Magento ADMIN SAML Extension User Guide

Table of Contents

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.

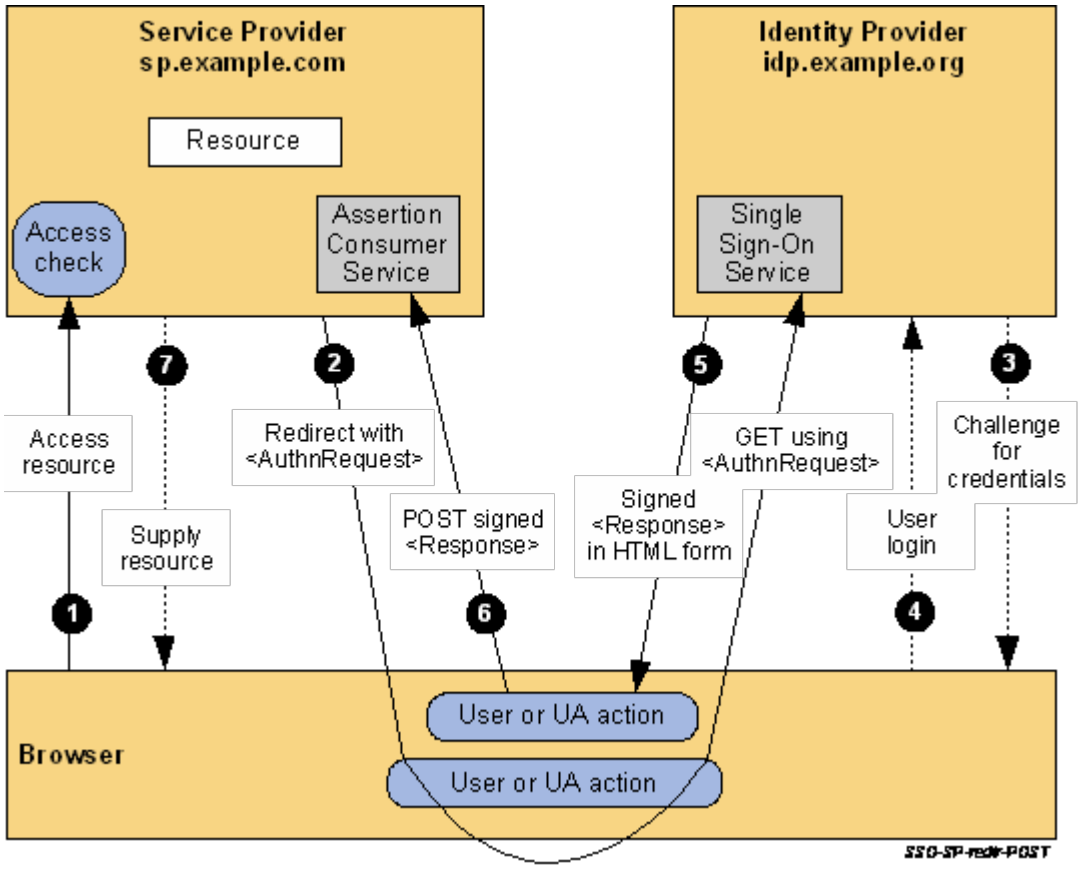
The Title and the text of the link is customizable (See Custom Message section).

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).

