Single Sign-On to TS

Different ways to sign in to a TS application, using an external IDP.

- Token login for apps
- Windows (AD) Authentication

Token login for apps

The URL of the service is **/token**

The following parameters are supported

- create
- login
  - redirect
- renew

For safety allways use HTTPS and only use POST method for transmitting the token

Using the token service

create

Returns a token that can be used for login.

```
https://site.acme.com/TempusServa/token?create
```

```
c8d10470f211c21794849ad0c3aab154
```

login

Creates a session for the user and redirects to the front page

```
https://site.acme.com/TempusServa/token?login=c8d10470f211c21794849ad0c3aab154
```

```
Directs to: https://site.acme.com/TempusServa/main
```

Additionally a custom page can be selected

```
https://site.acme.com/TempusServa/token?login=c8d10470f211c21794849ad0c3aab154&redirect=main?command=com.acme.tspages.CustomPage
```

```
Directs to: https://site.acme.com/TempusServa/main?command=com.acme.tspages.CustomPage
```

renew

Removes old token and creates a new one

```
https://site.acme.com/TempusServa/token?renew=c8d10470f211c21794849ad0c3aab154
```

```
098f6bcd4621d373cade4e832627b4f6
```

delete

Removes old token and creates a new one

```
https://site.acme.com/TempusServa/token?delete=c8d10470f211c21794849ad0c3aab154
```

Windows (AD) Authentication

Understanding AD integration

SSO happens between three entities in the same network domain:

- Tomcat server with TempusServa
- Domain controller (Active Directory)
- Client machine with a user
  - authenticated against the domain controller
  - accessing the TempusServa installation

After the initial contact with the user TempusServa validates the original AD authentication, and logs in the user if a matching username can be found. Optionally TempusServa can synchronize group memberships using regular LDAP querying.

The recommended approach for Tomcat is using a SPNEGO servlet filter mapped to the TempusServa login page. Other integrations methods include

- Waffle (support for other servers)
- Tomcat 7 native SPNEGO

Installing the SPNEGO servlet filter

Note the following guide is for Tomcat 6 or higher.

Installation part 1

The first part of the installation ensures the basic SSO communication is in place.

1. Run pre flight checklist
2. Run installation

Troubleshooting

- Check Tomcat is running in the same context as the domain user
- Ensure only one SPN exists (with fully qualified name)

After a succesfull test you should remove the jsp test file.

Installation part 2

The second part of the installation ensures TempusServa logs in the user based on the Windows authenticated username.

Install the SPNEGO filter on the TempusServa application

1. Copy filter setting from the guide to **<Tomcat>\webapps\<Application>\WEB-INF\web.xml**
2. Change the filter mapping from *.jsp to the login page

```
<filter-mapping>
   <filter-name>SpnegoHttpFilter</filter-name>
   <url-pattern>/login</url-pattern>
</filter-mapping>
```

Configure TempusServa to accept SSO by changing system configuration

```
ssoSpnegoAuthenticate = true
```

Finally restart Tomcat

Testing the setup

Find a suitable user

- Must exist as a Domain User in the AD server (ex. "TESTDOMAIN\DrStrangelove")
- Must exist as a user in Tempus Serva (ex. "DrStrangelove")

Login to a machine connected to the Domain controller

Navigate to the TempusServa login page and check if you are logged in and redirected to the main page.

Other results

- Login displayed with "Login failed" message: The SPNEGO is working but it was not possible to match the Windows authenticated user to a (valid) user in the Tempus Serva database
- Login displayed without any messages: The SPNEGO is NOT working or is deactivated