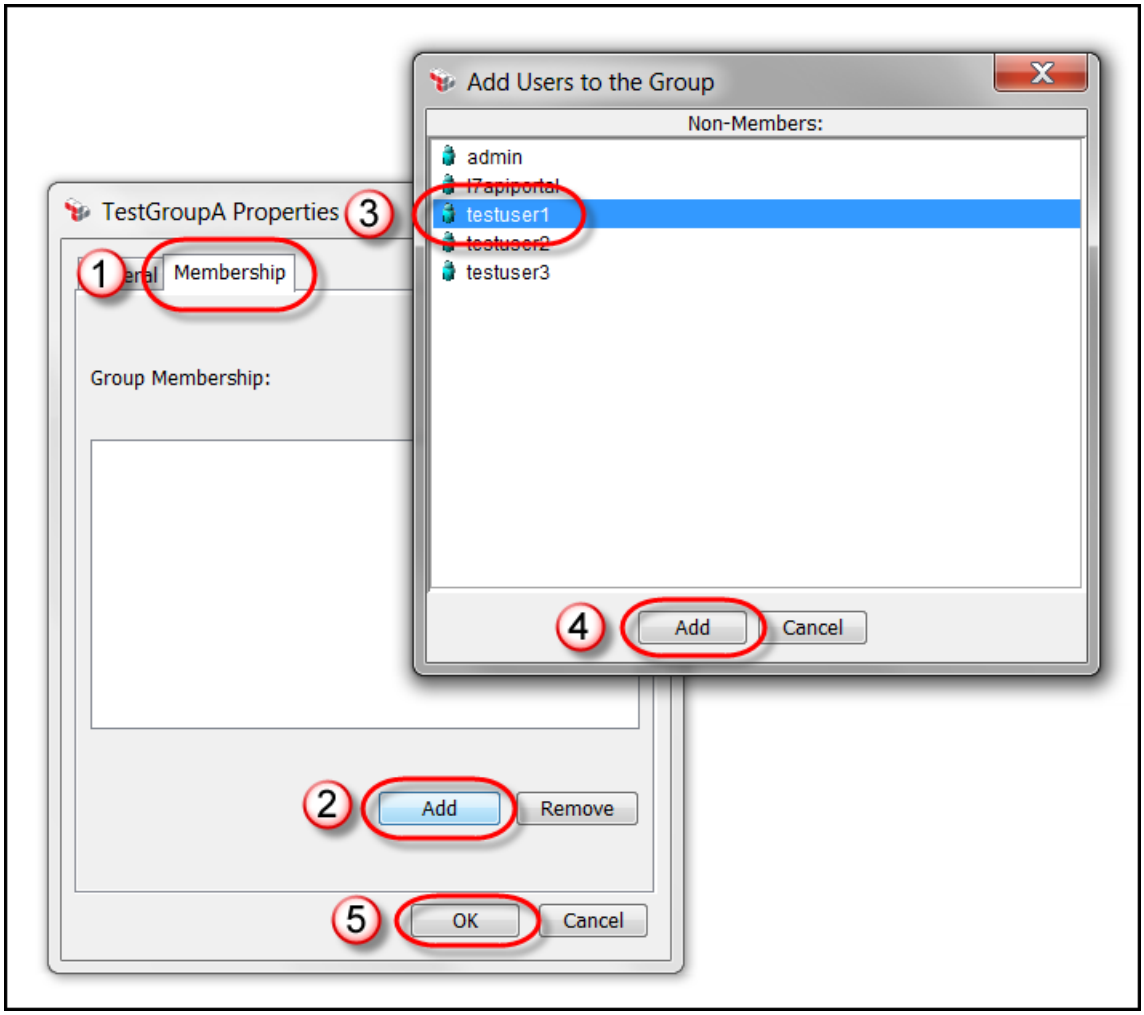
7. In the Identity Providers tree, right click on the ***Internal Identity Provider***, and in the context menu, select the ***Create Group*** item.



8. In the Create Internal Group dialog, in the Group Name field type ***TestGroupA***, check the ***Define Additional Properties*** option, and click the ***Create*** button.

