Zürcher Hochschule
für Angewandte Wissenschaften

Finanzen & Services

Business Applications &
Project Management

ProcessMaker SSO Plugin for IIS

Project name:	Internal
Project leader:	Philipp Hungerbühler
Document date:	22. February 2013

Inhalt

1 Introduction

ProcessMaker (PM) is a workflow and BPM (Business Process Management) Software. In order for designing internal processes and better defining them, the SUS team at the ZHAW has decided to use ProcessMaker as a BPM solution for a pilot project. Some processes have been designed, implemented and tested and are now ready for productive use for a small group of users.

The ZHAW has a lot of users, only some of them will ever use the IT-infrastructure related processes. The open source version of PM provides AD based authentication, however all users with access to PM would have to be imported into PM, before they have access and can us PM functionality.

PM can be installed in a Linux/Apache/MySQL (default) environment and also on IIS 7.5 (this is new). The ZHAW has decided to install PM on a Windows 2008 environment using IIS as web server. The main reason was the available infrastructure and knowledge.

Installed on a Linux environment the Enterprise Plugin for PM allows single-sign-on (SSO) and auto registration. The SSO functionality is not available for Windows based installations. After the initial tests, an introduction to PM and an evaluation of the Enterprise Plugin it became clear, that SSO and auto-registration is a key requirement for the ZHAW.

A first attempt to enable SSO for PM (hardcoded) failed because of missing knowledge. The second approach targeting the implementation of a PM SSO and auto-register plugin for IIS succeeded. This document describes the plugins functionality, the configuration and additional aspects to take into account when using the plugin.

2 Restriction

The ZHAW-SSO Plugin was developed after having a look at the implementation of the default LDAP plugin included in the current version of PM and the ldapAdvanced / windowsSSO plugin which are part of the Enterprise plugin (Copyright © Colosa Inc). The ZHAW-SSO Plugin is not a copy of the Enterprise Plugin code. Only openly available parts were analyzed to understand the implementation of a PM plugin.

The ZHAW-SSO plugin is free code and the ZHAW does not take any responsibilities or provide any support for this plugin. The code can be used as it is.

3 Basic concept

The ZHAW-SSO plugin takes advantage of the Windows Integrated authentication, which can be enabled in IIS. Once enabled (see installation) each request reaching PM will be authenticated be IIS. The corresponding user name can be accessed be checking the $_SERVER[“REMOTE_USER”] server variable.

The open source version by default does not provide a hook for bypassing the sysLogin screen, which is called and rendered even before the system is fully initialized. At the point when the login is shown the different plugins are still not loaded and cannot be accessed. This proved to be a challenge.

The resulting solution was to implement a small hack for the base PM framework. This hack consists of three files of the base PM framework, which were slightly extended to add a SSO hook.

Attention: As a result of these small changes to the base framework the plugin depends on the used version of PM. The plugin was only tested on PM 2.0.44. For previous or future versions of PM the changed files may need to be adapted.

4 Functionality

AS of writing this document the ZHAW-SSO plugin provides the following functionality:

- **Normal LDAP authentication:** If the IIS Windows Integrated authentication is not activated (the server variable is not set), the plugin provides the same functionality as the normal LDAP plugin (authenticating users by performing an LDAP bind).
- **SSO login, bypassing sysLogin:** When IIS Windows Integrated authentication is activated; IIS will set the REMOTE_USER variable to the users name. This user name is then taken for initializing PM, assuming, that this user is authenticated. PM does not have a password for this user; therefore a LDAP bind authentication is not possible. Once authenticated through the SSO plugin, the user is forwarded to his last location in PM.
- **Auto-registration:** If the user is not registered in PM, but is returned by the configured LDAP filter, a new user account is generated the first time the user logs in.
- **Auto-group-assignment**: When defining the authentication source and enabling automatic registration for users, it is possible to define a default user group. New users added through auto registration will be automatically added to this group. Currently only one group can be defined.
- **Revert to normal sysLogin:** In order for accessing the normal sysLogin (for example to login as Admin), a user can use the normal logout functionality. This will forward to the sysLogin and allow a normal login. A reload of the page will again perform a SSO login.
- **Web services:** The PM web services were not tested with SSO (open task). For the moment it is recommended to us a PM account when accessing the web services.

5 Installation

5.1 Installing PM on IIS

Installation of PM version 2.0.44 on IIS requires the following steps:

- Install a Windows Server 2008 R2 and install the IIS role.
- Download and install the Microsoft Web Platform Installer 4.0.
- Install the following options using the Web Platform installer:

  - PHP 5.3.16
  - MySQL
  - IIS recommended configuration
  - PHP manager
  - IIS rewrite 2.0 (important)
- Download PM 2.0.44 and copy the content to a folder below webroot (is not really necessary, it can be another directory).
- Configure a new IIS web pointing to PMFolder\workflow\public_html.
- PM should now already start in installation mode, telling about missing access rights to different folders. The Default user should have write access to the following folders:
  - pocessmaker/workflow/engine/config/
  - processmaker/workflow/engine/xmlform/
  - processmaker/workflow/public_html/
  - processmaker/workflow/engine/plugins/
  - processmaker/shared/
- After providing the MySQL account and password the basic PM installation on IIS should be up and running.

