Modules - OpenAM: installation and configuration

The module uses OpenAM RESTful API. The base URL of the API is a required configuration property of the module. When the module is enabled in the CzechIdM, users can authenticate to CzechIdM with their login and password valid for OpenAM.

Authentication token

Token for successfully authenticated users is set to the cookie of the (default) name iPlanetDirectoryPro for the current request domain.

The cookie is set only for secured (https) connections by default. If you need to set it for unsecured connections, configure the property `idm.sec.openam.sso.cookie.secure=false`. This is strongly discouraged for production use!

SSO

Single-Sign-On functionality of the OpenAM module is done by a new authentication filter. When unauthenticated users come to CzechIdM and have the cookie with OpenAM token, the value of the token is validated against OpenAM. If the token is valid, the filter retrieves the user's login from OpenAM attributes and logs the user in.

Multiple instances and realms

The module supports multiple instances of OpenAM. The URLs must be configured in the property `idm.sec.openam.base.url` separated by a comma. Authentication or token validation uses the configured instances one by one. The first instance that returns a success is the winner (no more calls are made to remaining instances).

The module also supports authentication realms in OpenAM. If configured, the realm(s) are used during authentication in the same order as the configured URLs of the instances.

REST endpoint

The module also provides a REST endpoint `/get-attributes` for retrieving OpenAM attributes for given SSO token. When calling the endpoint, the user's session by OpenAM can be refreshed (this is an optional parameter, default is false).

The attributes are returned in lower case.

Installation

Download the openam distribution package. The package contains a backend folder. Your IdM Tomcat installation we call IDM in the following example.

1. Copy content of the backend folder into your tomcat IdM installation - [IDM]/WEB-INF/lib
2. Set correct access rights to the files if needed (`chown tomcat:tomcat [IDM]/WEB-INF/lib/*`)
3. Restart the IdM application server (`service tomcat restart`)
4. Log in to CzechIdM as an privileged user and go to Settings → Modules and enable the openam module.
5. Go to the configuration and configure the OpenAM base url configuration property (see below).

Configuration

The module provides following configuration properties:

Property	Description
idm.sec.openam.base.url	REQUIRED. Base URL of the REST API (e.g. `https://amhost.domain.tld/openam/identity`). The property may contain multiple instances comma-separated.
idm.sec.openam.login.payload	The string that is appended to the authentication request, usually realm (e.g. `uri=realm=/customers`). If multiple URLs are configured, configure this property also as multivalued and in the order corresponding to those URLs. (default: *empty*)
idm.sec.openam.login.attr.name	Name of the OpenAM attribute which holds user login (default: uid)
idm.sec.openam.sso.cookie.name	Name of the cookie which holds OpenAM token (default: iPlanetDirectoryPro)
idm.sec.openam.sso.cookie.domain	Domain, for which the cookie will be set. If empty, request root domain will be used.
idm.sec.openam.sso.cookie.httponly	Whether the cookie should have Http-Only sign (default: true)
idm.sec.openam.sso.cookie.secure	Whether the cookie should be sent for encrypted sessions only (https) (default: true)
idm.sec.openam.returned.attributes	Which attributes will be returned by /get-attributes endpoint, written in lower case (default: uid,dn,destinationindicator,ou)
idm.sec.openam.connect.timeout	The time limit to establish the connection in ms (default: 2000), change requires restart
idm.sec.openam.socket.timeout	The time limit waiting for data after the connection was established in ms (default: 2000), change requires restart

Notes

Note that the module doesn't provide "Single-Sign-Off" - it doesn't check the validity of the users' sessions when they are already authenticated to CzechIdM.

The module has only the backend part.