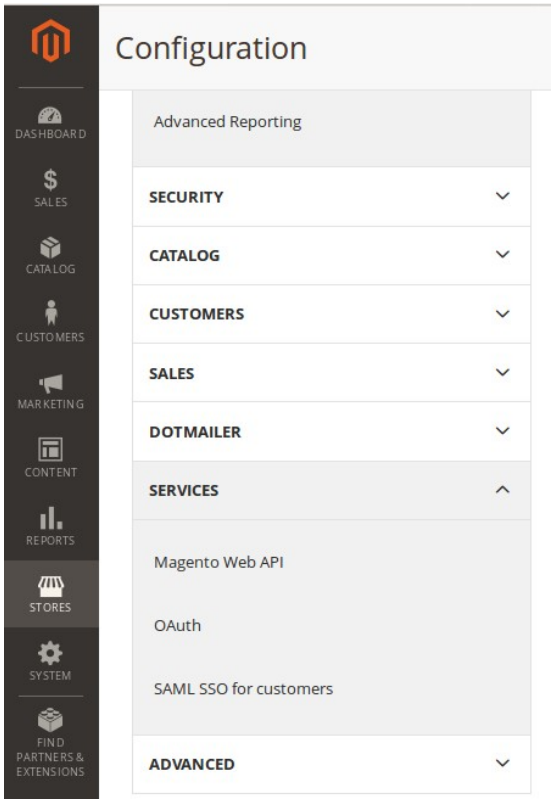
Single Sign On. SAML extension for M 2
(frontend, Implemented by Sixto Martin)

The Setting panel contains different sections with fields that need to be filled.

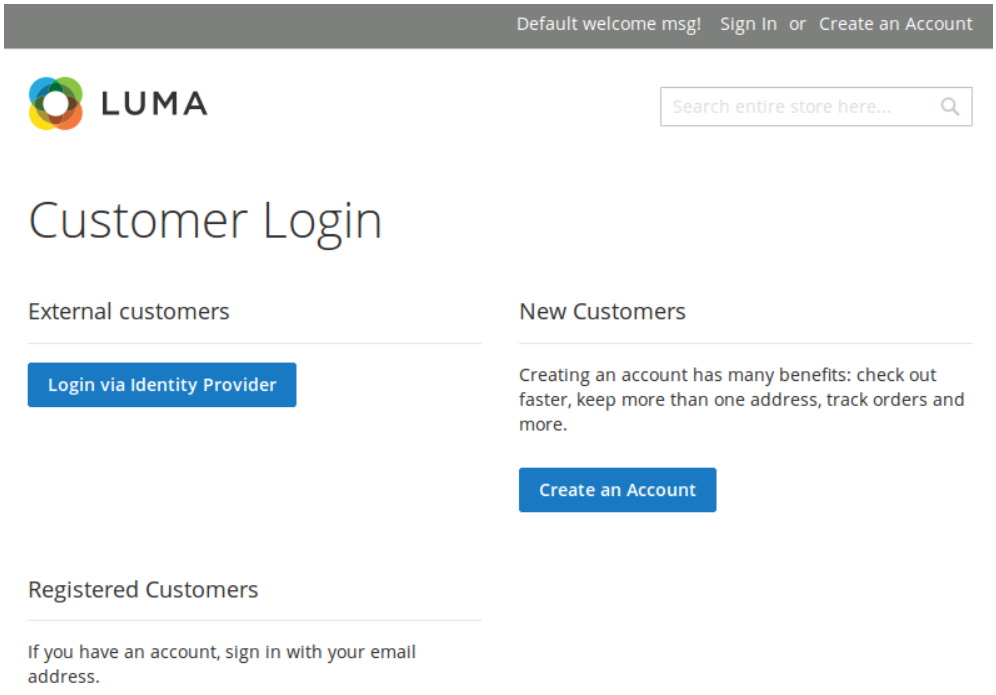
Sections and fields contains a description that contains enought information to understand what info need to be provided.



