



Magento ADMIN SAML Extension User Guide



Table of Contents

1 Introduction.....	4
2 How does it work?.....	5
2.1 Single Sign On.....	5
2.1.1 The normal usage (SP-SSO initiated).....	5
2.1.2 The alternative usage (IdP-SSO initiated).....	6
2.2 Single Log Out.....	7
2.2.1 SP-SLO initiated.....	7
2.2.2 IdP-SLO initiated.....	8
3 Magento ADMIN SAML Settings.....	9
3.1 Status.....	10
3.2 Identity Provider Settings.....	10
3.3 OPTIONS.....	11
3.4 ATTRIBUTE MAPPING.....	11
3.5 ROLE MAPPING.....	12
3.6 CUSTOM MESSAGES.....	12
3.7 ADVANCED SETTINGS.....	12
4 How to configure the Identity Provider.....	15
4.1 Onelogin.....	15
4.2 Okta.....	15
4.3 Ping Identity.....	15
4.4 ADFS 2.0.....	15
4.5 ADFS 3.0.....	15
4.6 Salesforce.....	15
4.7 Google.....	16
4.8 Forgerock.....	16
4.9 ServiceNow.....	16
4.10 Auth0.....	16
4.11 Shibboleth.....	16
4.12 simpleSAMLphp.....	16
4.13 secureAuth.....	16



<u>4.14 clearlogin.....</u>	<u>16</u>
<u>4.15 Identacor.....</u>	<u>16</u>
<u>4.16 Centrify.....</u>	<u>17</u>
<u>4.17 Bitium.....</u>	<u>17</u>
<u>4.18 CA Technologies.....</u>	<u>17</u>
<u>5 Warranty.....</u>	<u>18</u>



1 Introduction

Magento ADMIN SAML extension adds SAML Single Sign On support on the admin login page.

If you are working with a partner that has implemented a SAML identity provider, you can use this extension to interoperate with it, thereby enabling SSO for customers. It works with any IDP providers, including OneLogin, Okta, Ping Identity, ADFS, Salesforce, ...

Has the following features:

- Enable SAML Single Sign On to the backend with this extension simply.
- Connect a Magento instance with any SAML Identity Provider.
- Allow to Login via Identity Provider.
- Possible to single sign on/ log out service Url.
- Easily switch On/Off the Admin SAML Module.
- Provisioning/Auto-update user data.
- Single Sign On (IdP & SP initiated).
- Single Log Out (IdP & SP initiated).
- Just-In-Time Provisioning (user data + roles).
- Auto-provisioning: allow to create a new user with the data provided by the IdP.
- Auto-update: update the account of the user with the data provided by the IdP and Review the Mapping section.
- Possibly set the mapping between IdP fields and Magento fields.
- Roles supported.
- Customizable workflow.
- Easily install and use.



2 How does it work?

In order to perform SSO/SLO, the Identity Provider and the Service Provider may set a circle of trust by exchange its metadata. A metadata is a XML that describes the EntityID, a value that identifies the entity, the endpoints (using on the SSO/SLO process and a certificate, that allow the other part to validate the signature of the SAML message. Once set we will be able to execute SSO and SLO flows. Let's explain them.

2.1 Single Sign On

2.1.1 The normal usage (SP-SSO initiated)

Extension adds a link "Login via Identity provider" at the admin (backend) login form.

The screenshot shows the Magento Admin Panel login interface. On the left is the Magento logo. The main heading is "Log in to Admin Panel". Below this are two input fields: "User Name:" and "Password:". To the right of the "Password:" field is an orange "Login" button. Below the input fields are two links: "Forgot your password?" and "Login via Identity Provider". At the bottom of the form, there is a footer: "Magento is a trademark of Magento Inc. Copyright © 2016 Magento Inc."

The Title and the text of the link is customizable (See Custom Message section).

