6 Basic Authentication

6.1 Description

This tutorials shows you how to add some basic access control to your services using HTTP Basic credentials sent over SSL and authenticated against the gateway's internal identity provider.

6.2 Prerequisites

6.2.1 Environment

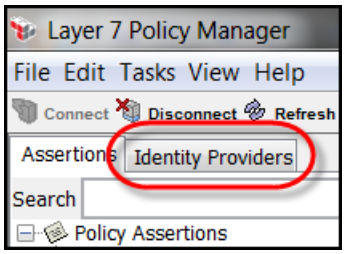
1. Layer 7 SecureSpan Gateway *(this tutorial was designed using a version 7.0 gateway; it may or may not work with earlier versions; it should work with later versions)*
2. Layer 7 Policy Manager *(this tutorial uses the Policy Manager software installation; the software installation version must match 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)*

6.2.2 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

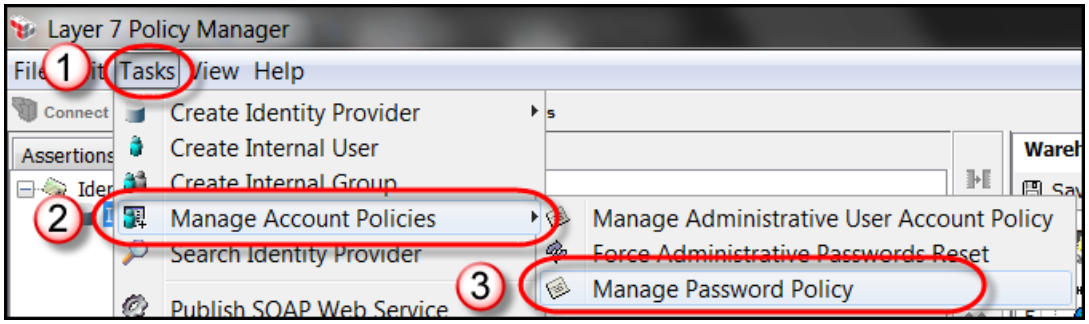
6.3 Tutorial Steps

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 5 Complete**.
3. In Policy Manager, select the ***Identity Providers*** tab.

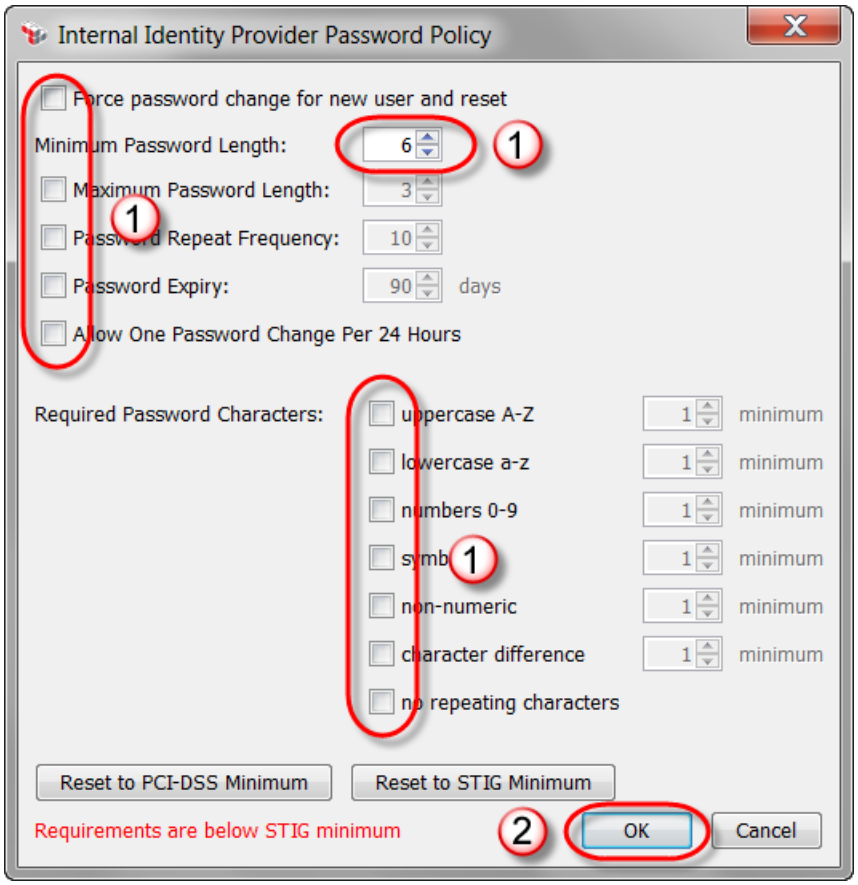


We will now add a test user to the Internal Identity Provider. If this gateway is only being used for evaluation or training purposes, and/or if internal identity provider password policies are not a concern for this gateway, then you may want to relax the gateway's default password policy to allow easier to remember passwords.