Other configurations:

- There are several PHP extensions (mainly MySQL) which then should be enabled in the PHP.ini file.
- In order for cron.php to work, php.exe needs to be part of the PATH environment variable.

5.2 Hotfix

PM version 2.0.44 comes with several small bugs concerning some core functionality. All this fixes are NOT related to the plugin, but improve the stability of some core functionality, which is not working as expected in version 2.0.44. The following fixes need to be applied:

- In order for the LDAP import to work, the file class.ldap.php should be taken from version 2.0.40 (rbac\engine\classes\plugins\class.ldap.php).
- In file workflow\engine\methods\processes\processes_Import_Ajax.php the missing PHP start tag (PHP) needs to be added at the top ("<?PHP" instead of "<?").
- In file workflow\engine\classes\class.spool.php on line 344 the code needs to be adjusted:

  $oPHPMailer->SMTPAuth = (isset($this->config['SMTPAuth']) ? ($this->config['SMTPAuth'] == "true"? true : false) : false);

The following two fixes are not critical, but help to prevent missing content in certain cases.

- In file class.system.php an additional check needs to be added on line 904:

```
if (!$customSkins) {
        $customSkins = array();}
```

- In file class.xmlform.php an additional check needs to be added on line 4384:

```
if (glob($filesToDelete)){
    foreach (glob($filesToDelete) as $fileToDelete) {
            @unlink($fileToDelete);
    }
}
```

5.3 Installing the ZHAW-SSO plugin

The plugin cannot be installed using the plugin manager. Currently it is not available as archive. Therefore the content of the ZIP should be extracted to the plugins folder (processmaker\workflow\engine\plugins) by hand. The structure is as follows:

```
pmzhawsso.php
pmzhawsso
        data
                class.pmzhawsso.php
        documentation
                121214_PM_IIS_SSO.PDF (this file)
        patch
                main.php
                sysGeneric.php
                sysLogin.php
        class.pmzhawsso.php
        pluginConfig.ini
        pmzhawsso.xml
        pmzhawssoEdit.xml
        VERSION
        zhawLogin.php
        zhawLoginVerify.php
```

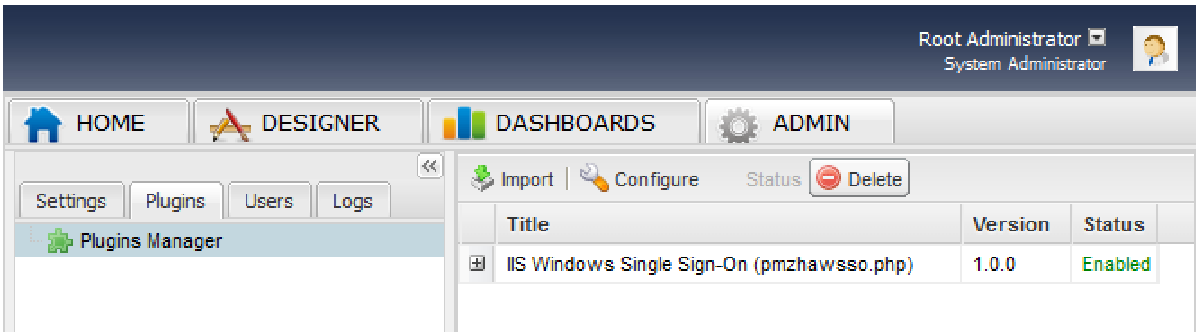
Once the plugin files are copied to the plugins folder, the three patch files need to be copied to the corresponding folders (overwriting the original files). Make a copy of the original files.

File	Target
main.php	processmaker\workflow\engine\controllers
sysGeneric.php	processmaker\workflow\public_html
sysLogin.php	processmaker\workflow\engine\methods\login

While the pmzhawsso plugin is not enabled, the normal operation of the PM environment is not changed by coping above files.