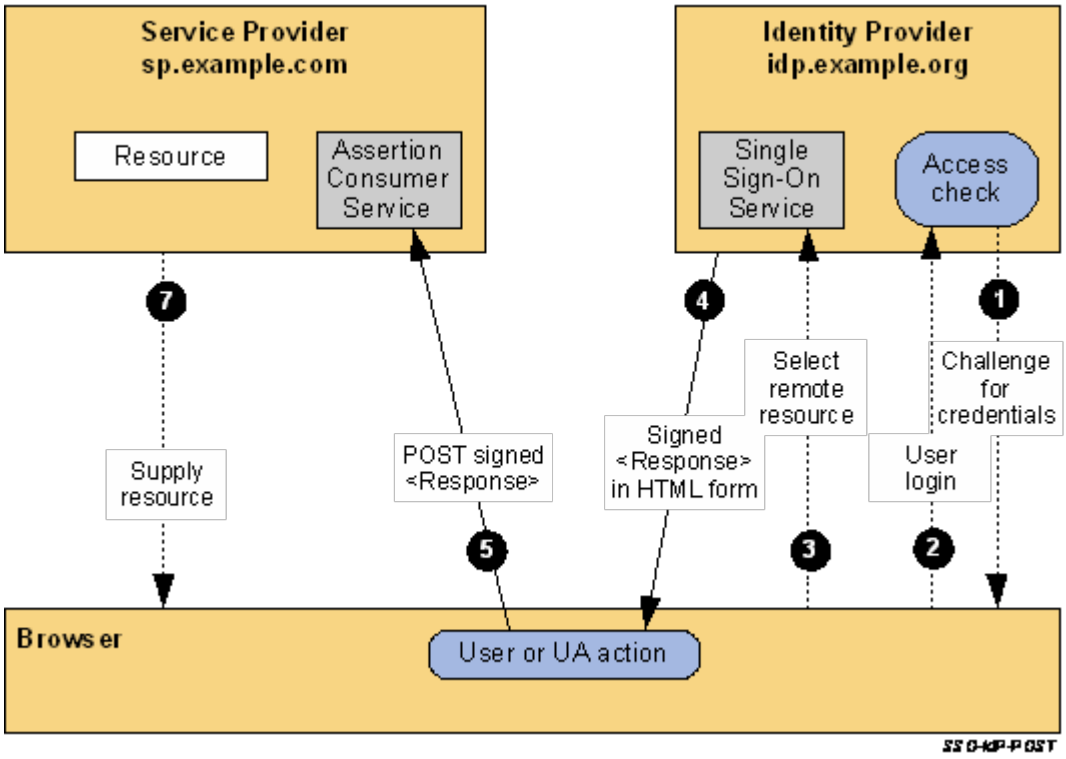
The following diagram details this process.



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).