To relax the gateway's default password policy, select the ***Tasks/Manage Account Policies/Manage Password Policy*** menu item.

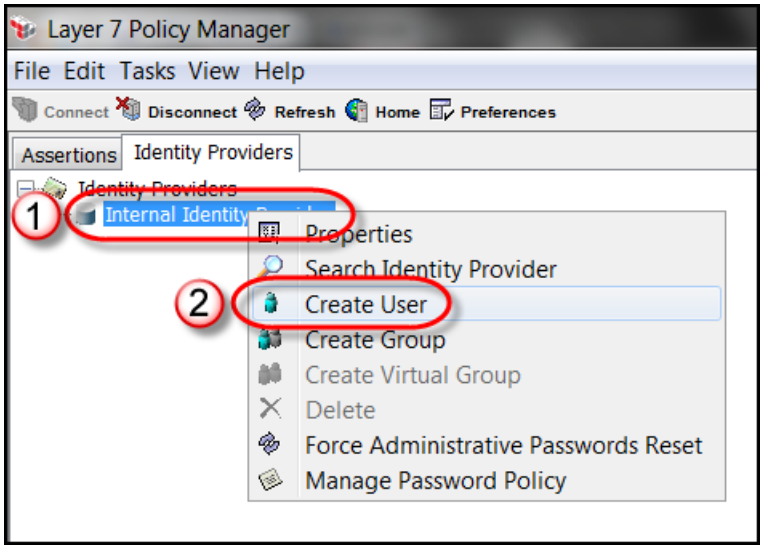


In the Internal Identity Provider Password Policy dialog, uncheck all options and reduce the ***Minimum Password Length*** to a smaller length that suits you, and then click the ***OK*** button.

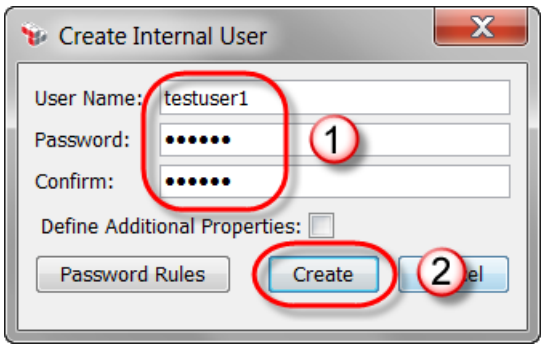


Note: Should you ever want to go back to a higher standard password policy, you can simply return to this dialog and click on either the ***Reset to PCI-DSS Minimum*** *or* ***Reset to STIG Minimum*** *buttons.*

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

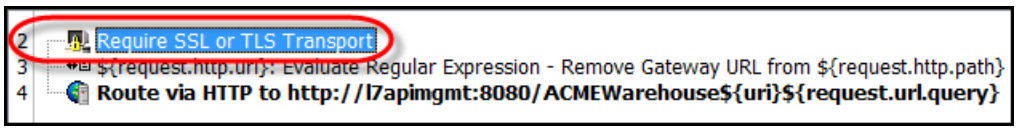


5. In the Create Internal User dialog, in the ***User Name*** field type ***testuser1***, type and confirm a password of your choice, and click the ***Create*** button.



