
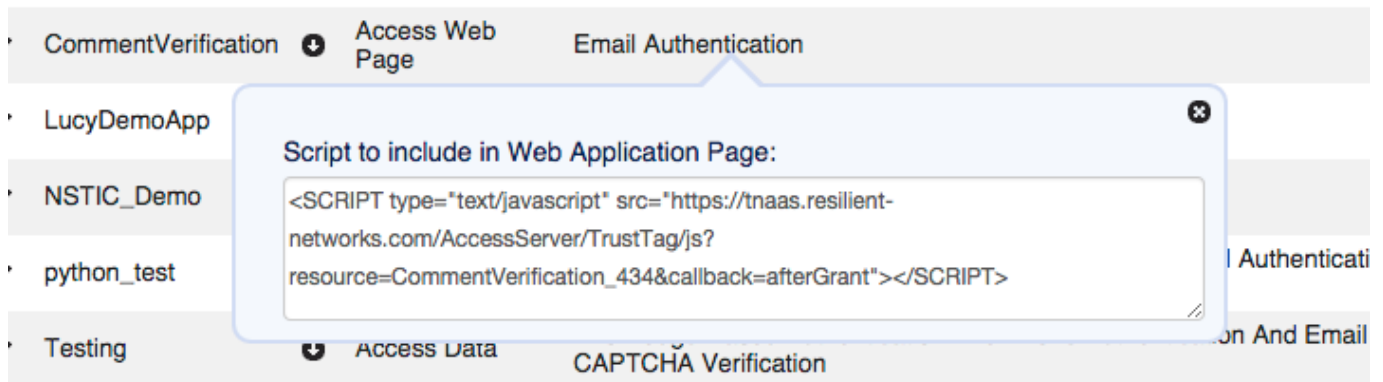


This variant of Trust Tag is well suited for enforcing a policy in a web page or specific sections of a web page. In this interactive guide we have used the Email Authentication policy to verify the user is in possession of the email address they entered before they can post a comment.

This variant of Trust Tag enforces the policy purely through Javascript. After creating a policy of type **Access Web Page**, from the Policy list click on the  icon next to the policy to use. It will display the HTML SCRIPT tag code to insert into your HTML or server script page as shown below:



Simply copy the SCRIPT tag and insert it into the <head> tag of each web page that you wish to enforce the policy on. This script tag should be the first SCRIPT tag in the HTML source. This will instantly integrate the Trust Network policy evaluation engine into your web page through javascript injection.

Since this variant of Trust Tag enforces the policy through javascript after the server has returned the response for the web page, it is recommended to dynamically build the web page using AJAX techniques so that sensitive information is only visible to the end user if the policy evaluation succeeds. Trust Tag facilitates this by invoking a Javascript function called "afterGrant" if it is defined in the page. It is recommended to use AJAX to retrieve and render contents of the page in this callback function.

Access Web Page Trust Tag uses [Cross Origin Resource Sharing \(CORS\)](#) to facilitate the secure execution of cross-domain Javascript code. This feature works in all modern browsers as shown in the Browser Support section of the Wikipedia link. In order to successfully execute Access Web Page Trust Tag, the web page should be served from the domain value specified in the **Application Hosting Domain** field including the HTTP scheme, e.g. *https://www.example.com*