RSA SecurID Access SAML Configuration for TalentLMS

Last Modified: May 31, 2017

TalentLMS is a SaaS eLearning platform. The platform offers tools for content creation and re-purposing, test building, assignment management, reporting, internal messaging & discussions, surveys, and others. It can also be used to sell courses online. TalentLMS also supports Auto provisioning of users.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and TalentLMS.

The instructions in this guide use the following SP Login URL, ACS URL and Issuer ID (entity ID) values:

SP Login URL	*https://www.talentlms.com/login*
ACS URL	*https://rsasso.talentlms.com/simplesaml/module.php/saml/sp/saml2-acs.php/rsasso.talentlms.com*
Service Provider Issuer ID	*rsasso.talentlms.com*

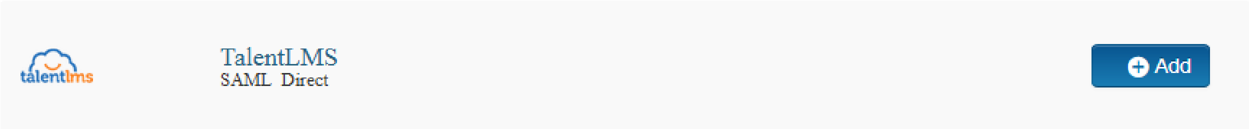
Procedure

1. Add the Application in RSA SecurID Access
2. Configure TalentLMS to Use RSA SecurID Access as an Identity Provider

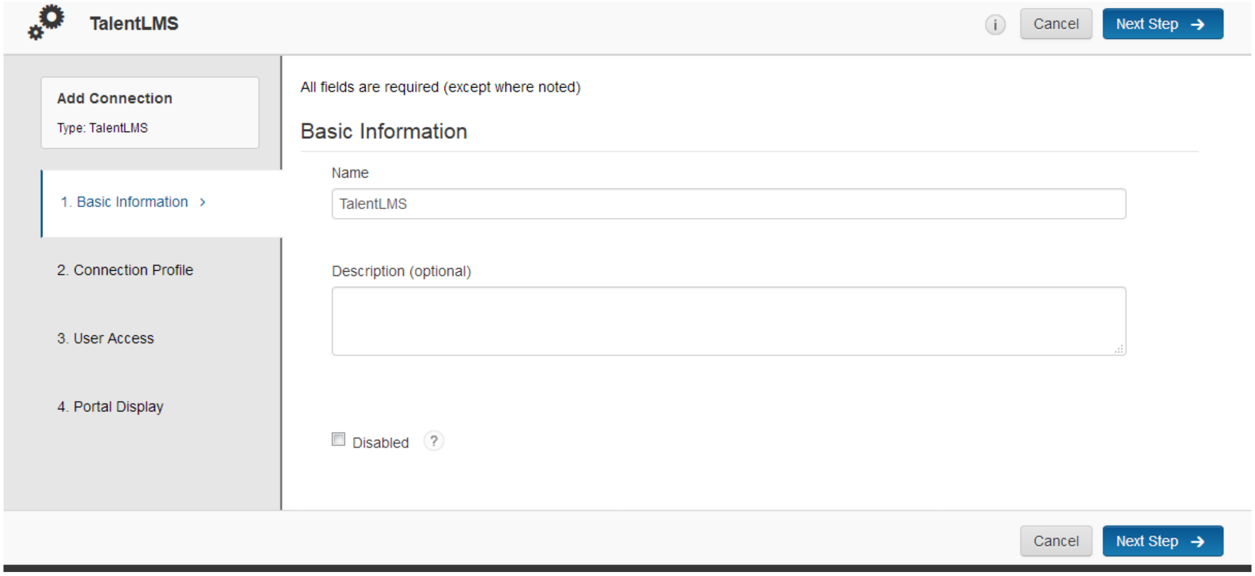
Add the Application in RSA SecurID Access

Procedure

1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** TalentLMS.



