dimelo
Drive profitable conversations

Feedback 2.0 SSO link setup

DIMELO
29, rue du Louvre 75002 PARIS
Tél.: + 33(0)1 48 56 88 25
Fax. : + 33(0)1 74 18 00 14

1. Introduction

This document describes the Dimelo SSO link feature and provides the technical document to implement it.

To be enabled the sso link feature needs to be activated in the Dimelo back-office.

In this document the « Authentication server » is the Dimelo application that manage users and application accounting. Its url has the following pattern: https://your_community_name.users.dimelo.com.

2. Feature description

The SSO feature is a url to be generated per user and shared as a hypertext link in a web page, an email, ...

This link will create and/or connect users on the Dimelo applications. The main use is to provide your own user a seamless experience between your web application and the Dimelo application: they will keep there identity from your application to your Dimelo application.

The Dimelo sso link has the following form:

https://AUTHENTICATION_SERVER_HOSTNAME/cas/login?auth=sso&type=acceptor&service=DIMELO_APPLICATION_TARGET_URL&uuid=UNIQUE_USER_IDENTIFIER&token=TOKEN&expires=EXPIRATION_DATE...

The SSO link feature principle is simple. When a user browse this link, he willl be directed to your Dimelo authentication server. The url parameters are then checked (see token calculation section):

If the parameters are correct:

- If no account already exists with the UUID provided in the url, a new account is created with the parameters provided (uuid, firstname, lastname, email, …). The user is redirected to the Dimelo application target url and is logged as the new account identity
- If an account with this uuid already exists, the account parameters are updated, the user is redirected to the application target url and is logged under this account

3. SSO link parameters

Parameter	Token into account during token creation ?	Mandatory ?	Value example	Format
auth	NO	YES	sso	«sso»
type	NO	YES	acceptor	«acceptor»
service	NO	YES	http://mondomain.ideas.dimelo.com	Valid url
firstname	YES	YES	Renaud	Alphabetical, figures, simple quote, dash
uuid	YES	YES	uniq_identifier_12	Any character valid in a url. Usually a internal id or username
expires	YES	YES	1249081200	Timestamp UNIX (= POSIX date)
token	NON	YES	bfc9396b7c710746b19a1297e70d1716	Hexadecimal string
avatar_url	YES	NO	http://google.com/logo.png	Valid image url
email	YES	NO	renaud.morvan@dimelo.com	Valid email address
lastname	YES	NO	Morvan	Alphabetical, figures, simple quote, dash
charset	NO	NO	latin1	« latin1» or «latin15» or «winlatin1»
custom_field_*n* with *n* between 1 and 10	YES	NO	Custom value	Any character valid in a url.

4. Mandatory SSO parameters

- **auth** : MUST be **sso**.
- **type** : MUST be **acceptor.**
- **service** : Dimelo application where you want the user to be redirected, usually something like http://yourapp.ideas.dimelo.com.
- **firstname** : user firstname (or nickname).
- **uuid** : unique identifier (e.g. : email or id in your database ou son username in your application).
- **expires** : expiration time value under UNIX time format (http://en.wikipedia.org/wiki/Unix_time). This is the time when this sso link will be expired (and thus useless).
  Example: you generate the sso link 2009 august the first at 00:00 and you want it to expire an hour later. Then expires parameter should be 1249081200 (1249077600 + 3600). You don't have to worry about your timezone as this format is NOT timezone dependent.
- **token** : This is an hexadecimal string calculated from the parameters, its purpose is to sign the parameters so that Dimelo can check if someone try to modify them: If a parameter is spoofed the token check will fail and the sso link will not be taken into account (cf: token calculation section).

5. Optional parameters

- **avatar_url** : URL of a user avatar (must be a picture).
- **email** : user email, if you don't provide this parameter, the user will not be notified in case of new comment.
- **lastname** : user lastname.
- **charset** : Parameter encoding (Cf: Parameter encoding section).
- **custom_field_*n*** : with *n* between 1 and 10, this field is free to use and can be used as needed.

When an optional parameter is passed with an empty value to an existing account, the account's attribute will be cleared, whereas if the attribute is not passed at all, it will be left untouched.

