PfizerAuthentication API Guide

# Table of Contents

[Table of Contents 2](#_Toc347751806)

[1 Introduction 3](#_Toc347751807)

[2 Nomenclature 3](#_Toc347751808)

[3 Requirements 4](#_Toc347751809)

[4 Module Setup Walkthrough 4](#_Toc347751810)

[4.1 Installation 4](#_Toc347751811)

[4.2 Configuration 5](#_Toc347751812)

[4.3 Login feature (by Janrain Service Provider) 5](#_Toc347751813)

[4.4 Login feature (with IDP initiated) 6](#_Toc347751814)

[4.5 Auto login link 6](#_Toc347751815)

[4.6 Logout feature 7](#_Toc347751816)

[4.7 Displaying user information 7](#_Toc347751817)

[4.8 Additional configurations/features 9](#_Toc347751818)

[4.8.1 Configuring IDP initiated settings 9](#_Toc347751819)

[4.8.2 Configuring external javascripts 9](#_Toc347751820)

[4.8.3 Configuring Drupal’s user settings 9](#_Toc347751821)

[4.8.4 Configuring Janrain settings 9](#_Toc347751822)

# **Introduction**

The purpose of this document is to provide a straightforward walkthrough guide to enable Pfizer Authentication (Pfizer Account Center and Employees) on any Pfizer Drupal site. This feature is currently available only for Managed Cloud sites.

# **Nomenclature**

* Pfizer Authentication

Pfizer Authentication is a Drupal module that makes easier to setup Pfizer Account Center and Employees authentication, where healthcare professionals can register once with Pfizer and then be able to access appropriate information across a range of Pfizer sites.

* JanRain

JanRain offers Software as a Service (SaaS) solutions to connect applications to the social web and other networks. This project leverages two of their products:

* ***JanRain Engage***

A turnkey social login and social sharing solution. Janrain Engage lets a website's visitors register or login with their existing social network accounts from Facebook, Google, Twitter, Yahoo, LinkedIn or other networks, and share content or their site activities with friends on multiple social networks. Additional functionality lets users import their social network profile data and invite their friends to visit a website.

* ***JanRain Federate***

A turnkey single sign-on solution that lets users register or login once for multiple web properties or partner sites.

* Pfizer Account Center (PAC)

PAC is an application where Health Care Professionals (HCPs) can register and have access to several other sites within Pfizer’s organization.

* Single Sign-On

Single sign-on (SSO) is a session/user authentication process that permits a user to enter one name and password in order to access multiple applications. The process authenticates the user for all the applications they have been given rights to and eliminates further prompts when they switch applications during a particular session.

* Drupal

Drupal is a free software package that allows you to easily organize, manage and publish your content, with an endless variety of customization.

Currently there are two platforms where Drupal sites can be served from:

* ***Drupal Gardens (DG)***

Site builder platform in a Software as a Service (SaaS) model. Non-complex sites are easily created through an interface and can be production-live within minutes.

* ***Managed Cloud (MC)***

The platform of choice when talking about custom Drupal site development for Pfizer, Managed Cloud is a Platform as a Service (PaaS) where complex sites are deployed.

# **Requirements**

* Domain whitelist

The site domains (development, testing and production environments) need to be whitelisted in Janrain Dashboard. There are currently the following domains in our whitelist:

* + - localhost
    - \*.local
    - \*.localhost
    - \*.acquia-sites.com
    - www.pfizer.edrupalgardens.com
    - webinars.local
    - toviaz1.net.quodem.net
    - \*.champix-uat.co.uk
    - pfizerline.localhost
    - \*.pfizer.com
* Public pages

The module requires public access to the following URLs:

* <http://[site-domain]/pfizer-auth/redirect>
* <http://[site-domain]/xdreceiver>

These URLs must be accessible to anonymous users, and must be excluded from any rule of “access denied” or redirection.

* SSL

All transactions occur through secure protocol. HTTPS has to be supported before the installation of the module.

* Drupal Managed Cloud Platform

This module is currently available only for MC sites.