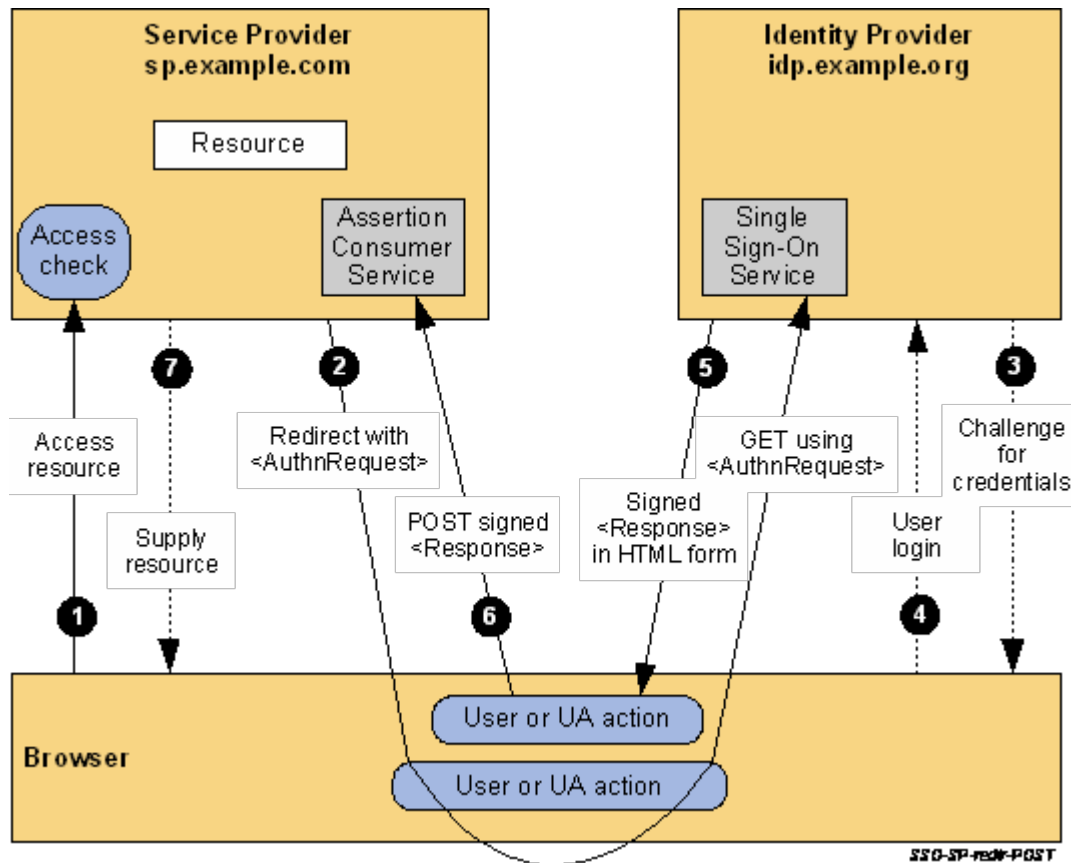
Following the "Login via SAML link" initiates the SP-SSO initiated flow.

The Service Provider (Magento) will send an Authentication Request using the [HTTP-Redirect binding](#), the Identity Provider (if there is not an active user session will a login form in order to allow the user to insert it credentials and after authenticate the user, the IdP may send a SAMLResponse to the Service Provider's Assertion Consumer endpoint ([HTTP-POST binding](#)).



The SAMLResponse must contains the user data that Magento needs in order to log the user (an email) or to provision on the fly an account (user, group and address data).

