Configure a Service Provider to Force Re-Authentication

This document describes how to configure a Shibboleth Service Provider (SP) to force re-authentication of a user instead of using Single Sign-On (SSO).

After a user is authenticated with Cornell Identity Provider (IdP), they may be able to access other Shibboleth/CUWebAuth protected applications without having to logon again for up to 10 hours. In some cases, however, an application may wish to force users to re-authenticate even if they present a valid session cookie. This is sometimes done for sensitive applications that want to reduce the risk of a valid user session at an unattended computer being used by another person to access data inappropriately.

Configuration

Forced re-authentication can be configured in the `shibboleth2.xml` file.

```
<SSO entityID="https://mysites.com/shibboleth" forceAuthn="true">
     SAML2
</SSO>
```

If you use Apache, you also have the option to define forced re-authentication in shib.conf

```
ShibRequestSetting forceAuthn true
```

See Also

Shibboleth Project's ForceAuthn