# **Module Setup Walkthrough**

## Installation

To setup Pfizer Authentication in a Drupal site, you first need to install/enable the following modules:

* Janrain (<http://drupal.org/project/rpx>)
  + Janrain Engage Core
  + Janrain Engage UI
  + Janrain Engage Widgets
* Token (<http://drupal.org/project/token>)
* Token Filter (<http://drupal.org/project/token_filter>)
* Pfizer Authentication (<https://github.com/pfizer/pfizer_auth>)

## Configuration

Configure Pfizer Authentication module (*Configuration » People » Pfizer Authentication* or access the URL /admin/config/people/pfizer-auth):

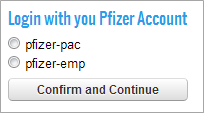
* Pfizer Authentication Settings: There must be at least one SAML provider enabled if the site uses the authentication service provided by PAC or Employees. If the site uses the IDP initiated, there is no need to enable these providers (see section 4.4).

You can also configure if the login interface opens inside a modal overlay or in a window popup. Note that the overlay is not applicable for stock browsers (Internet Explorer and Safari) due to privacy limitations.

* Other configurations can be left with the predefault values. More information about these settings can be found in the section 4.8.

## Login feature (by Janrain Service Provider)

The system should have a login interface where the user can choose the SAML provider. In the following image we have an example of this interface:



To create this login interface, you can create a new Drupal block and insert this HTML into it (Full HTML filter):

<h2>**Login with your Pfizer Account**</h2>

<div id=**"pfizer-auth-saml-providers"**>&nbsp;</div>

<input id=**"pfizer-auth-login-submit"** type=**"button"** value=**"Confirm and Continue"** />

<script type=**"text/javascript"**>

**var** providers **=** Drupal.settings.pfizerAuthentication.SAMLProviders**;**

**var** providerList **=** jQuery**(**'#pfizer-auth-saml-providers'**);**

**if** **(**providers.length **>** 0**)** **{**

**for** **(var** x **in** providers**)** providerList.append**(**jQuery**(**'<label>'**).**text**(**providers**[**x**]).**prepend**(**jQuery**(**'<input>'**).**attr**({**

'type' **:** 'radio'**,**

'name' **:** 'pfizer-auth-saml-providers'**,**

'value' **:** providers**[**x**]**

**})));**

**if** **(**providers.length **==** 1**)** jQuery**(**':radio'**,** providerList**).**attr**(**'checked'**,** 'checked'**);**

**}**

jQuery**(**'#pfizer-auth-login-submit'**).**click**(function(){**

**var** provider **=** jQuery**(**':radio:checked'**,** providerList**).**val**();**

PfizerAuthentication.login**(**provider**);**

**});**

</script>

Once the user clicks on “Confirm and Continue” button, an external login page should be shown (in a modal overlay or window popup) so the user can enter its credentials and authenticate into the application. As the EMP provider authenticates the user automatically through the network, this provider does not display any login interface.

**Note:** this structure is a generic example that covers all the basic scenarios and allows the user to choose the identity provider. To build a custom interface, the unique requirement is to trigger the JavaScript function *PfizerAuthentication.login(provider)*.

## Login feature (with IDP initiated)

The IDP initiated form does not call an external window so the HCP can enter the credentials. The form is already embedded on the page.

After enabling the Pfizer Authentication module, check the “*[Pfizer Authentication] PAC Login form*” block in blocks configuration page (Administration » Structure » Blocks). Drag the block to the appropriated theme region and save.

Note that the form has a default style, but it can be disabled or customized (by overriding the rules) for specific themes.

## Auto login link

If an application needs to auto-login user then they can use an “auto login link” in the following format:

*https://qa.pfizerpro.com/sites/registration/pages/CheckSso.aspx?successUrl=https%3A%2F%2Fdevfederate.pfizer.com%2Fidp%2FstartSSO.ping%3FPartnerSpId%3D****<PARTNER\_SP\_ID>****%26TARGET%3D****<TOKEN\_HANDLER>****&failureUrl=****<FAILURE\_URL>***

