Search

Tempo
INTALIO OpenSSO support of tempo UI

Log In

| View | Attachments (3) | Info |

Browse Space

Added by Ark Xu, last edited by Ark Xu on Dec 12, 2008

Introduction

Intalio|BPMS provides a web application that allows the end users to access to their task list: Intalio|Workflow UI Framework (UI-FW).
And the user can choose to use OpenSSO as single sign-on technology in their IT infrastructure, this document is to describe what needs to be enhanced or implemeted for UI-FW to support openSSO.

Scope

Adapt Intalio|Workflow UI-FW to leverage OpenSSO for single sign-on.
OpenSSO support certification will target Geronimo application server.

Out of scope

- OpenSSO support will be restricted to Intalio|Workflow UI Framework. Intalio|Console and Intalio|BAM Dashboard web applications will not be OpenSSO-enabled.
- OpenSSO support for web services published or consumed by Intalio|BPMS
- Support for specific user stores such as specific LDAP server brands and versions. OpenSSO handles user authentication and shields applications participating in SSO from user store details
- Support for specific user credentials (user name/password, certificate, etc). OpenSSO handles user authentication and shields applications participating in SSO from user credential details
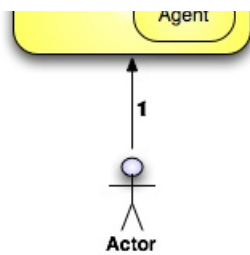
Architecture

**General OpenSSO architecture that is suitable for tempo**
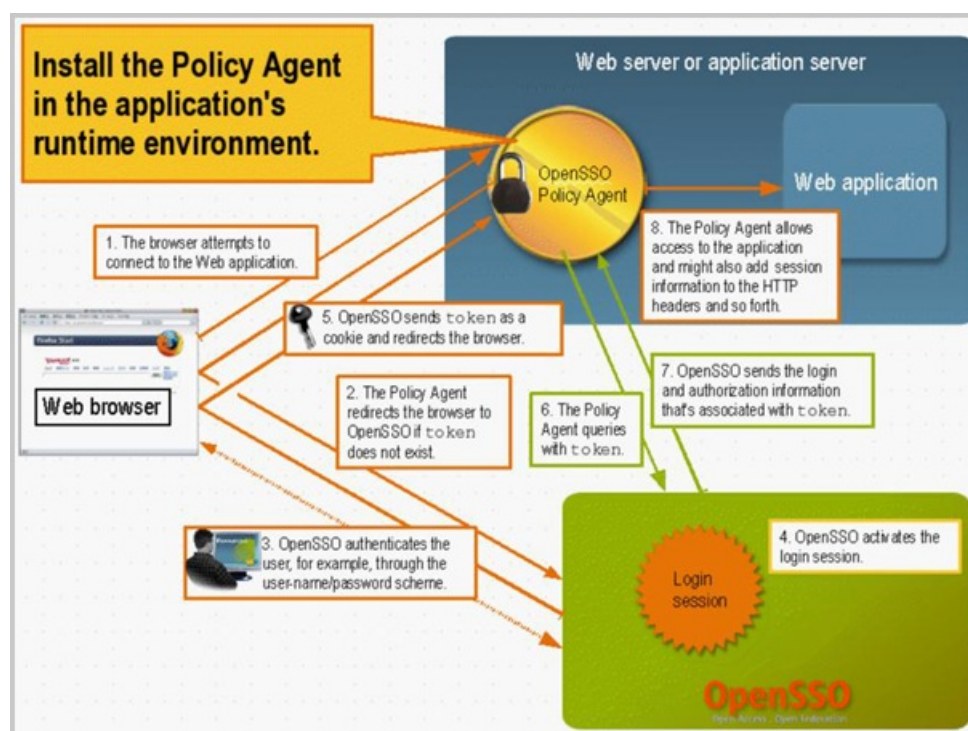
Tempo UI-FW supported by OpenSSO architecture in general
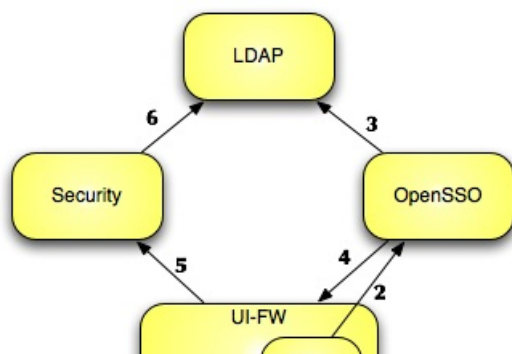
1. User access UI-FW
2. Agent communicates with OpenSSO and see that there is no token available, redirect to OpenSSO login page
3. After the user input the username/password, OpenSSO calls the tempo security for authentication
4. OpenSSO direct back to UI-FW
5. UI-FW calls the tempo security using the OpenSSO token to get the tempo token and simulate the tempo user login.
6. Tempo security should be configured to use LDAP for authentication. It gets the user info from LDAP server and generates the related token.