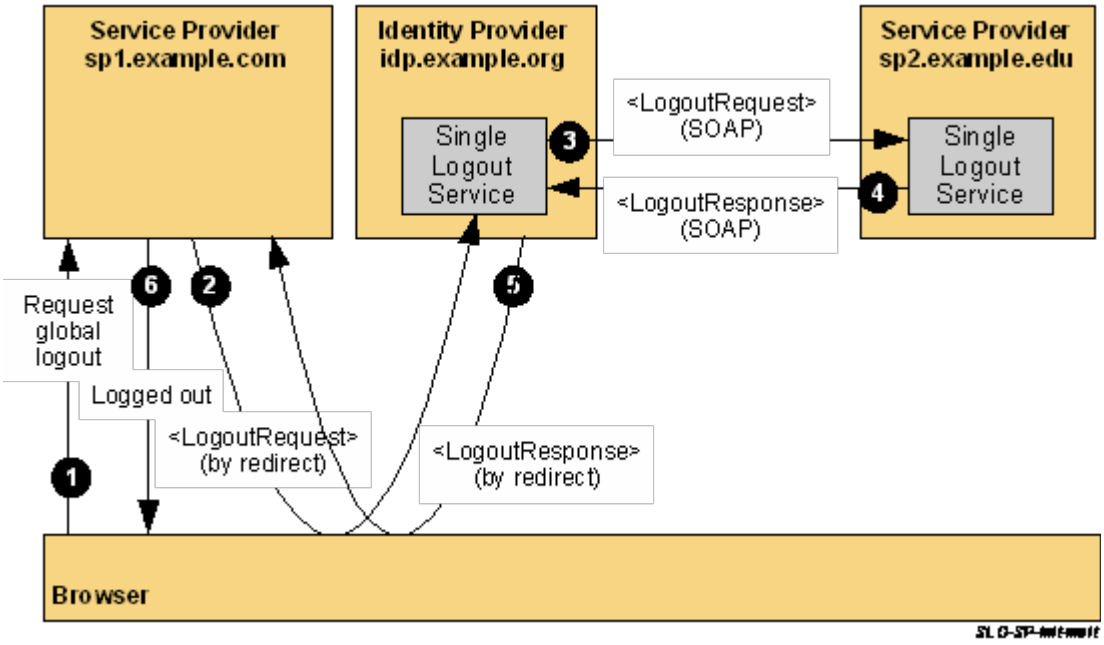


2.2 Single Log Out

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

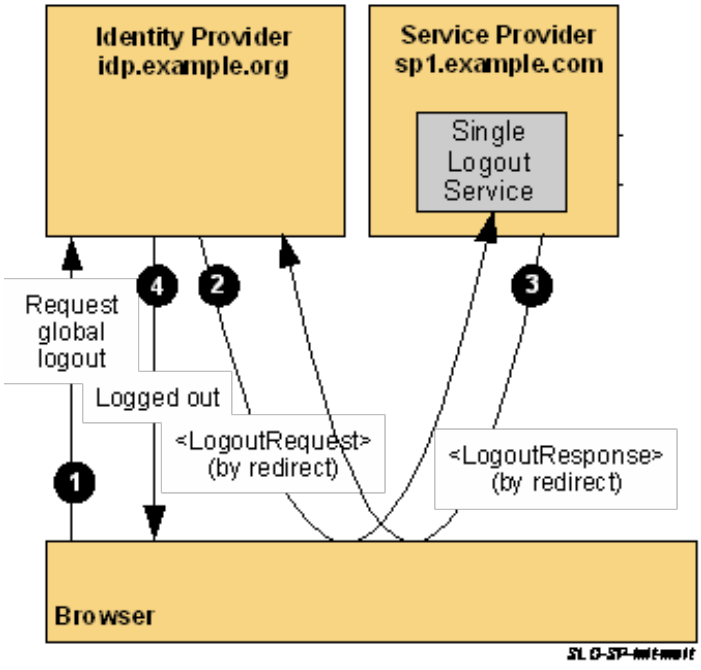
In this scenario the Service Provider (Magento) initiates the Single Logout Process. It will send a LogoutRequest to the Identity Provider, the Identity Provider will close the active sessions (including those SP that initiaited a SSO process before) and send a LogoutResponse to the Service Provider. 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).

