MidPoint and SSO HOWTO

OUT OF DATE

This documentation is outdated. It may no longer apply to recent midPoint versions.

SSO integration in midPoint 4.0 and earlier is unofficial functionality and it is not supported without a special support contract (see below). Therefore this is not part of official midPoint documentation and it is not updated.

It is planned that MidPoint 4.1 will introduce official support for (some) SSO functionality in midPoint.

Unofficial functionality

This functionality requires modification of midPoint build, or even modification of midPoint source code. Therefore it is not officially supported - unless the support is explicitly negotiated in subscription.
The real solution to this problem would be Flexible Authentication. MidPoint platform subscription could be used to fund improvements in midPoint authentication mechanisms.

Introduction

Currently midPoint does **not** have a convenient SSO support. However as midPoint is built on top of Spring Security there are ways how to integrate midPoint to SSO. This page describes methods how it can be done.

SSO Support in MidPoint

If you are interested in a proper SSO support then your best option is to contact the Evolveum team. You can support this feature by purchasing Platform subscription or even contribute the code. Or even if you purchase a midPoint subscription you can use your influence to prioritize the development of SSO integration.

Setup

In order to enable SSO support in current midPoint you need to modify a couple of files in midPoint source code and rebuilt it. Therefore please make sure you can installing midPoint from source code.

Currently midPoint has no SSO plugin of its own. The recommended way is to use an SSO agent in front of midPoint. E.g. to configure Apache HTTP server as a reverse proxy for midPoint and place an SSO agent into Apache. The agent should be able to inject a HTTP header with a username of currently logged-in user. Then midPoint can be configured to accept the "authentication" based solely on the presence of the username in the HTTP header.

The Spring Security configuration for midPoint is in the `gui/admin-gui/src/main/webapp/WEB-INF/ctx-web-security.xml` file. This file needs to be modified.

Basically what needs to be done is to uncomment the following line:

```
<custom-filter position="PRE_AUTH_FILTER" ref="requestHeaderAuthenticationFilter" />
```

and adjust the `principalRequestHeader` parameter in the `requestHeaderAuthenticationFilter` bean:

```
<beans:bean id="requestHeaderAuthenticationFilter" class="org.springframework.security.web.authentication.
preauth.RequestHeaderAuthenticationFilter">
        <beans:property name="principalRequestHeader" value="SM_USER"/>
        <beans:property name="authenticationManager" ref="authenticationManager" />
</beans:bean>
```

You may also want to adjust logout URL to point to the SSO single-logout page:

```
<beans:bean id="logoutHandler" class="com.evolveum.midpoint.web.security.AuditedLogoutHandler">
        <beans:property name="defaultTargetUrl" value="http://sso.example.com/logout"/>
</beans:bean>
```

Then rebuild and re-deploy midpoint.

Limitations and Notes

Even though this method works reasonably well there are some limitations:

1. The username provided by the agent needs to be the same as the `name` of the user object in midPoint. There is no support for name mapping now. As the SSO system will usually be a configured resource in midPoint a care should be taken to map midPoint usernames to the resource usernames one-to-one without any transformation.
2. Web services and REST: Web services have their own authentication and authorization (WS-Security). As does REST. These cannot be currently connected to the SSO. MidPoit does not yet support STS and/or OAuth. Therefore the services are still limited to username/password authentication. However do not forget to specify SSO enforcement exceptions (e.g. non-enforcement list) for the service URLs:
    a. /model/* and /ws/* for web services
    b. /rest/* for REST service

See Also

- MidPoint as CAS Client (Apache CAS Agent Method)
- Installing midPoint from Source Code v3.0
- midPoint Development Snapshot