Detail Design
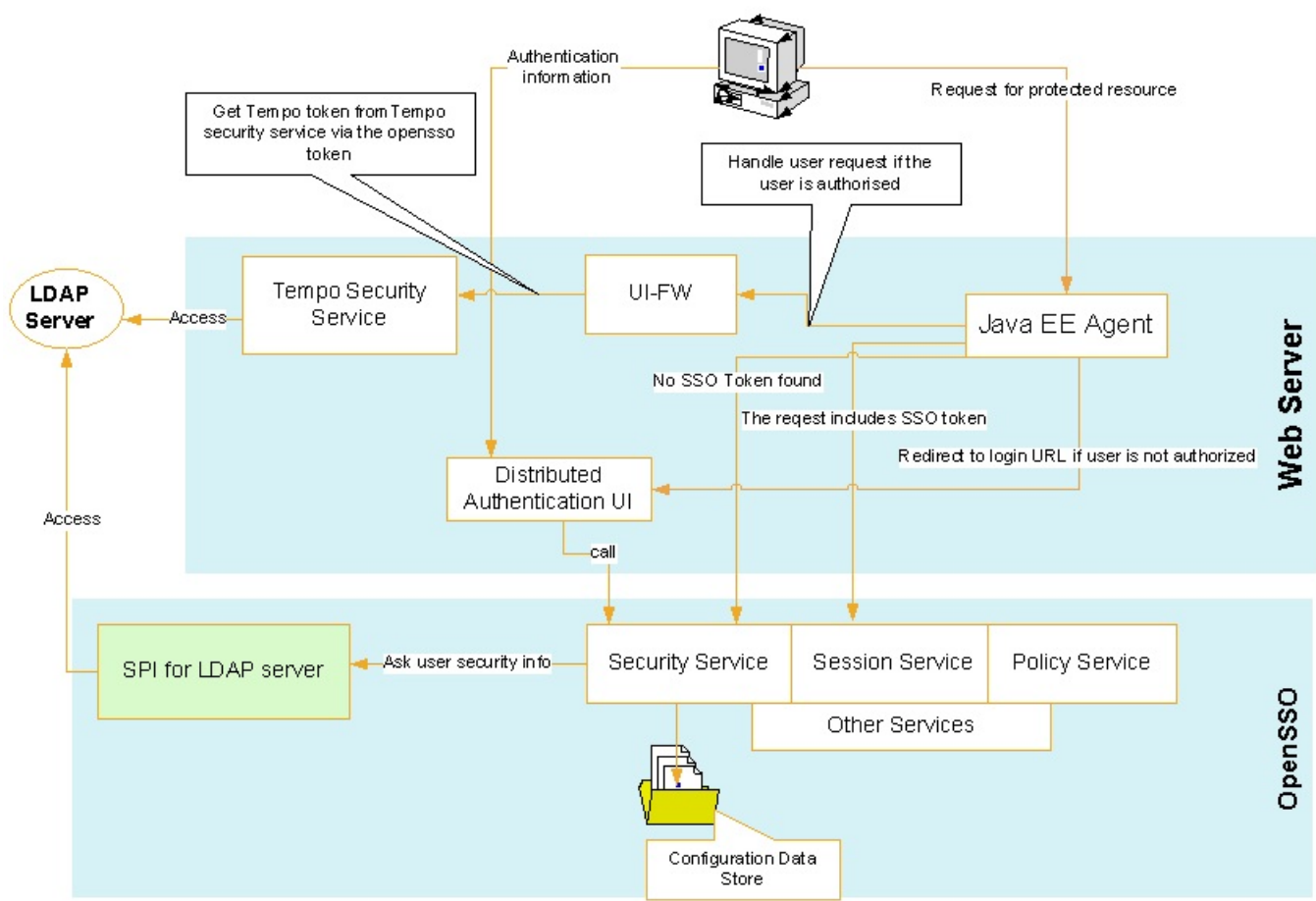
Changes/Enhancement made to the current tempo:

1. Integrate Java EE Agent into UI-FW
2. Enhance tempo security to get the tempo token from OpenSSO token. Because Tempo UI-FW still needs its own security token to do further process. It is necessary to generate the Tempo security token according to SSO token.
3. Extend the OpenSSO to use LDAP server for authentication: SPI for Tempo security service: SPI means Service Provider Interfaces. In here, it is used to access user data in a specified identity repository, the design is to use external LDAP server.
   The implemenatation needs to comply with OpenSSO Authentication Service SPI specification. Document
   https://opensso.dev.java.net/public/use/docs/fampdf/FAMDEVG.pdf provides some guideline and sample about how to implemented.

Reference

Sun OpenSSO Documentation: http://docs.sun.com/app/docs/coll/1767.1
Sun OpenSSO Early Access Documentation: https://opensso.dev.java.net/public/use/docs/fampdf/index.html

Comments