The bold faced parameters should be replaced appropriately following the table below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Parameter** | **Description** | **Example URL** | **Value to be used** |
| **PARTNER\_SP\_ID** | SSO Server (encoded URL) | https://dm-sso.pfizer.com | https%3A%2F%2Fdm-sso.pfizer.com |
| **TOKEN\_HANDLER** | Janrain token handler + optional Drupal destination parameter (encoded URL) | https://pfmrobitussdev.prod.acquia-sites.com/rpx/token\_handler?destination=/e-details/ed\_0001 | https%3A%2F%2Fpfmrobitussdev.prod.acquia-sites.com%2Frpx%2Ftoken\_handler%3Fdestination%3D%2Fe-details%2Fed\_0001 |
| **FAILURE\_URL** | Target URL in case authentication fails | https://pfmrobitussdev.prod.acquia-sites.com/pac/idp | https://pfmrobitussdev.prod.acquia-sites.com/pac/idp |

## Logout feature

To get the Single Sign Off feature working (user should log out from all the applications at once), the system need to call a javascript function when the user clicks on the log out link. Example:

<script type=**"text/javascript"**>

jQuery(document).ready(function(){

// Prevent the user from opening the logout page

  jQuery("a.logout-link").attr('href', 'javascript:void(0);');

// Trigger the logout function when user clicks on the logout link

jQuery("a.logout-link").click(**function**(event){

     event.preventDefault();

    PfizerAuthentication.logout();

  });

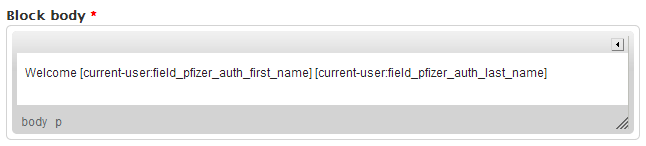
});

</script>

**Note:** Change the "a.logout-link" selector to your own logout link selector.

## Displaying user information

SAML providers can also provide additional user information upon login, such as first and last name, addresses, etc. This data is stored in the session and also in the Drupal’s user account. To access these information, you can use Tokens in combination with the module Token Filter:

The tokens are commonly used inside node contents or blocks due to the ease and speed of setting up through Drupal’s interface.

*The string “Welcome [current-user:field\_pfizer\_auth\_first\_name] [current-user:field\_pfizer\_auth\_last\_name]” will be replaced dynamically by token values.*

The tokens available are based on the fields available and can be accessed in Help > Token (/admin/help/token). The user information tokens to be used are under the “Current user” section.

Example: Displaying some user information:

<h2>**Profile**</h2>

<ul>

<li><b>**First name:**</b> **[current-user:field\_pfizer\_auth\_first\_name]**</li>

<li><b>**Last Name:**</b> **[current-user:field\_pfizer\_auth\_last\_name]**</li>

<li><b>**Email:**</b> **[current-user:field\_pfizer\_auth\_email]**</li>

<li><b>**Created:**</b> **[current-user:field\_pfizer\_auth\_created]**</li>

<li><b>**Postal address:**</b> **[current-user:field\_pfizer\_auth\_postal\_address]**</li>

<li><b>**Postal code:**</b> **[current-user:field\_pfizer\_auth\_postal\_code]**</li>

<li><b>**Preferred username:**</b> **[current-user:field\_pfizer\_auth\_pref\_username]**</li>

<li><b>**Telephone Number:**</b> **[current-user:field\_pfizer\_auth\_phone\_number]**</li>

</ul>

<h2>**PAC provider**</h2>

<ul>

<li><b>**Subject:**</b> **[current-user:field\_pfizer\_auth\_subject]**</li>

<li><b>**PFPZip:**</b> **[current-user:field\_pfizer\_auth\_pfp\_zip]**</li>

<li><b>**Party ID:**</b> **[current-user:field\_pfizer\_auth\_party\_id]**</li>

<li><b>**Groups:**</b> **[current-user:field\_pfizer\_auth\_groups]**</li>

<li><b>**Categories:**</b> **[current-user:field\_pfizer\_auth\_categories]**</li>

</ul>

<h2>**EMP provider**</h2>

<ul>

<li><b>**UID:**</b> **[current-user:field\_pfizer\_auth\_uid]**</li>

<li><b>**Group:**</b> **[current-user:field\_pfizer\_auth\_emp\_group]**</li>

</ul>

**Important:** make sure to enable the “Replace tokens” filter in the text formats (/admin/config/content/formats)

## Additional configurations/features

Although the module is ready to go, maybe the project can have some different requirements. Below are some custom settings and features supported by the module.