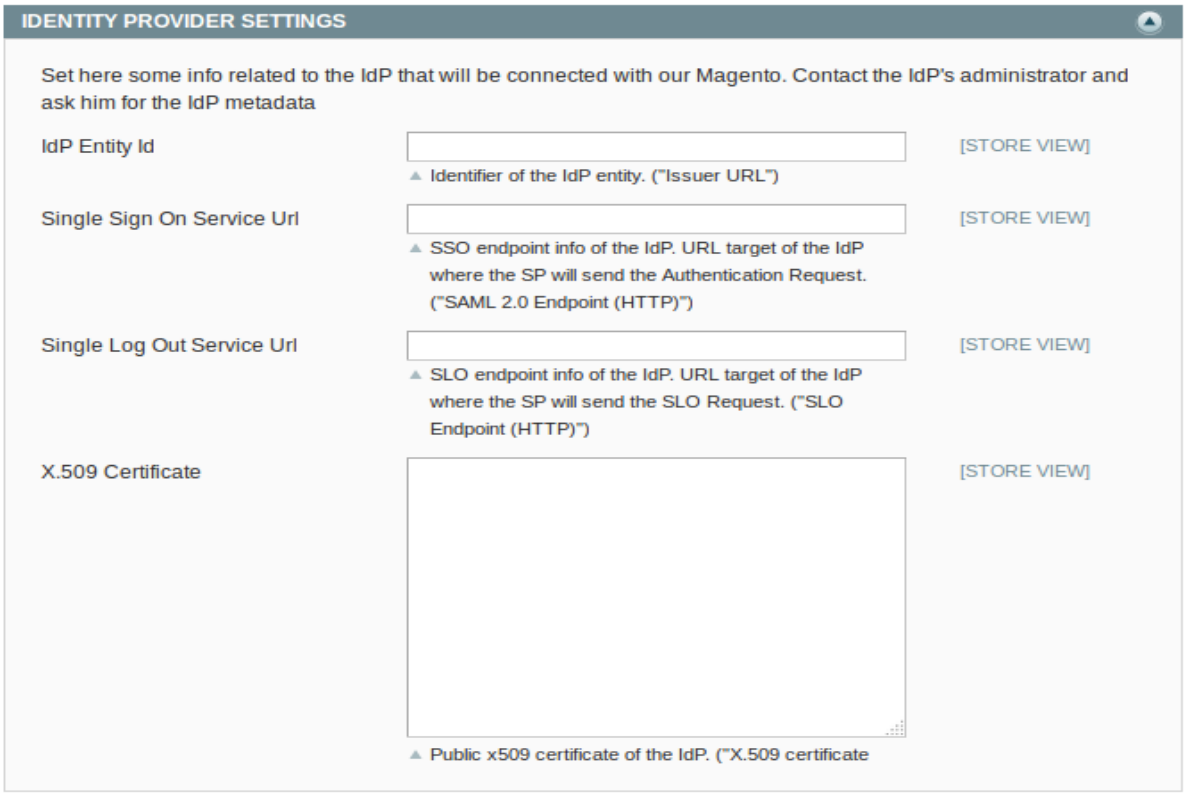
If you are using Magento Multi-site you will be able to configure/enable SAML in each store. Each store will have its own panel/settings.

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).