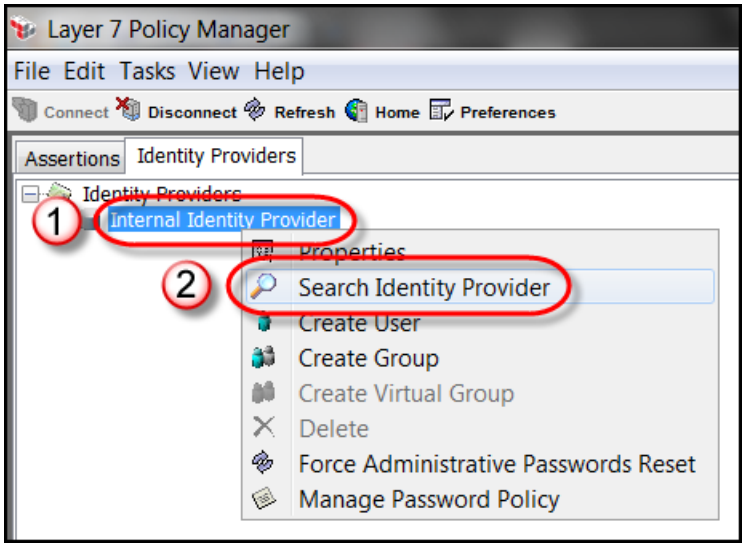


9. In the TestGroupA Properties dialog, select the ***Membership*** tab, and click the ***Add*** button. In the Add Users to the Group dialog, select the ***testuser1*** user, and click the ***Add*** button. In the TestGroupA Properties dialog, click the ***OK*** button.