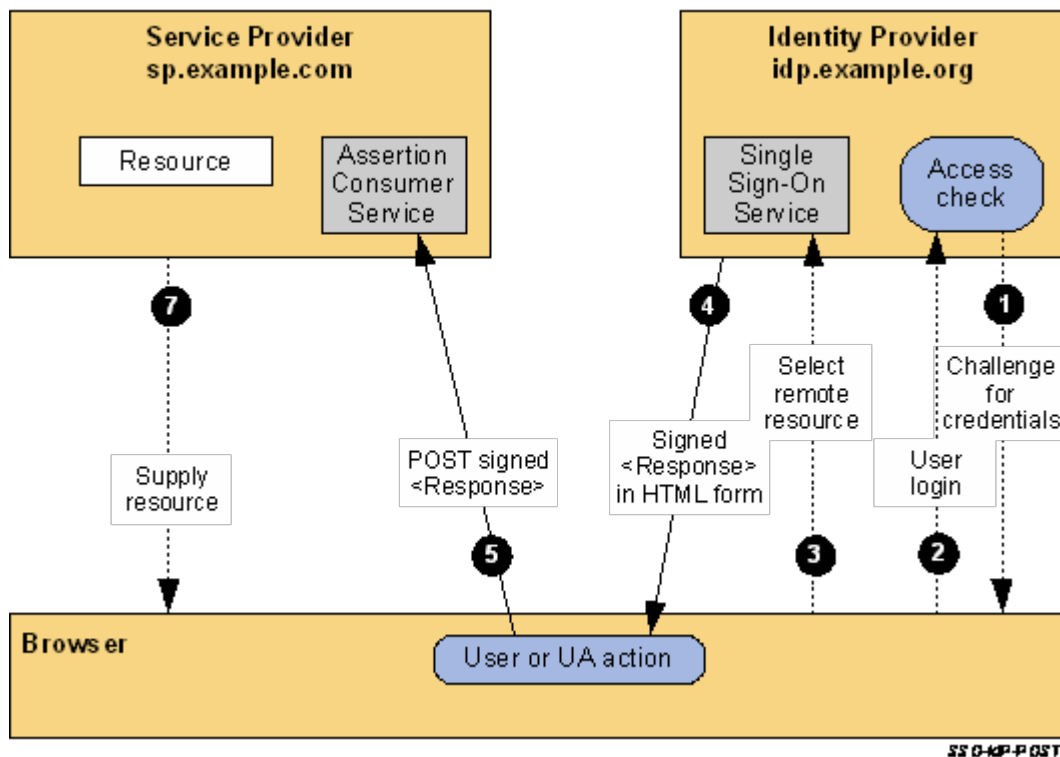
The following diagram details this process.



2.1.2 The alternative usage (IdP-SSO initiated)

Some IdPs like Onelogin or Okta offer a dashboard with the integrated apps.

When you click on the icon of the Magento app, a IdP-SSO initiated flow will happens, this consists in directly send the SAMLResponse to the Service Provider's Assertion Consumer endpoint ([HTTP-POST binding](#)).

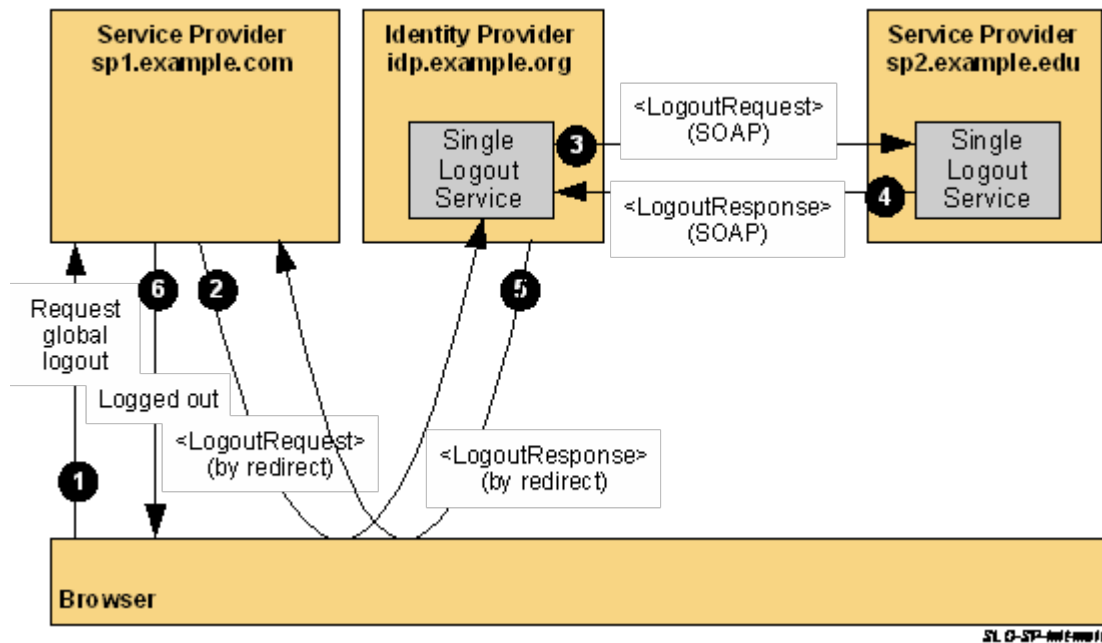


2.2 Single Log Out

The SAML extension also supports Single Log Out using the [HTTP-Redirect binding](#), but you will need to enable it on the SAML setting panel (Options section).