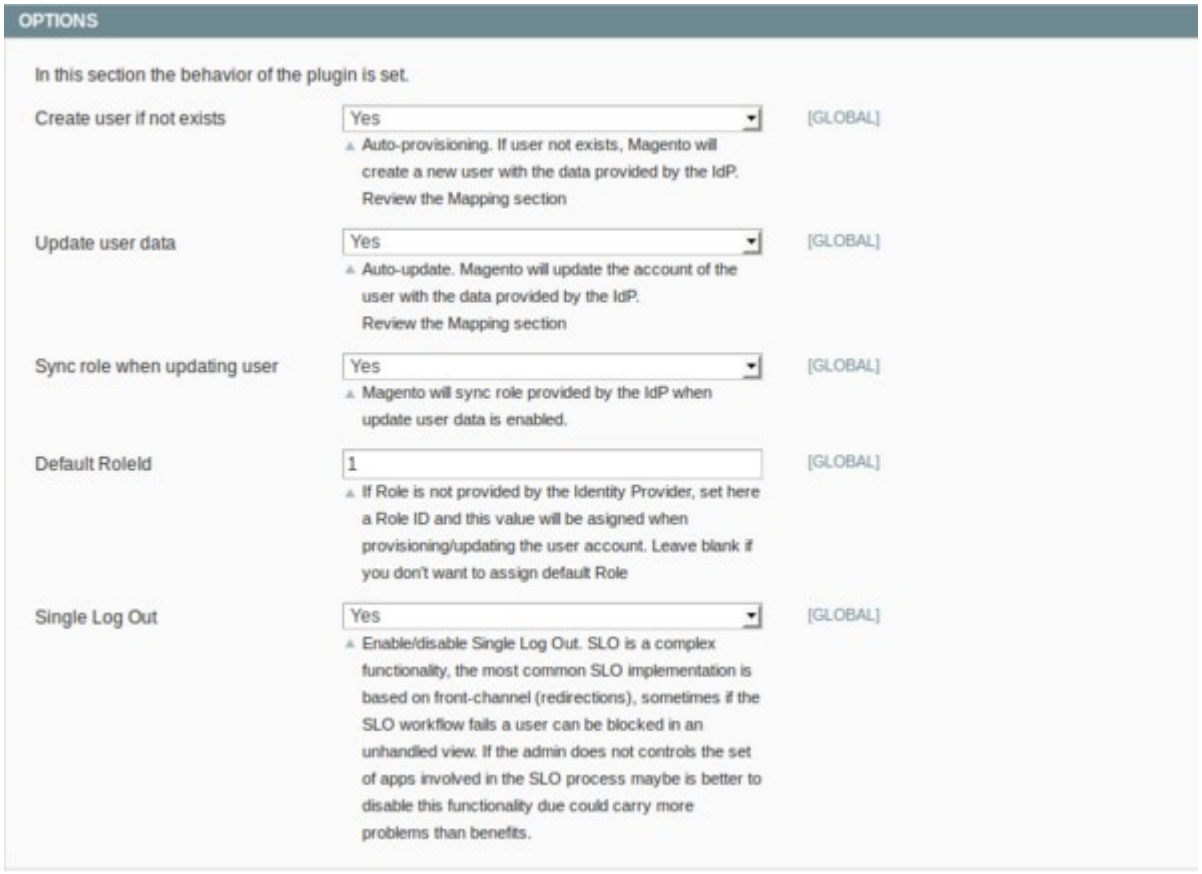
3.2 Identity Provider Settings

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.



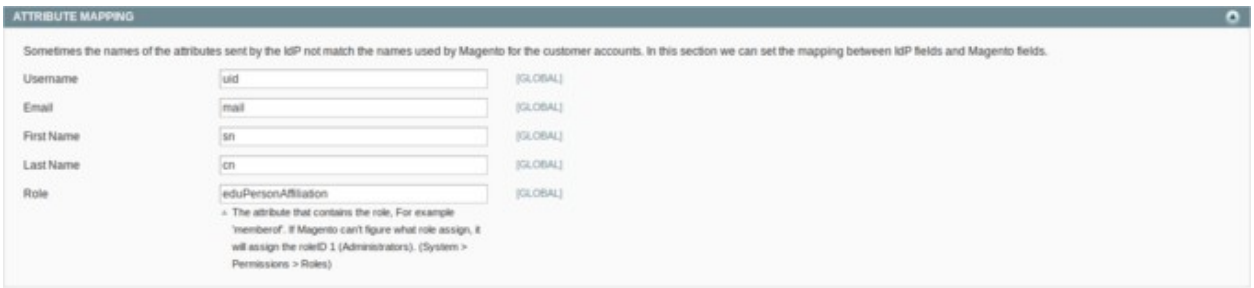
3.3 OPTIONS

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



3.4 ATTRIBUTE MAPPING

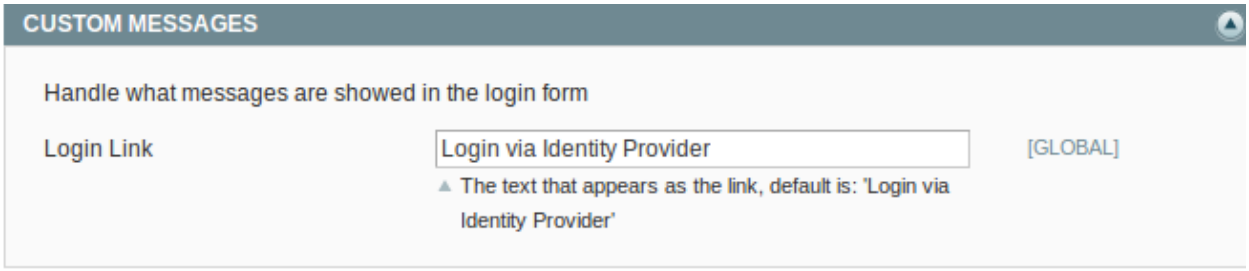
In this section, we can set the mapping between IdP fields and Magento fields. Notice that this mapping could be also set at Onelogin's IdP. Note that the attribute that contains the group of the customer.



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.