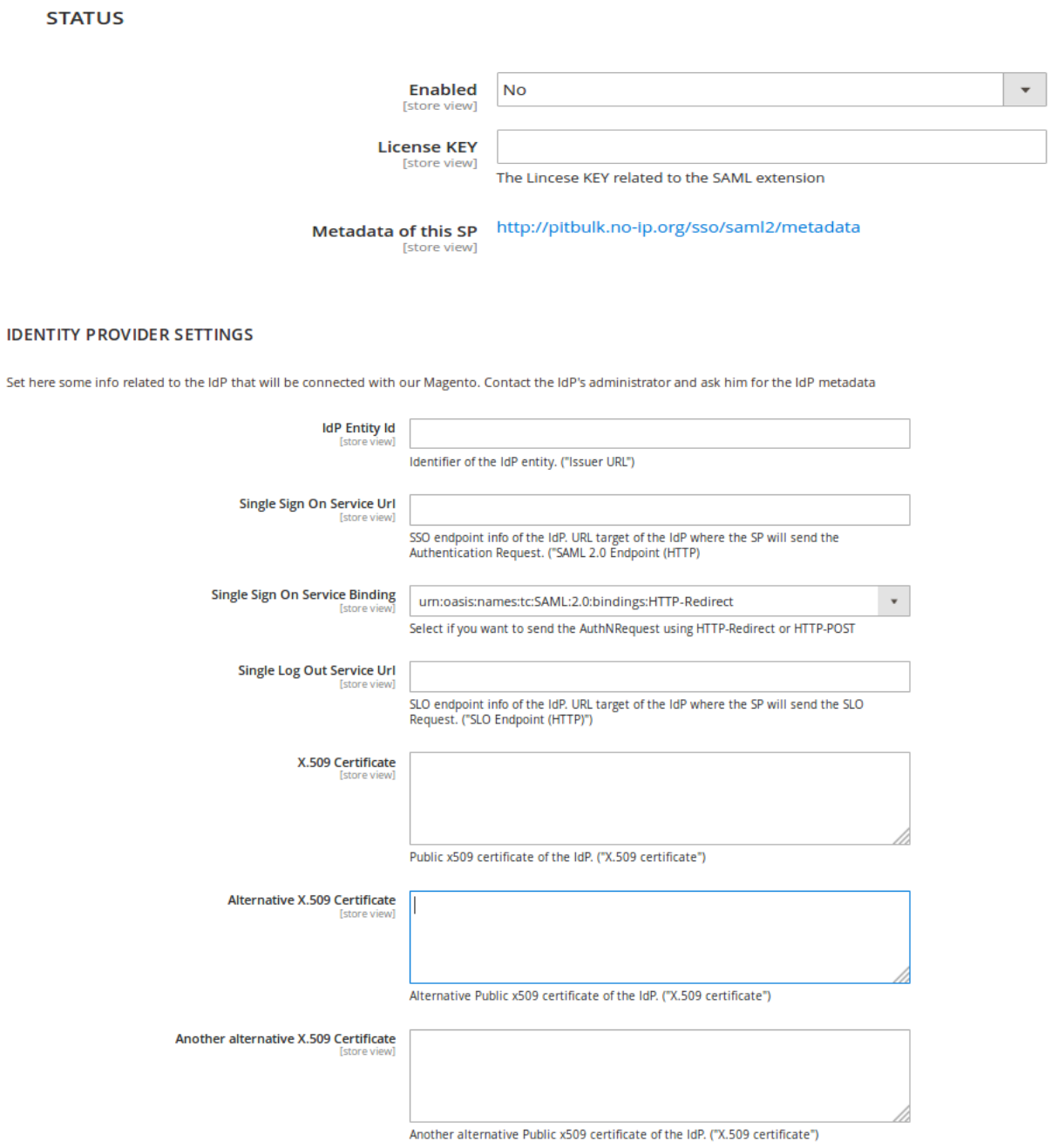
In order to access to the setting panel, log in the admin instance of M2, and got to Stores > Configuration. At the Services tab, the "SAML SSO for customers" link.

The extension support multi-sites, so if you access to the setting panel of each store you will be able to enable SAML on it. (Each store has its own settings).

Once enabled the customer will see the login form modified, with the new “External customer” section. Notice that the title and the text of the button can be customized on the “Custom messages” setting.



Those are the sections of the SAML setting panel for the front-end.



OPTIONS

In this section the behavior of the extension is set.

Create user if not exists [store view]
Yes
Auto-provisioning. If user not exists, Magento will create a new user with the data provided by the IdP.
Review the Mapping section

Disable welcome email [store view]
Yes
Disable sending the welcome email to new customers.

Update user data [store view]
Yes
Auto-update. Magento will update the account of the customer with the data provided by the IdP (firstname, lastname, groupid. If custom attribute used to identify customer then Email is updated. Otherwise if custom attribute defined but not used to identify, it is updated. Address registered if no previusly address found).
Review the Mapping section

Default customer group id [store view]
If extension is not able to read group from IdP, assign this user group when creating new customer account. Otherwise Magento default goup will be used

Force SAML SSO [store view]
No
Enable it if you want to force the customer to log at the IdP when visiting the login page (it applies customer view only, not admin panel).

Single Log Out [store view]
Yes
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.

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.