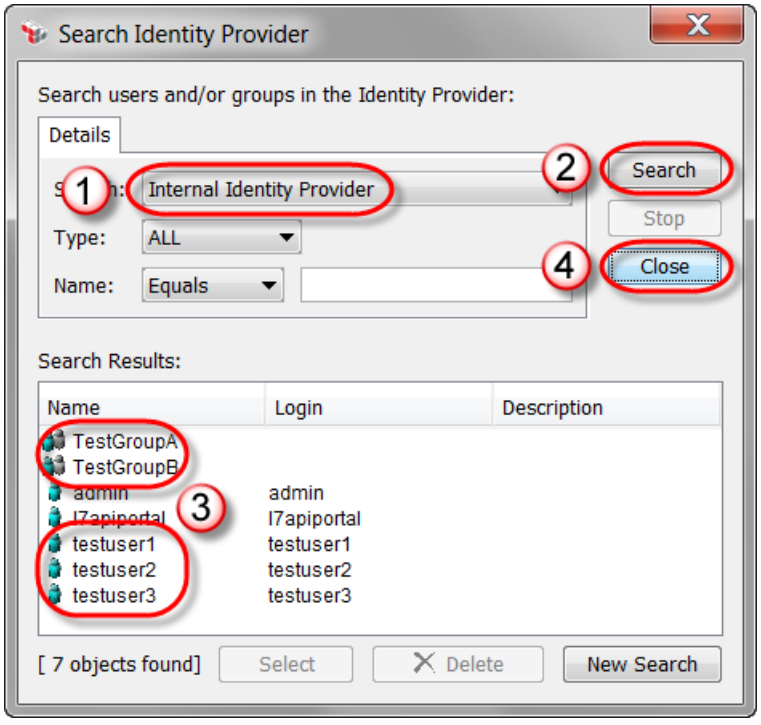


10. Repeat steps 7 - 9 to add a group called ***TestGroupB*** containing the user ***testuser2***.

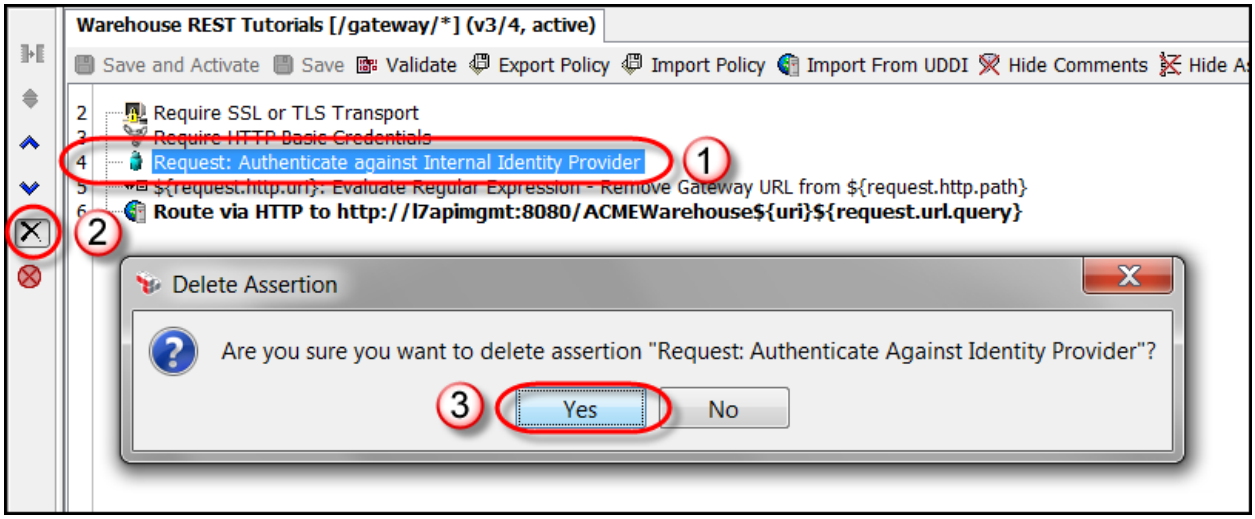
11. In the Identity Providers tree, right click on the ***Internal Identity Provider***, and in the context menu, select the ***Search Identity Provider*** item.



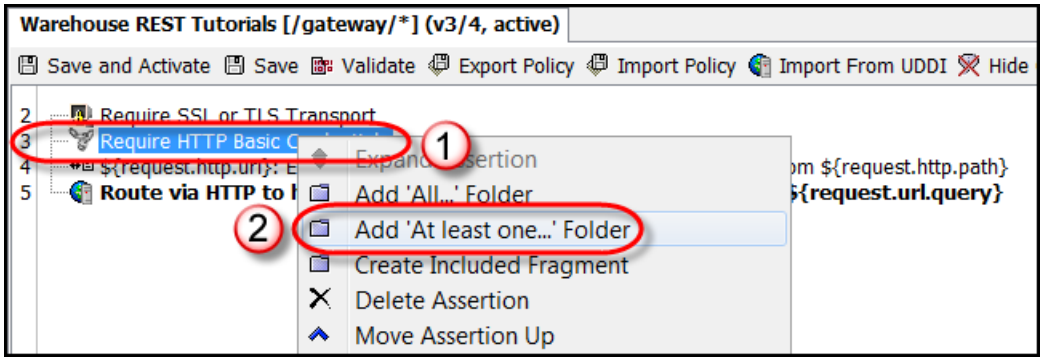
12. In the Search Identity Provider dialog, make sure ***Internal Identity Provider*** is selected in the Search dropdown list, and click the ***Search*** button. Make sure that you see the new test users and groups in the search results, and then close the dialog using the ***Close*** button in the upper right corner.



13. In the policy editor, right click on ***assertion #4, the Request: Authenticate against Internal Identity Provider*** assertion, and in the toolbar on the left, click the ***Delete*** toolbar button. In the Delete Assertion dialog, click the ***Yes*** button.