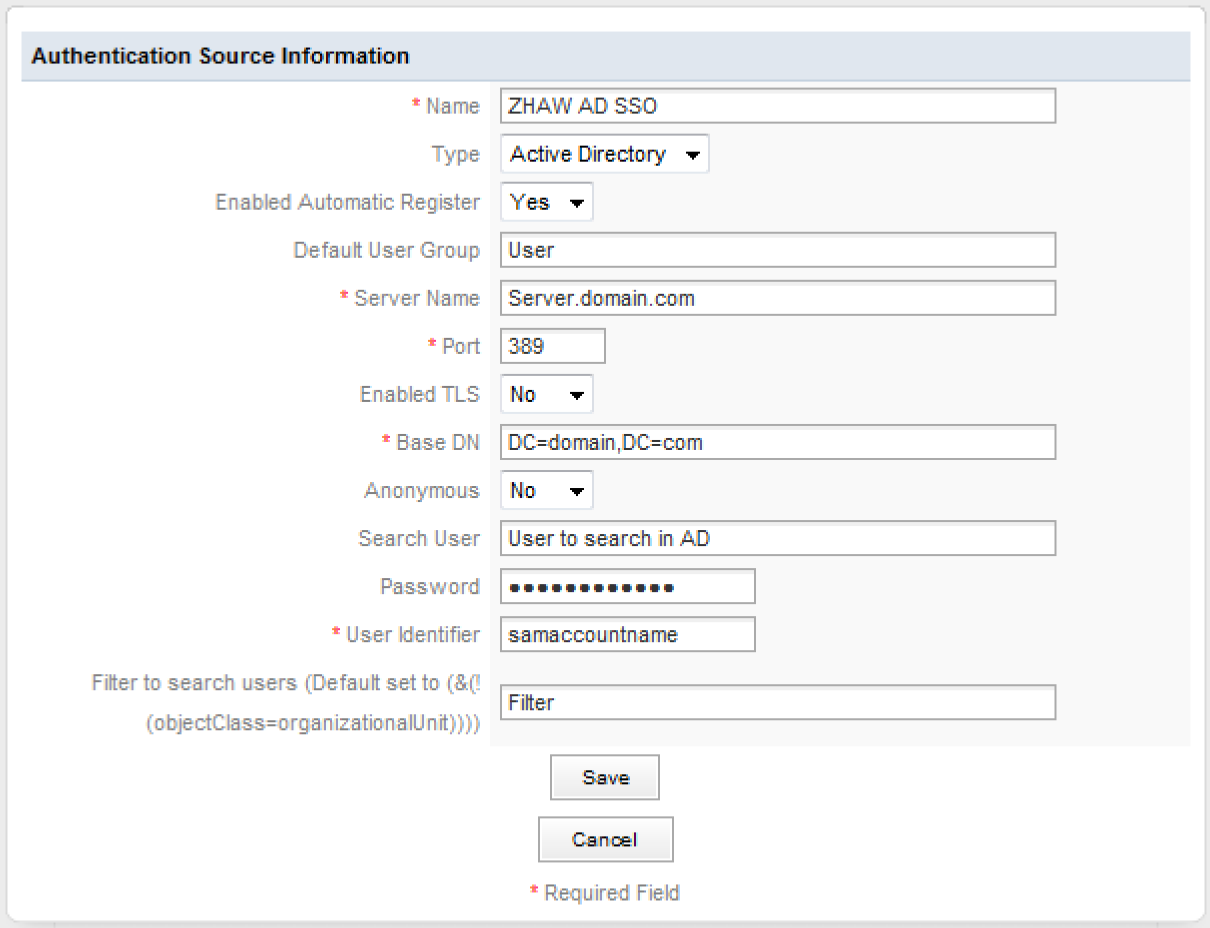
5.4 Configuration

Now the new plugin should be visible under Plugins in the PM user interface. It can now be activated.



Title	Version	Status
IIS Windows Single Sign-On (pmzhawsso.php)	1.0.0	Enabled

Once activated a new authentication source needs to be configured.



Authentication Source Information

* Name	ZHAW AD SSO
Type	Active Directory
Enabled Automatic Register	Yes
Default User Group	User
* Server Name	Server.domain.com
* Port	389
Enabled TLS	No
* Base DN	DC=domain,DC=com
Anonymous	No
Search User	User to search in AD
Password	●●●●●●●●●●●●●
* User Identifier	samaccountname
Filter to search users (Default set to (&(!(objectClass=organizationalUnit))))	Filter

* Required Field

Field	Description
Name	Name of the authentication source.
Type	Type (= AD).
Enabled Automatic Register	Depending if automated registration is required or not.
Default User Group	If defined, new users will automatically be added to this group.
Server Name	The domain controller.
Port	The port to connect to the domain controller.
Enable TLS	Should TLS be enabled?
Base DN	(important) Where users should be searched.
Anonymous	Normally = no.
Search User	The user name to connect to the domain controller. Should have rights to also retrieve members of groups.
Password	The corresponding password.
User Identifier	The id to use for identifying a user, normally samaccountname.
Filter to search users	(important) Additional filter for searching in the AD.

Comment to the AD search filter: An example for a search filter would be:

```
(&(objectClass=user)(memberof=CN=GroupName,OU=OUNAME,OU=OUName,OU=OUName,DC=domain,DC=com))
```

This filter for example gives access to all users which are member of the group GroupName.