2.2.1 SP-SLO initiated

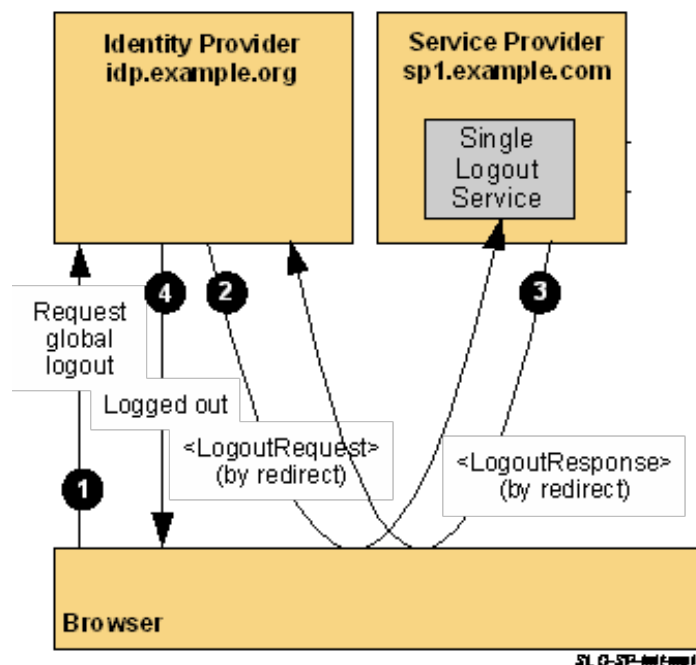
In this scenario the Service Provider (Magento) initiates the Single Logout Process. It will send a LogoutRequest to the Identity Provider, the Identity Provider will close the active sessions (including those SP that initiated a SSO process before) and send a LogoutResponse to the Service Provider. After receive this LogoutResponse and validate it, the Magento session will be closed.



2.2.2 IdP-SLO initiated

In this scenario the Identity Provider initiates the process, it will send a LogoutRequest to each Service Provider that initiated a SSO session and will wait for a LogoutResponse.

The Service Provider after validate the LogoutRequest, will close the Magento session and reply the LogoutResponse to the IdP.





3 Magento ADMIN SAML Settings

The Settings of the extension are available at System > Configuration. At the Services tab, the "SAML (Admin Panel)" link.

There you will be able to fill several sections:

- Status. To enable or disable the extension.
- Identity Provider. Set parameters related to the IdP that will be connected with our Magento.
- Options. The behavior of the extension.
- Attribute Mapping. Set the mapping between IdP fields and Magento user fields.
- Group Mapping. Set the mapping between IdP groups and Magento groups.
- Address Mapping. Set the mapping between IdP fields and Magento address fields.
- Custom messages. To handle what messages are showed in the login form.
- Advanced settings. Handle some other parameters related to customizations and security issues.

The metadata of the Magento Service Provider will be available at http://<magento_base_url>/sso/saml/metadata

If you access to this URL you will be able to "See the source of the page" and see the XML and download it. You need to share this data with the administrator of the Identity Provider in order to let him register the SP metadata there (entityID, endpoints and public certificate if the SP is signing the Messages).

If you are using Magento Multi-site you will be able to configure/enable SAML in each store. Each store will have its own panel/settings.



3.1 Status

When the SAML settings are set, you may enable the SAML feature. The metadata of the SP url is important (you will need to share it with the IdP administrator). Also I recommend to use the value of that URL as the SP EntityID (see advanced settings).