Email [store view]

First Name [store view]

Last Name [store view]

Group [store view]

GROUP MAPPING

The IdP can use it's own groups. Set in this section the mapping between IdP and Magento customer groups. Accepts multiple valued comma separated. Example: admin,owner,superuser. There are 5 fields, The id means that Role id=1 will match the Magento groups that has id=1 if exists. Review the Group list at Stores > Other Settings > Customer Groups

Group id=1 [store view]	
Group id=2 [store view]	
Group id=3 [store view]	
Group id=4 [store view]	
Group id=5 [store view]	
Group id=6 [store view]	
Group id=7 [store view]	
Group id=8 [store view]	
Group id=9 [store view]	
Group id=10 [store view]	

ADDRESS MAPPING

If the IdP has address data, set in this section the mapping between IdP address data and Magento.

Company [store view]	
Street 1 [store view]	
Street 2 [store view]	
City [store view]	
Country [store view]	
State/Province [store view]	
Zip/Postal Code [store view]	
Fax [store view]	
Telephone [store view]	

CUSTOM FIELD MAPPING

If you have a custom attribute on Magento that you want to support, add its code and mapping value here.

Custom Attribute Code
[store view]

Custom Attribute Mapping
[store view]

Identify customer by custom field
[store view]

No

By default the SAML extension will identify the customer by the Email, but in some scenarios, is required to identify the customer by a custom attribute like EmployeeID. If that is your case, enable this checkbox and configure properly the previous fields

Custom Attribute Code 2
[store view]

Custom Attribute Mapping 2
[store view]

Custom Attribute Code 3
[store view]

Custom Attribute Mapping 3
[store view]

Custom Attribute Code 4
[store view]

Custom Attribute Mapping 4
[store view]

CUSTOM MESSAGES

Handle what messages are showed in the login form.

Login Header
[store view]

The text that appears as the title, default is: 'External customers'

Login Link
[store view]

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

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 extension. (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
[store view]
No
Enable it when your are debugging the SAML workflow. Errors and Warnigs will be showed

Strict Mode
[store view]
No
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

SP Entity Id
[store view]
Set the Entity ID for the Service Provider. If not provided, the url where the metadata is published will be used.

NameID Format
[store view]
urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
Specifies constraints on the name identifier to be used to represent the requested subject.

Encrypt nameID
[store view]
No
The nameID sent by this SP will be encrypted

Sign AuthnRequest
[store view]
No
The samlp:AuthnRequest messages sent by this SP will be signed

Sign LogoutRequest
[store view]
No
The samlp:logoutRequest messages sent by this SP will be signed

Sign LogoutResponse
[store view]
No
The samlp:logoutResponse messages sent by this SP will be signed

Reject Unsigned Messages
[store view]
No
Reject unsigned samlp:Response, samlp:LogoutRequest and samlp:LogoutResponse received

Reject Unsigned Assertions
[store view]
No
Reject unsigned saml:Assertion received

Reject Unencrypted Assertions
[store view]
No
Reject unencrypted saml:Assertion received

Requested AuthN Context
[store view]

urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
urn:oasis:names:tc:SAML:2.0:ac:classes:Password
urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTrans
urn:oasis:names:tc:SAML:2.0:ac:classes:X509
urn:oasis:names:tc:SAML:2.0:ac:classes:Smartcard
urn:oasis:names:tc:SAML:2.0:ac:classes:Kerberos
urn:federation:authentication:windows

Authentication context. Unselect all to accept any type, otherwise select the valid contexts

Service Provider X.509 Certificate
[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
[store view]

Private Key of the SP. Leave this field empty if you gonna provide the private key by the sp.key

Signature Algorithm
[store view]

http://www.w3.org/2000/09/xmldsig#rsa-sha1

Algorithm that the toolkit will use on signing process (if enabled).

Digest Algorithm
[store view]

http://www.w3.org/2000/09/xmldsig#sha1

Algorithm that the toolkit will use on digest process (if signature enabled).

Lower Case URL Encoding
[store view]

No

Set True if you are connecting with ADFS and you experience issues validating signatures.

Sign Metadata
[store view]

No

The metadata published by this SP will be signed.

You will need to provide the Service Provider metadata to the Identity Provider administrator.

At the “status” section you will find the link to access a view where the metadata is published (see the source code on the browser to get the XML). It looks like:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
                     validUntil="2016-05-18T18:17:43Z"
                     cacheDuration="PT604800S"
                     entityID="http://magento2.example.com/sso/saml2/metadata">
    <md:SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
                        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
                                Location="http://magento2.example.com/sso/saml2/sls" />
        <md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
                                     Location="http://magento2.example.com/sso/saml2/acs"
                                     index="1" />
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Also, at the Status section you are asked for a license key. Use the Order ID of your magento marketplace’s purchase.