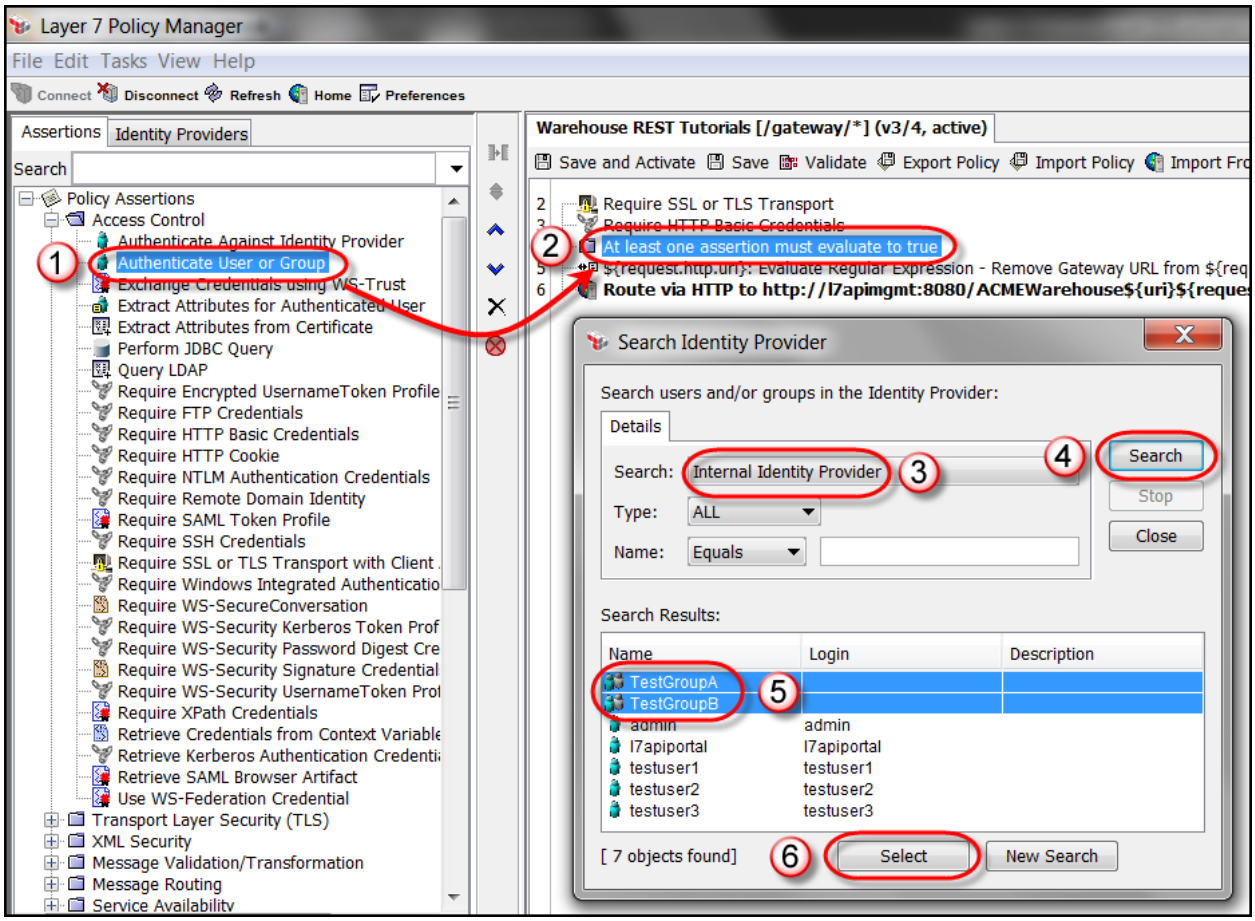


14. In the policy editor, right click on ***assertion #3, the Require HTTP Basic Credentials*** assertion, and in the context menu, select the ***Add 'At least on...' Folder*** menu item.