The screenshot shows a configuration window titled "STATUS". It contains the following fields:

- Enabled:** A dropdown menu set to "Yes" with a "[GLOBAL]" label to its right.
- License KEY:** An empty text input field with a "[GLOBAL]" label to its right. Below the field is a small red triangle icon and the text "The License KEY related to the Admin SAML extension".
- Metadata of this SP:** A text input field containing the URL <http://207.171.10.10/magento/index.php/admin/saml/metadata/> with a "[GLOBAL]" label to its right.

3.2 Identity Provider Settings

In this section, you can set up some info related to the IdP that will be connected with your Magento. You can find these values at the Onelogin's platform in the Magento App at the Single Sign-On tab: IdP Entity Id, Single Sign On Service Url, and Single Log Out Service Url.

The screenshot shows a configuration window titled "IDENTITY PROVIDER SETTINGS". It contains the following fields:

- IdP Entity Id:** An empty text input field with a "[STORE VIEW]" label to its right. Below the field is a small red triangle icon and the text "Identifier of the IdP entity. ("Issuer URL")".
- Single Sign On Service Url:** An empty text input field with a "[STORE VIEW]" label to its right. Below the field is a small red triangle icon and the text "SSO endpoint info of the IdP. URL target of the IdP where the SP will send the Authentication Request. ("SAML 2.0 Endpoint (HTTP)")".
- Single Log Out Service Url:** An empty text input field with a "[STORE VIEW]" label to its right. Below the field is a small red triangle icon and the text "SLO endpoint info of the IdP. URL target of the IdP where the SP will send the SLO Request. ("SLO Endpoint (HTTP)")".
- X.509 Certificate:** A large empty text area with a "[STORE VIEW]" label to its right. Below the field is a small red triangle icon and the text "Public x509 certificate of the IdP. ("X.509 certificate)".



3.3 OPTIONS

In the “Options” section the behavior of the plugin is set, so you just select “Yes” for some important fields: Create user if not exists, Update user data, Sync role when updating user, default RoleId and Single Log Out.

OPTIONS

In this section the behavior of the plugin is set.

Create user if not exists	<input type="text" value="Yes"/>	[GLOBAL]
	<small>▲ Auto-provisioning. If user not exists, Magento will create a new user with the data provided by the IdP. Review the Mapping section</small>	
Update user data	<input type="text" value="Yes"/>	[GLOBAL]
	<small>▲ Auto-update. Magento will update the account of the user with the data provided by the IdP. Review the Mapping section</small>	
Sync role when updating user	<input type="text" value="Yes"/>	[GLOBAL]
	<small>▲ Magento will sync role provided by the IdP when update user data is enabled.</small>	
Default RoleId	<input type="text" value="1"/>	[GLOBAL]
	<small>▲ If Role is not provided by the Identity Provider, set here a Role ID and this value will be assigned when provisioning/updating the user account. Leave blank if you don't want to assign default Role</small>	
Single Log Out	<input type="text" value="Yes"/>	[GLOBAL]
	<small>▲ Enable/disable Single Log Out. SLO is a complex functionality, the most common SLO implementation is based on front-channel (redirections), sometimes if the SLO workflow fails a user can be blocked in an unhandled view. If the admin does not controls the set of apps involved in the SLO process maybe is better to disable this functionality due could carry more problems than benefits.</small>	

3.4 ATTRIBUTE MAPPING

In this section, we can set the mapping between IdP fields and Magento fields. Notice that this mapping could be also set at Onelogin's IdP. Note that the attribute that contains the group of the customer.

ATTRIBUTE MAPPING

Sometimes the names of the attributes sent by the IdP not match the names used by Magento for the customer accounts. In this section we can set the mapping between IdP fields and Magento fields.

Username	<input type="text" value="uid"/>	[GLOBAL]
Email	<input type="text" value="mail"/>	[GLOBAL]
First Name	<input type="text" value="sn"/>	[GLOBAL]
Last Name	<input type="text" value="cn"/>	[GLOBAL]
Role	<input type="text" value="eduPersonAffiliation"/>	[GLOBAL]

▲ The attribute that contains the role. For example 'memberof'. If Magento can't figure what role assign, it will assign the roleID 1 (Administrators). (System > Permissions > Roles)



3.5 ROLE MAPPING

In the “Role mapping” section, we can set the mapping between IdP Role values and Magento Roles. Example: admin, owner, super-user. There are 10 fields, the id means that Role id=1 will match the Magento role that has id=1 if exists.

