# Users Prompted for Authentication When SaaS with Identity Provider Initiated Flows and NTLM

**Document ID: 118275**

Contributed by David Paschich and Siddharth Rajpathak, Cisco TAC Engineers.
Aug 12, 2014

## Contents



## Question

Why are users prompted for authentication when SaaS with Identity Provider initiated flows and NTLM?

## Environment

- Cisco Web Security Appliance (WSA) running AsyncOS versions 7.0 or later
- NTLM used for transparent authentication
- SaaS Access Control configured using identity−provider initiated flow
- SaaS SSO configured

I have SaaS Access Control configured with my external application, using the identity provider−initiated flow and SAML for single sign−on. I am also using NTLM to transparently authenticate my users. However, how can I prevent them from seeing this prompt?

## Symptoms

- When users click on their bookmark for the SaaS SSO URL, they sometimes see the authentication prompts.
- Access works fine if the users access another external website and then click the SaaS SSO URL bookmark.

This problem occurs when/because the first request the WSA sees from the client is to the special SSO URL, which is served directly from the WSA.

Content which is served directly from the WSA − such as EUN pages or PAC files − is normally exempt from authentication. While the SaaS feature can access the authentication surrogates maintained by the proxy, it cannot itself request authentication using any method besides form−based authentication (NTLM or LDAP). So the observed behavior is per design but is not an optimal solution.

Defect CSCzv55859 is filed to track this problem and to provide a better mechanism to address this issue.

There are two workarounds available.

# Workaround 1

1. The first is to use a Service Provider−Initiated flow in the SaaS configuration. In an SP−initiated flow, the user starts by browsing to the target SaaS application, which then issues the redirect through the SSO URL.
    - Because this initial traffic goes through the proxy, the user will get authenticated properly using NTLM. This workaround only works if the target application supports SP−initiated flows.
2. Create a new SSO URL in the WSA policy, forcing authentication and then redirecting the client to the "real" SSO URL.

# Workaround 2

1. Decide on a new SSO URL. This URL will never actually be accessed by the proxy; it will simply act as a point to initiate the sign−on process.

    - For instance, if the current SSO URL is "***wsa.mycompany.com/SSOURL/WebEx***", you may use "***wsa.example.com/SSOURL/WebEx***".
    - The important consideration is making sure the hostname portion you use will be proxied through the WSA.

        ◊ When the WSA is deployed as an explicit proxy, the hostname can be just about anything.
        ◊ If the WSA is deployed as a transparent proxy, then the hostname will need to be a real hostname which resolves to an external IP address.

2. Create a custom URL category (***GUI > Web Security Manager > Custom URL categories***) which matches the new URL.You will need to create one custom URL category for each SaaS application you need to apply the workaround to.
    - Use the regular expression match to match on the full URL.

3. Go to access policies (***GUI > Web Security Manager > Access Policies***) and under the URL filtering column for an access policy which the user's request will match. This may be the global policy or another policy earlier in the table.
    - Include the new custom URL category in this access policy, and set its action to ***redirect***. The target of the redirection should be the "real" SSO URL.

4. Submit and commit the changes to apply the new configuration.

Users should now use the new SSO URL to access the application. Because access to this URL is processed by the proxy, NTLM authentication will be invoked and the user always be will be signed in transparently, avoiding authentication prompts.

---

Updated: Aug 12, 2014 Document ID: 118275