3. On the Basic Information page, specify the application name and click **Next Step**.



All fields are required (except where noted)

Basic Information

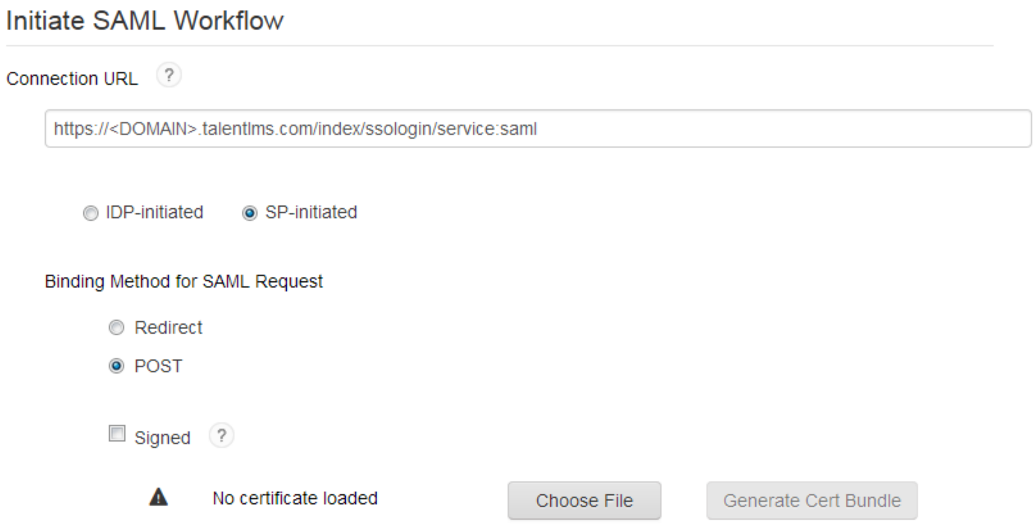
Name: TalentLMS

Description (optional):

□ Disabled

4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, Specify url https://<DOMAIN>.talentlms.com/index/ssologin/service:saml
   b. Choose **SP-initiated.**
   c. Replace <DOMAIN> value with your organization account value.

Note: The following SP-initiated configuration works for IDP-initiated connections as well.