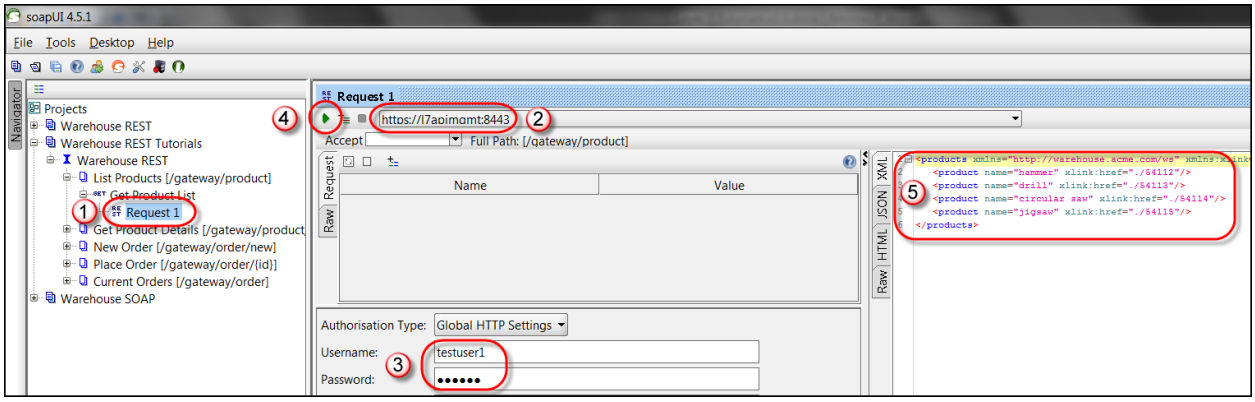
*Note: The **At least one assertion must evaluate to true** assertion folder requires that at least one immediate child assertion within the folder must succeed for the folder itself to succeed, and it represents the "OR" condition in conditional policy logic. The **All assertions must evaluate to true** assertion folder requires that all immediate child assertions within the folder must succeed for the folder to succeed, and it represents the "AND" condition in conditional policy logic. These folders can be nested within each other as many levels deep as you like to support very sophisticated conditional policy logic. These assertions can also be dragged from the Policy Logic category in the policy assertion tree.*

15. From the policy assertion tree, drag and drop the ***Policy Assertions/Access Control/Authenticate User or Group*** assertion on top of ***assertion #4, the At least one assertion must evaluate to true*** assertion folder. In the Search Identity Provider dialog, make sure ***Internal Identity Provider*** is selected in the Search dropdown list, and click the ***Search*** button. In the Search Results table, select the **TestGroupA** and **TestGroupB** groups, and click ***Select*** button.

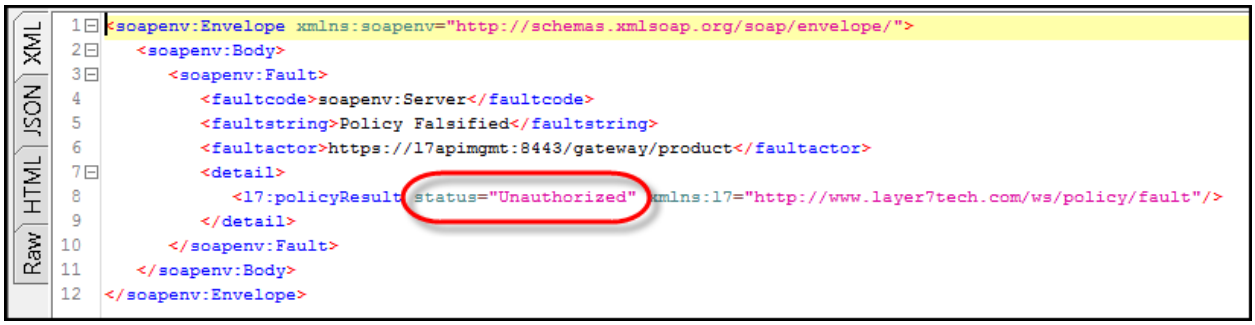


16. On the policy editor toolbar, click the ***Save and Activate*** button.
17. Open soapUI, and use the ***Warehouse REST Tutorials*** project created in the ***Tutorial 5 - Publish REST Service*** tutorial to test this tutorial's policy.

18. Open the ***Get Product List*** request, select the ***HTTPS endpoint*** on your gateway, enter the username ***testuser1*** and corresponding password, and send the message using the ***green arrow***. You should receive a successful response (because testuser1 is a member of TestGroupA).



19. Repeat step 18 using username ***testuser2***. You should receive another successful response (because testuser2 is a member of TestGroupB).
20. Repeat step 18 using username ***testuser3***. You should receive an error response (because testuser3 is neither a member of TestGroupA nor TestGroupB).



21. Per ***Layer 7 Tutorials - Getting Started/Basic Policy Concepts/Policy Authoring/Policy Revisions***, and as demonstrated at the end of ***Tutorial 1 - Deploy Tutorial Services***, comment the active policy revision of the ***Warehouse REST Tutorials*** service with the comment, **Tutorial 8 Complete**.
22. You are done with this tutorial.

8.4 Additional Context

None