ROLE MAPPING

The IdP can use it's own roles. Set in this section the mapping between IdP and Magento roles. Accepts multiple valued comma separated. Example: administrators. There are 5 fields, The id means that Role id=1 will match the Magento role that has id=1 if exists (Administrators). Review the Role list at System > Permissions > Roles

Role id=1	<input type="text" value="admin"/>	[GLOBAL]
Role id=2	<input type="text"/>	[GLOBAL]
Role id=3	<input type="text"/>	[GLOBAL]
Role id=4	<input type="text"/>	[GLOBAL]
Role id=5	<input type="text"/>	[GLOBAL]

3.6 CUSTOM MESSAGES

CUSTOM MESSAGES

Handle what messages are showed in the login form

Login Link	<input type="text" value="Login via Identity Provider"/>	[GLOBAL]
------------	--	----------

▲ The text that appears as the link, default is: 'Login via Identity Provider'

3.7 ADVANCED SETTINGS

In this section, you can easily handle some other parameters related to customizations and security issues. If sign/encryption is enabled, then x509 cert and private key for the SP must be provided.

I recommend to set a SP EntityID to identify the SP and use as its value the metadata URL where the SP is published. This URL appears on the “Status” section.



ADVANCED SETTINGS

Handle some other parameters related to customizations and security issues.
If sign/encryption is enabled, then x509 cert and private key for the SP must be provided. There are 2 ways:
1. Store them as files named sp.key and sp.crt on the 'certs' folder of the plugin. (be sure that the folder is protected and not exposed to internet)
2. Store them at the database, filling the corresponding textareas. (take care of security issues)

Debug Mode	<input type="text" value="Yes"/>	[STORE VIEW]
	<small>▲ Enable it when your are debugging the SAML workflow. Errors and Warnigs will be showed</small>	
Strict Mode	<input type="text" value="Yes"/>	[STORE VIEW]
	<small>▲ If Strict mode is Enabled, then Magento will reject unsigned or unencrypted messages if it expects them signed or encrypted. Also will reject the messages if not strictly follow the SAML standard: Destination, Nameid, Conditions ... are validated too</small>	
Service Provider Entity Id	<input type="text" value="https://pitbulk.no-ip.org/magento/index.hp/sso/saml"/>	[STORE VIEW]
	<small>▲ Set the Entity ID for the Service Provider. We recommend to set as SP EntityID the URL where its metadata is published (review status section). If not provided, 'php-saml' will be used</small>	
NameID Format	<input type="text" value="urn:oasis:names:tc:SAML:1.1:nameid-format:un"/>	[STORE VIEW]
	<small>▲ Specifies constraints on the name identifier to be used to represent the requested subject.</small>	
Encrypt nameID	<input type="text" value="No"/>	[STORE VIEW]
	<small>▲ The nameID sent by this SP will be encrypted</small>	
Sign AuthnRequest	<input type="text" value="No"/>	[STORE VIEW]
	<small>▲ The samlp:AuthnRequest messages sent by this SP will be signed</small>	
Sign LogoutRequest	<input type="text" value="No"/>	[STORE VIEW]
	<small>▲ The samlp:logoutRequest messages sent by this SP will be signed</small>	
Sign LogoutResponse	<input type="text" value="No"/>	[STORE VIEW]
	<small>▲ The samlp:logoutResponse messages sent by this SP will be signed</small>	
Reject Unsigned Messages	<input type="text" value="No"/>	[STORE VIEW]
	<small>▲ Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received</small>	
Reject Unsigned Assertions	<input type="text" value="Yes"/>	[STORE VIEW]
	<small>▲ Reject unsigned saml:Assertion received</small>	

If you are using multi-store, depending on the type of configuration is possible that this value appears wrong on the "Status" section, but you can calculate it by adding "/sso/saml/metadata" to the URL where the store is published.



