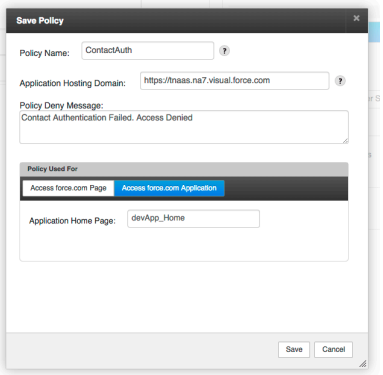
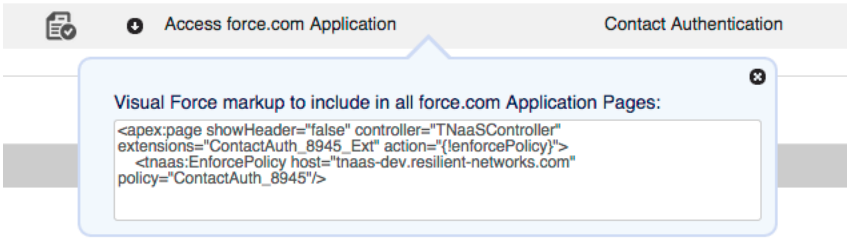
The Salesforce administrator/developer can create policies that use any combination of Resilient Access out of the box authorities and custom authorities created by them as described in Create Policies. To use the policy for access control in a Visual Force Page, follow the steps below

1. Define the Policy expression as described in Create Policies and specify how the authority parameters will receive values at runtime and click the **Next** button.




2. In the **Save Policy** popup enter the Salesforce instance domain the Salesforce organization is in for the **Application Hosting Domain** box
3. Provide a custom deny message that users accessing the Visual Force page that uses this Policy will see if the policy evaluation results in a DENY *(optional)*
4. Select the **Access force.com Application** tab in the **Policy Used For** section.
5. Enter the name of the Visual Force page that will be the applications home page
6. Click **Save** to save the policy. Resilient Access will automatically generate the following Visual Force page and apex class to integrate policy enforcement into the force.com application:
    - ***<PolicyName>_Login*** VF Page. This page initiates the policy evaluation. Loading an application pages with the appropriate VF markup as show below will redirect to the Login page to evaluate the policy. The app developer may customize this page to include their application branding.
    - ***<PolicyName>_Logout*** VF Page. This page is loaded when the Logout button is clicked. This page will terminate the application and Resilient Access sessions and redirect back to the Login page. The app developer may customize this page to include their application branding.
    - ***<PolicyName>_PostEval*** VF Page. This page will be loaded in the browser at the end of a successful policy evaluation. This page will establish the application session and then redirect the browser to the application home page in the logged in state.
    - ***<PolicyName>_Ext*** Controller Extension. This apex class extends the package provided Resilient AccessController and enforces the application session verification when the force.com app page is loaded.
7. In the Policy list click on the button for the policy created to get the Visual Force markup to




8. Copy and paste the VF markup into the beginning of each application page. If the app developer has their own controller then it must be a descendant of the Resilient Access Controller. The VF markup can be modified accordingly.
insert into each application page.