### Configuring IDP initiated settings

Some IDP initiated URLs can be configured. They are related to success in login, Single Sign Off and registration URLs, and error messages (when the authentication fails).

**Login action URL Example:**

<https://qa.pfizerpro.com/sites/registration/pages/Login.aspx?resume=/idp/eQ6ON/resumeSAML20/idp/SSO.ping&amp;spentity=https://dm-sso.pfizer.com>

**Login success URL Example:**

[https://devfederate.pfizer.com/idp/startSSO.ping?PartnerSpId=https://dm-sso.pfizer.com&TARGET=[pfizer-auth:token-handler-url](https://devfederate.pfizer.com/idp/startSSO.ping?PartnerSpId=https://dm-sso.pfizer.com&TARGET=%5bpfizer-auth:token-handler-url)]

Available token: [pfizer-auth:token-handler-url] – token validation callback URL.

**Logout URL Example:**

<https://accountcenter.pfizer.com/sites/registration/pages/Logout.aspx>

**Registration URL Example:** [https://qa.pfizerpro.com/sites/registration/pages/registration.aspx?CampaignID=1-26435951:1-26435967&**successURL=https%3A%2F%2Fdevfederate.pfizer.com%2Fidp%2FstartSSO.ping%3FPartnerSpId%3Dqf3.pfizer.com%26TARGET%3Dhttps%3A%2F%2Fqa3proxies.pfizer.com%2Firj%2Fservlet%2Fprt%2Fportal%2Fprtroot%2Fcom.wyeth.security.auth.HCPLogin&siteID=2**](https://qa.pfizerpro.com/sites/registration/pages/registration.aspx?CampaignID=1-26435951:1-26435967&successURL=https%3A%2F%2Fdevfederate.pfizer.com%2Fidp%2FstartSSO.ping%3FPartnerSpId%3Dqf3.pfizer.com%26TARGET%3Dhttps%3A%2F%2Fqa3proxies.pfizer.com%2Firj%2Fservlet%2Fprt%2Fportal%2Fprtroot%2Fcom.wyeth.security.auth.HCPLogin&siteID=2)

Please note that successURL parameter in this case is pointing to development and siteID is different across sites.

Servers:

|  |  |  |
| --- | --- | --- |
|  | **Development** | **Production** |
| **PAC** | [qa.pfizerpro.com](http://qa.pfizerpro.com/) | [accountcenter.pfizer.com](https://accountcenter.pfizer.com/sites/registration/pages/Logout.aspx) |
| **PingFederate** | [devfederate.pfizer.com](http://devfederate.pfizer.com/) | prodfederate.[pfizer.com](http://pfizer.com/) |
| **Site ID** | Site specific | Site specific |

### Configuring external javascripts

External files might be generic for most of the sites. They are responsible for Single Sign on/off, cross domain requests and connection between Drupal, Janrain and the Identity Provider. In specific cases, they can be customized to supply the requirements. The new javascript urls can be set in the Pfizer Authentication module settings.

### Configuring Drupal’s user settings

To get the Pfizer Authentication module working, the site must allow visitors to register accounts. This way, the module can create accounts for users authenticated externally.

Also, the site should not require a verification email when users create their accounts, as they are already verified by the Identity Provider. The default “Welcome email” (Drupal’s core feature) is disabled automatically after the Pfizer Authentication installation.

**Important:** There is an issue in Drupal that does not allow enabling/disabling the email messages triggered after account creation. The MailControl module (<http://drupal.org/project/mailcontrol>) makes these settings fully customizable. This is recommended for Drupal sites that uses Pfizer Authentication and also triggers these notification emails.

### Configuring Janrain settings

* API key: The same API key should be used for most of Pfizer sites. In case of a new API key is provided to a specific site, it can be changed through the configuration pages.
* Engage on sign-in forms: As Pfizer Authentication uses a custom call to the Identity Provider, the default login buttons (Gmail, Twitter, Facebook, etc.) are disabled. But if the site uses other external Identity Providers, this option should be enabled.
* Request extended profile data: To be able to access user information upon login, this option must be enabled. See section 4.7 to see how to retrieve this information.
* Bypass email verification: this option can be customized if the site requires the system to send an email when users access the site for the first time (when the account is created). The message content can also be customized.