Reject Unencrypted Assertions	<input type="text" value="No"/> [STORE VIEW] ▲ Reject unencrypted saml:Assertion received
Requested AuthN Context	<input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:unspec"/> <input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo"/> <input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo"/> <input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:X509"/> <input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:Smartc"/> <input type="text" value="urn:oasis:names:tc:SAML:2.0:ac:classes:Kerber"/> <input type="text" value="urn:federation:authentication:windows"/> [STORE VIEW] ▲ Authentication context. Unselect all to accept any type, otherwise select the valid contexts
Service Provider X.509 Certificate	<input type="text"/> [STORE VIEW] ▲ Public x509 certificate of the SP. Leave this field empty if you gonna provide the cert by the sp.crt
Service Provider Private Key	<input type="text"/> [STORE VIEW] ▲ Private Key of the SP. Leave this field empty if you gonna provide the private key by the sp.key
Signature Algorithm	<input type="text" value="http://www.w3.org/2001/04/xmldsig-more#rsa-sh"/> [STORE VIEW] ▲ Algorithm that the toolkit will use on signing process (if enabled).

If you plan to support Encrypted Assertions or Sign the SAML Messages you will need a public certificate/private key. SAML protocol let you to use self-signed ones. If you don't know how generate them, use this tool:

https://www.samltool.com/self_signed_certs.php



4 How to configure the Identity Provider

Here is a list of the main Identity Provider available with a link to a guide to configure them, some of them mention how to integrate with another Service Provider, but you will get an idea about how integrate it with Magento.

4.1 Onelogin

<https://support.onelogin.com/hc/en-us/articles/202673944-How-to-Use-the-OneLogin-SAML-Test-Connector>

4.2 Okta

http://developer.okta.com/docs/guides/setting_up_a_saml_application_in_okta.html

4.3 Ping Identity

<https://documentation.pingidentity.com/display/SLC10/Complete+Setup+of+SAML+SSO+to+Slack>

4.4 ADFS 2.0

<http://support.talentlms.com/knowledgebase/articles/328229-how-to-configure-sso-with-microsoft-active-directo>

4.5 ADFS 3.0

http://wiki.servicenow.com/index.php?title=Configuring_ADFS_3.0_to_Communicate_with_SAML_2.0#gsc.tab=0

4.6 Salesforce

https://help.salesforce.com/apex/HTViewHelpDoc?id=identity_provider_enable.htm

https://help.salesforce.com/HTViewHelpDoc?id=service_provider_define.htm&language=en_US

https://help.salesforce.com/HTViewHelpDoc?id=sso_saml.htm



4.7 Google

<https://support.google.com/a/answer/6087519?hl=en>

4.8 Forgerock

<https://backstage.forgerock.com/#!/docs/openam/12.0.0/admin-guide/chap-federation#configure-cot>

4.9 ServiceNow

http://wiki.servicenow.com/index.php?title=SAML_2.0_Setup#gsc.tab=0

4.10 Auth0

<https://auth0.com/docs/samlso-auth0-to-auth0>

4.11 Shibboleth

<https://wiki.shibboleth.net/confluence/display/SHIB2/IdPSPCommunicate>

4.12 simpleSAMLphp

https://simplesamlphp.org/docs/stable/simplesamlphp-idp#section_7

4.13 secureAuth

<https://www.pagerduty.com/docs/guides/secureauth-integration-guide/>

4.14 clearlogin

<https://clearlogin.zendesk.com/hc/en-us/articles/208168156-SAML-App-Connections>

4.15 Identacor

<https://identacor.zendesk.com/hc/en-us/articles/202023743-How-to-Add-A-Custom-App-Using-Secure-Auto-Login>



4.16 Centrify

https://www.centrify.com/downloads/public/sdk/knox/HTML_Doc/Implementation_Guide/Mobile_SDK_SAML_scripting.14.4.html

4.17 Bitium

https://support.bitium.com/customer/portal/articles/2093598-how-to-add-saml-to-a-custom-app-?b_id=4928

4.18 CA Technologies

<https://docops.ca.com/ca-single-sign-on-12-52-sp1/en/configuring/legacy-federation/configure-a-saml-2-0-service-provider>



5 Warranty

Support by mail <sixto.martin.garcia@gmail.com> guaranteed. Get a reply in less than 48h (business day).