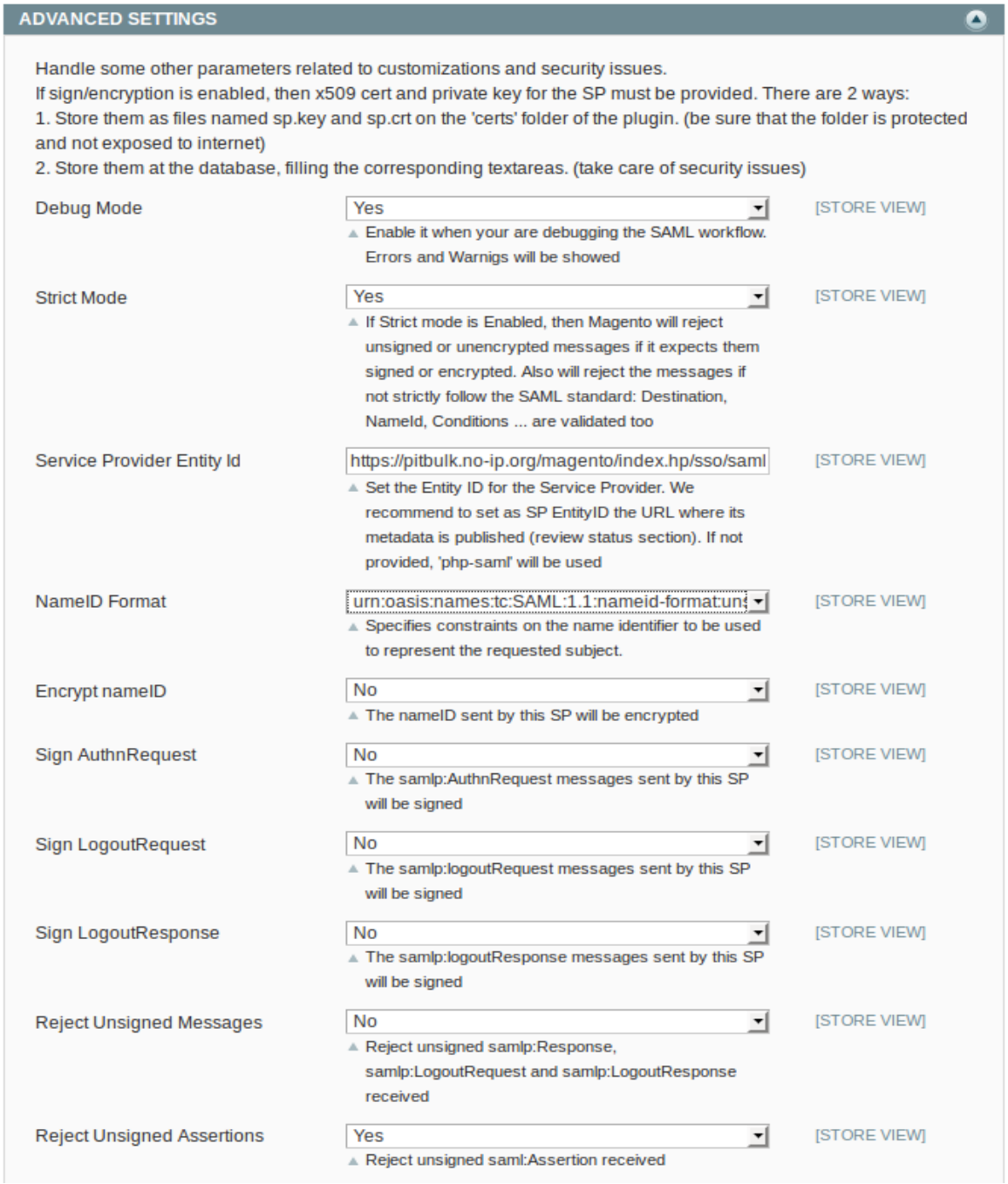
3.6 CUSTOM MESSAGES



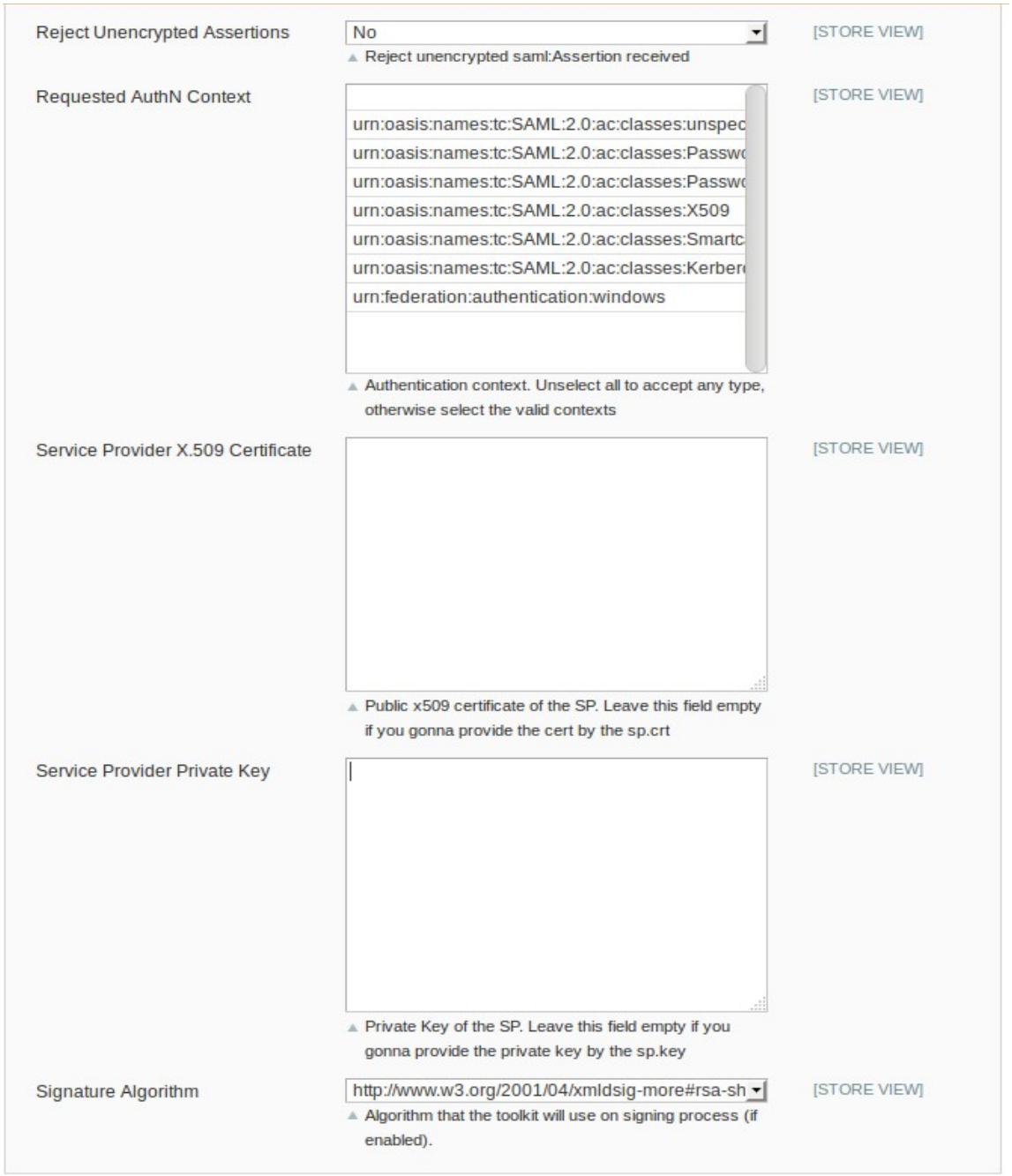
3.7 ADVANCED SETTINGS

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.



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.



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/samlsso-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).