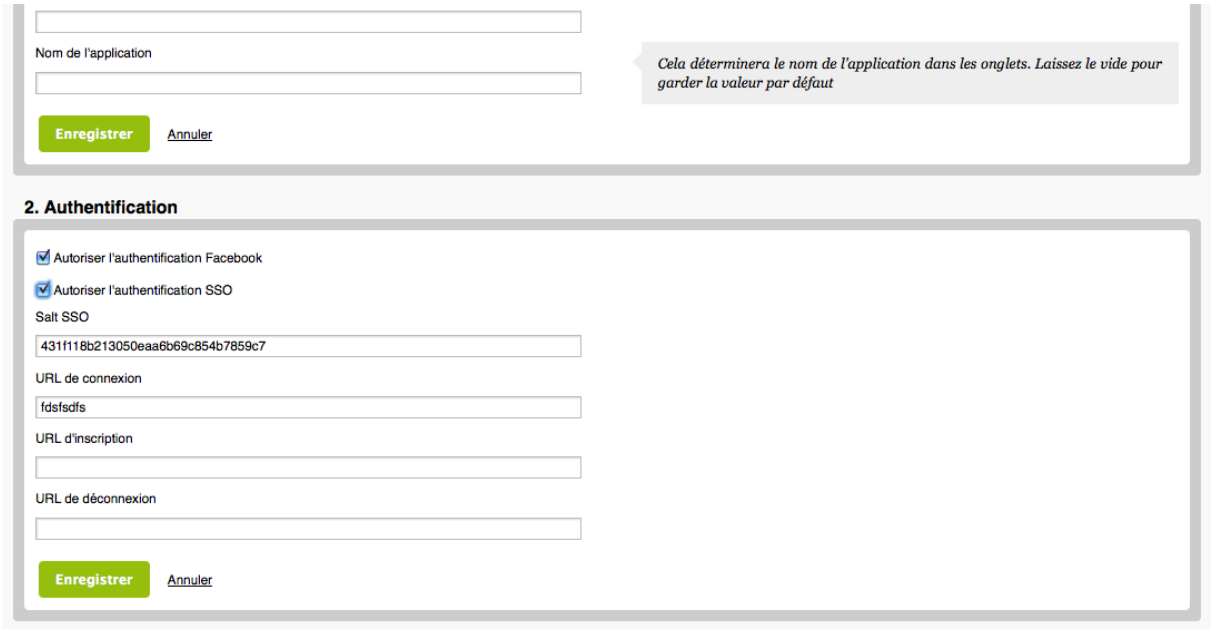
6. Token calculation prerequisite

In order to calculate the token you need a shared password between your application and Dimelo which is called the **salt**.

This salt is specific per application (if you have more than one). You need to use the salt corresponding to the application in the service parameter (**DIMELO_APPLICATION_TARGET_URL**).

You can get this this salt in the Dimelo authentication server back-office, in the application tab, click on modify.

You should get the following screen:



7. Token calculation

Lets consider a user with the following parameters:

auth: sso
type: acceptor
firstname : Jean
email :jp@mail.com
uuid: jpmar0112
avatar_url: http://avatar.com/jp.png
expires: 1300000000 (march 11th 2011 at 08:06:40)

The only parameters to be taken into account in the token calculation are : **avatar_url**, **email**, **expires**, **firstname**, **lastname**, **uuid** and all the **custom_field_*n*** (See parameter table in SSO link parameters section).

Any other parameters (**auth**, **type**, **service**, …) **MUST not be taken into account** in the token calculation (or in the token concatenation) but are mandatory in the url.

The token purpose is to "sign" the parameters in the sso link so that nobody can modify them and thus gain ungranted access.

In order to generate this token, you first have to concatenate them (in a certain order), and then use the SHA1 hash function to obsuscate the result. This is the token.

The concatenation should be done carefully:

- you have to concatenate parameters in **alphabetical order** (avatar_url, custom_field_1, custom_field_10, custom_field_2, …, custom_field_9, email, expires, firstname, uuid)
- You only have to concatenate parameters that are present in the URL even if the value is empty
- You only have to concatenate parameters that should be taken into account in sso calculation (cf sso link parameters)
- each parameter will be concatenated with the parameter name following the following pattern "parameter_name-parameter_value"
- each concatenated parameter are separated by a colon

If should give you a string like this (don't forget the parameter order):

'param1-value1:param2-value2:param3-value3...paramN-valueN'

In our example the concatenated string will then be

params = 'avatar_url-http://avatar.com/jp.png:email-jp@mail.com:expires-1300000000:firstname-Jean:uuid-jpmar0112'

Parameters MUST NOT be url encoded during the token calculation.

Then you have to concatenate this string with the salt:

final = concatenated_params + 'salt'

The token is the result of the sha1 function on this string:

token = sha1(final)

In our example the token will then be bc8d80b2440697c1434298623e1dd441b459cf3b if the salt is bfc9396b7c710746b19a1297e70d1716

This token will be c5b3570f1a2973af44e78bfcb817131535a676a1, which is sha1('avatar_url-http://avatar.com/jp.png:email-jp@mail.com:expires-1300000000:firstname-Jean:uuid-jpmar0112bfc9396b7c710746b19a1297e70d1716')

The complete sso link then is:

https://domain-test.users.dimelo.com/cas/login?auth=sso&type=acceptor&service=http://domain-test.ideas.dimelo.com&firstname=Jean&email=jp@mail.com&uuid=jpmar0112&avatar_url=http://avatar.com/jp.png&expires=1300000000&token=bc8d80b2440697c1434298623e1dd441b459cf3b

8. Character encoding

The character encoding may be different between your website where you calculate the token and the Dimelo platform.
As sha1 is a bit level hash function, you need to add the charset parameter to the sso link.

The Dimelo architecture is built around utf-8 so you only need to provide this parameter if it is not your case and your parameters can be non ASCII.

The charset parameter accept the following value:

Charset parameter value	Encoding name	Informations
latin1	ISO-8859-1	Western latin1.
latin15	ISO-8859-15	Extended western latin1 « € »
winlatin1	CP1252	Microsoft Windows version derived from latin1