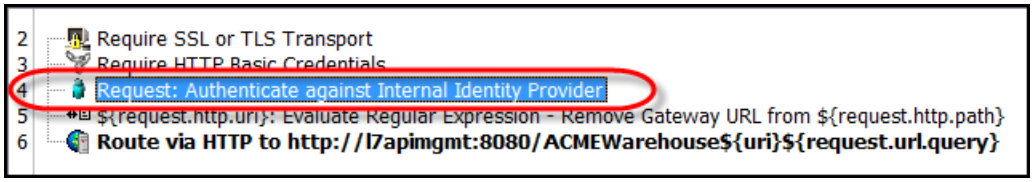
Note: "7layer" is a password that Layer 7 often uses by default. If the Internal Identity Provider's password policy has been relaxed, it's an easy to remember password that many Layer 7 employees will think to try first if they help you with your tutorials. You may also want to use "7layer" for this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

6. From the policy assertion tree, drag and drop the ***Policy Assertions/Transport Layer Security (TLS)/Require SSL or TLS Transport*** assertion to place it at the top of the ***Warehouse REST Tutorials*** service policy in the policy editor.

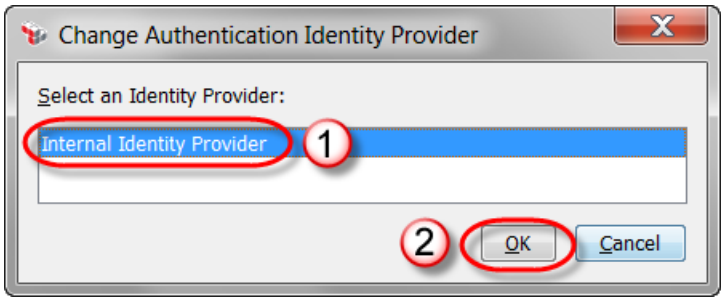


7. From the policy assertion tree, drag and drop the ***Policy Assertions/Access Control/Require HTTP Basic Credentials*** assertion so that it's assertion #3 in the ***Warehouse REST Tutorials*** service policy in the policy editor.

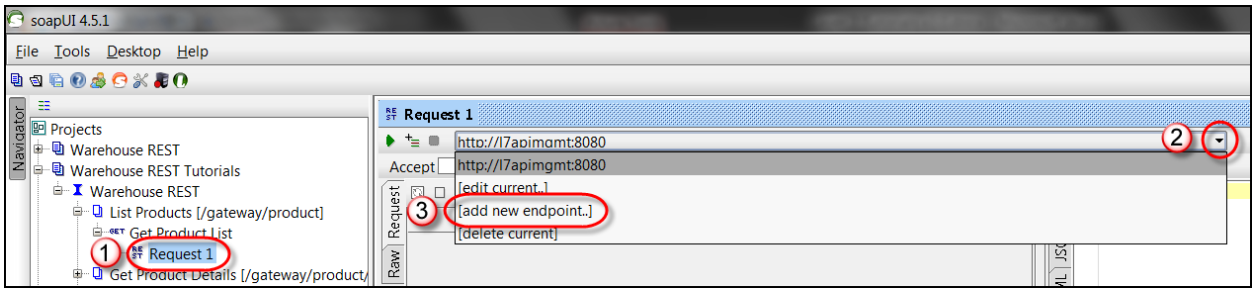
8. From the policy assertion tree, drag and drop the ***Policy Assertions/Access Control/Authenticate Against Identity Provider*** assertion so that it's assertion #4 in the ***Warehouse REST Tutorials*** service policy in the policy editor.



9. In the Change Authentication Identity Provider dialog that pops up when dragging and dropping the Authenticate Against Identity Provider assertion to the policy editor, select the ***Internal Identity Provider*** and click the ***OK*** button.



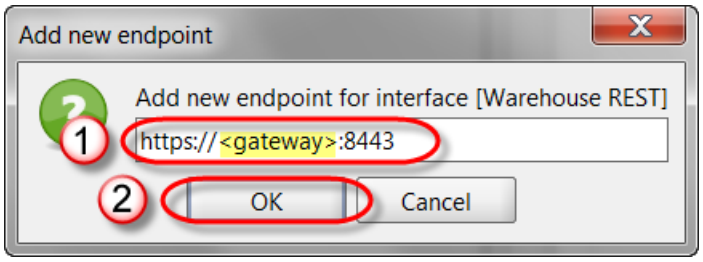
5. On the policy editor toolbar, click the ***Save and Activate*** button.
6. Open soapUI, and use the ***Warehouse REST Tutorials*** project created in the ***Tutorial 5 - Publish REST Service*** tutorial to test this tutorial's policy.
7. In soapUI, in a request dialog (e.g. the Get Product List request), you will need to add a new HTTPS endpoint.