Initiate SAML Workflow

Connection URL: https://<DOMAIN>.talentlms.com/index/ssologin/service:saml

○ IDP-initiated ● SP-initiated

Binding Method for SAML Request

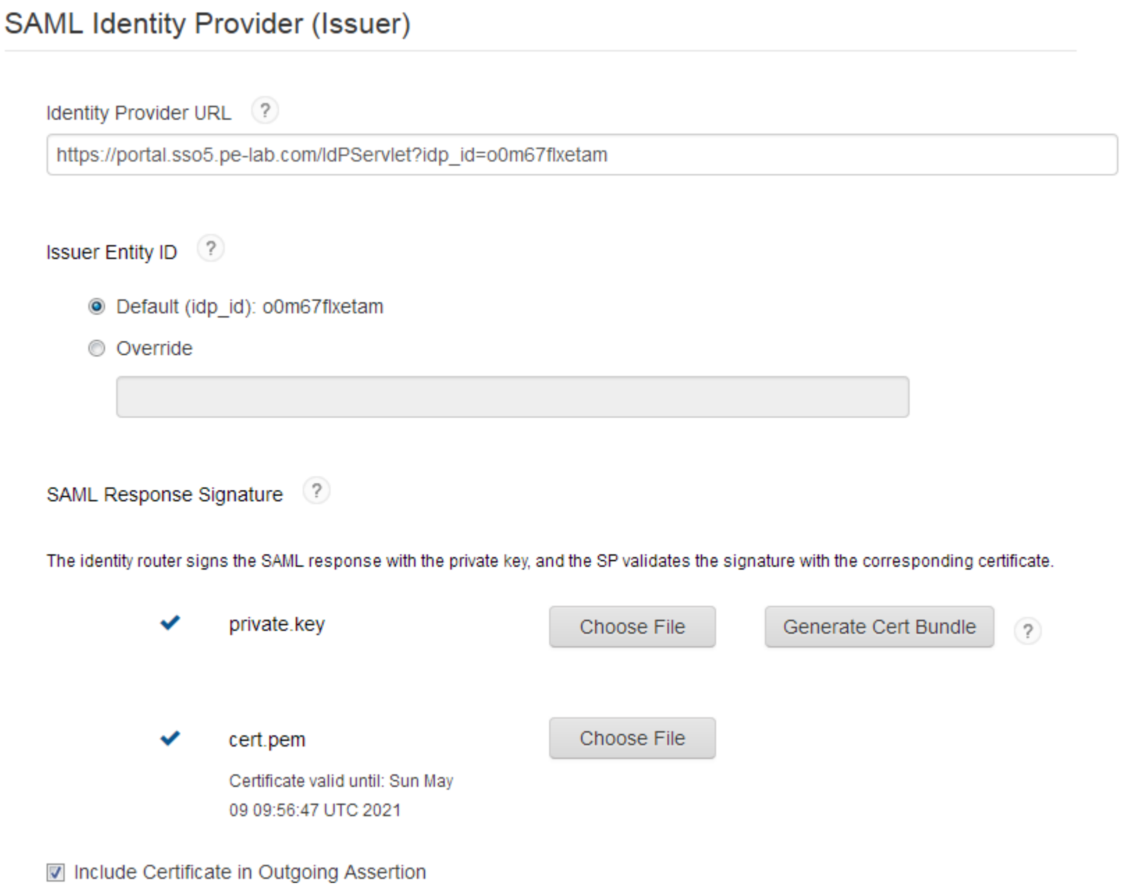
○ Redirect

● POST

□ Signed

No certificate loaded

5. Scroll down to **SAML Identity Provider (Issuer)** section.



SAML Identity Provider (Issuer)

Identity Provider URL ?

https://portal.sso5.pe-lab.com/IdPServlet?idp_id=o0m67flxetam

Issuer Entity ID ?

● Default (idp_id): o0m67flxetam

○ Override

SAML Response Signature ?

The identity router signs the SAML response with the private key, and the SP validates the signature with the corresponding certificate.

