IdPAuthExternal

Configuring the IdP for External Authentication System User Authentication

This login handler supports the use of an external (to the IdP) authentication mechanisms that is integrated with the web server, Servlet container, or IdP.

This login handler requires additional code to be written in order to trigger the external authentication system. If you're simply looking to authenticate based on the presence of the REMOTE_USER header use the Remote User login handler.

How It Works

This login handler forwards to a configurable (see below) URL. A custom-developed Filter, Servlet, or JSP must then trigger the external authentication system in whatever manner is appropriate for that system. Once completed, the custom-developed code must then set the `HttpServletRequest` attributes required by the `edu.internet2.middleware.shibboleth.idp.authn.LoginHandler` interface and invoke `edu.internet2.middleware.shibboleth.idp.authn.AuthenticationEngine#returnToAuthenticationEngine(HttpServletRequest, HttpServletResponse`.

When the IdP invokes the configured URL the following `HttpServletRequest` attributes will be available:

- **forceAuthn** - a boolean indicating whether force authentication is required
- **isPassive** - a boolean indicating whether passive authentication is required
- **authnMethod** - the authentication method the external authentication system is expected to perform
- **relyingParty** - the entity ID of the relying party that is requesting the user be authenticated

The external authentication system **must** honor the request for forced and/or passive authentication.

Define the Login Handler

This login handler is defined with the element `<LoginHandler xsi:type="ExternalAuthn">` with the following required attributes:

- **externalAuthnPath** - context-relative path to the Filter, Servlet, or JSP used to interact with the external authentication system
- **supportsForcedAuthentication** - indicates the external authentication system supports forced authentication (default value: false)
- **supportsPassiveAuthentication** - indicates the external authentication system support passive authentication (default value: false)

This login handler configuration element also supports the following optional attributes:

- **authenticationDuration** - length of time in minutes that the authentication method associated with this login handler is active; default: 30 minutes

Additionally the login handler **must** contain one or more `<AuthenticationMethod>` elements that contain authentication method(s) serviced by the login handler.

Example External Authentication Login Handler Configuration

```
<ph:LoginHandler xsi:type="ph:ExternalAuthn"
                 externalAuthnPath="/authn/external"
                 supportsForcedAuthentication="true" >
    <ph:AuthenticationMethod>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</ph:
AuthenticationMethod>
</ph:LoginHandler>
```