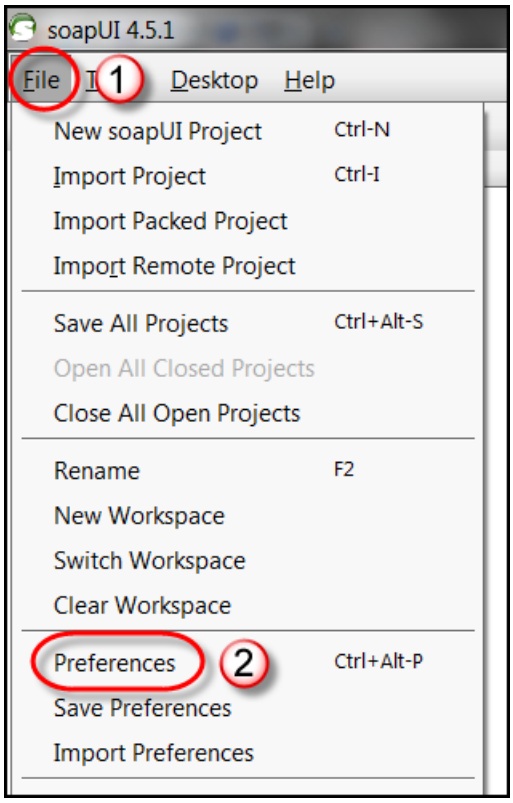
Add the following endpoint (with <gateway> replaced by the host name or IP address of your gateway):

https://<gateway>:8443

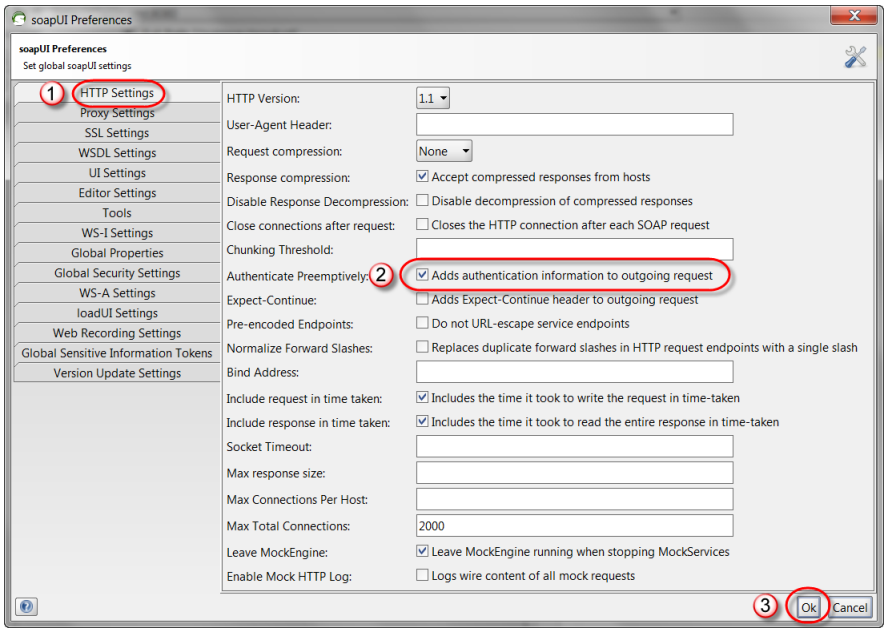
For example:



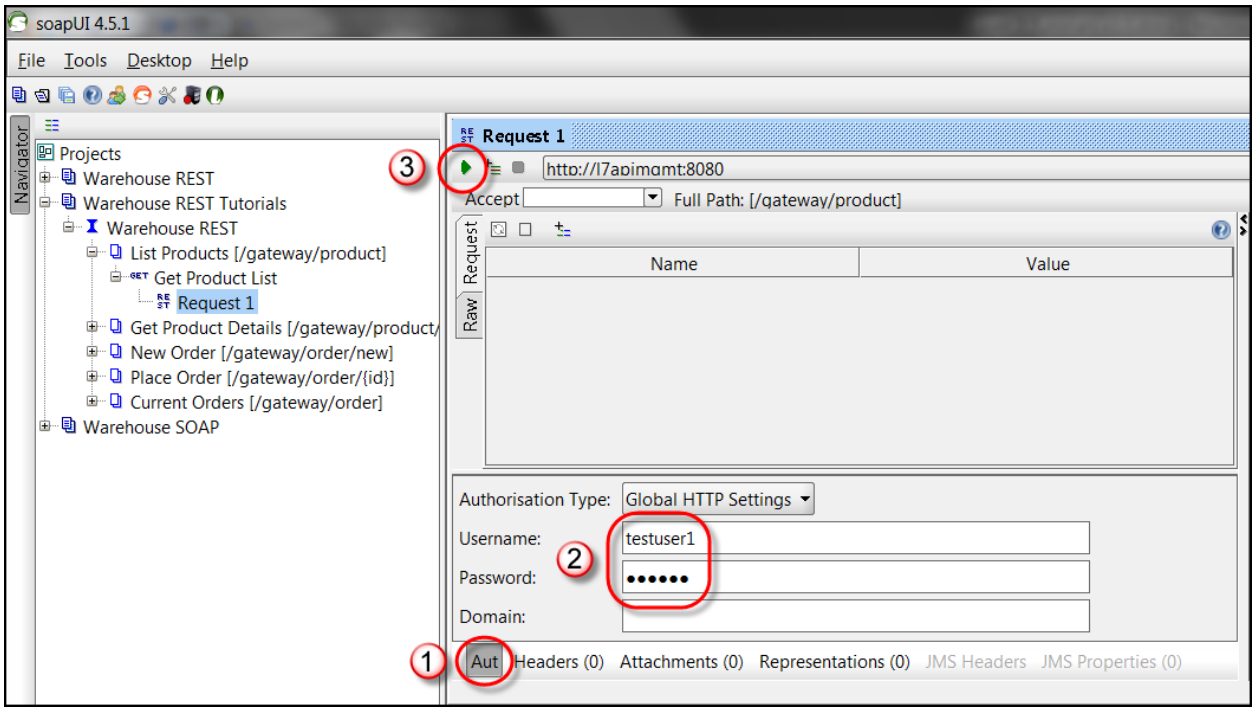
8. In soapUI, to send HTTP Basic credentials preemptively (i.e. without first waiting to be challenged), select the ***File/Preferences*** menu item.



9. In the soapUI Preferences dialog, select the ***HTTP Settings*** tab, check the ***Authenticate Preemptively*** option, and click the ***OK*** button.



10. In soapUI, to specify your HTTP Basic credentials, in a request dialog, select the ***Aut*** tab at the bottom, enter your ***username and password*** in the provided fields, and use the ***green arrow*** button to send your request.



11. Try sending a request without credentials, sending a request with bad credentials (e.g. **baduser/<password>**) and sending a request with good credentials (e.g. **testuser1/<password>**).
12. 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 6 Complete**.

13. You are done with this tutorial.

6.4 Additional Context

This tutorial demonstrates a basic access control pattern for Layer 7 beginning with collecting credentials from the request message content or context, and then authenticating those credentials. This is normally a two step process. In other words, collecting the credentials alone does not ensure that they are authenticate, and trying to perform authentication without first collecting the credentials will fail.

This tutorial uses the Internal Identity Provider for authentication. The Internal Identity Provider contains users and groups stored in the gateway's database. To begin with, the Internal Identity Provider contains the initial administrator user for role based access control to the gateway itself. As this and later tutorials demonstrate, the Internal Identity Provider can be used to store additional users, groups and certificates for role based access control to the gateway's configuration as well as access control of traffic passing through the gateway.

In fact, customers more commonly use an LDAP Identity Provider (e.g. Microsoft Active Directory) for the above purposes. Though the Layer 7 Sales Demonstration Environment (SDE) can install a LDAP directory for customer's use, to avoid a dependency on the SDE or other LDAP directories, the tutorials in this document will use the Internal Identity Provider in place for LDAP Identity Providers.

Besides the initial configuration of LDAP Identity Providers, and the Query LDAP assertion, the Internal Identity Provider and LDAP Identity Providers are essentially interchangeable in policy and elsewhere in Policy Manager. In other words, if you do have a LDAP directory to work within your environment, and you successfully configure a LDAP Identity Provider on your gateway for that LDAP directory, you should be able to use it instead of the Internal Identity Provider for most tutorials.