✓ private.key

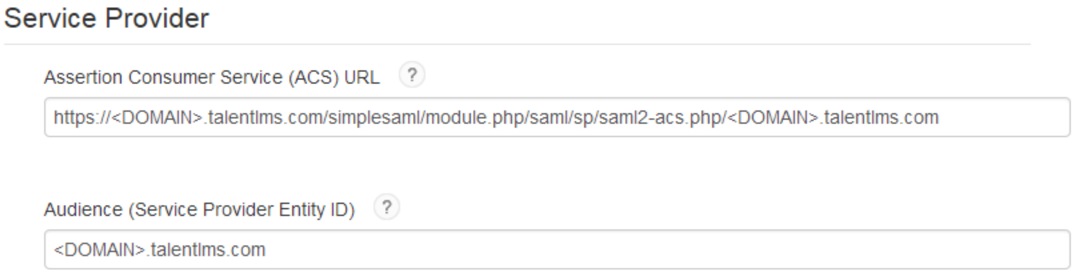
✓ cert.pem

Certificate valid until: Sun May 09 09:56:47 UTC 2021

☑ Include Certificate in Outgoing Assertion

a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

6. Scroll down to the **Service Provider** section.



Service Provider

Assertion Consumer Service (ACS) URL

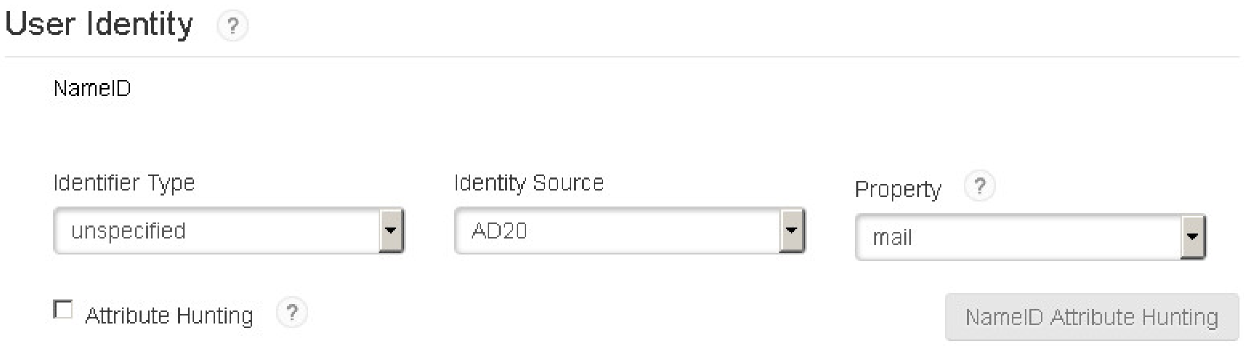
https://<DOMAIN>.talentlms.com/simplesaml/module.php/saml/sp/saml2-acs.php/<DOMAIN>.talentlms.com

Audience (Service Provider Entity ID)

<DOMAIN>.talentlms.com

   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> value with your organization account value.
   b. In the **Audience (Service Provider Issuer ID)** field, provide value as per received from service provider. , replace <DOMAIN> value with your organization account value.

7. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in email format and the user account will be validated against the User Store selected.



User Identity

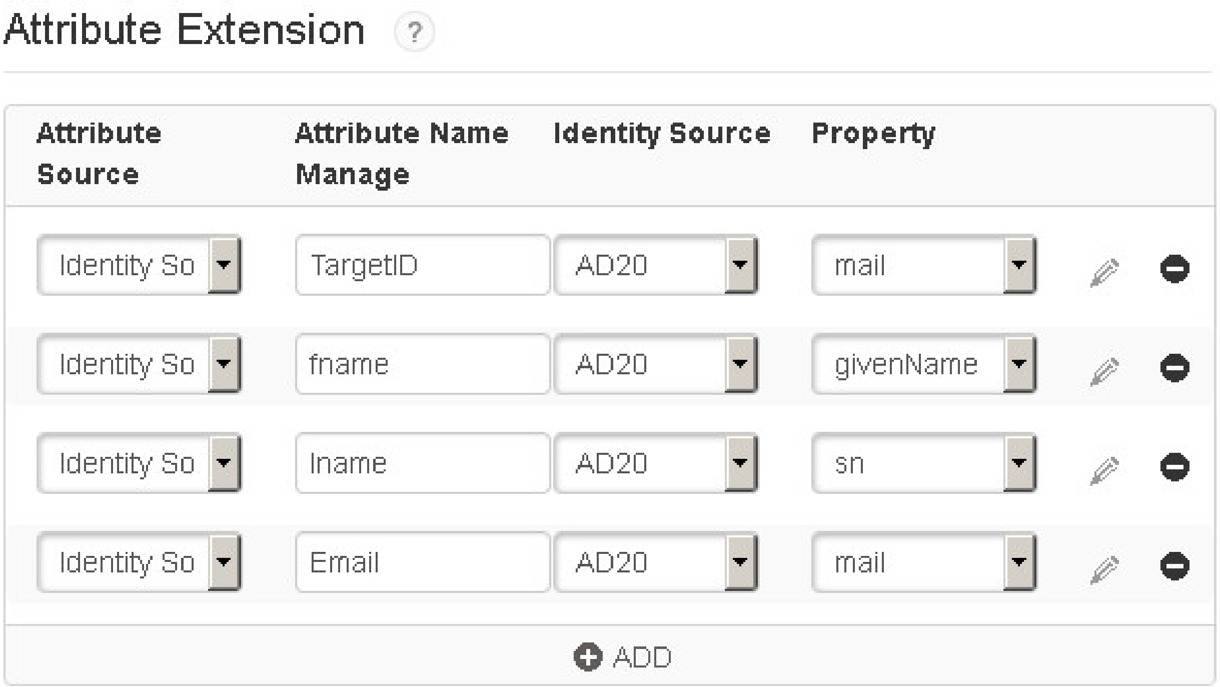
NameID

Identifier Type	Identity Source	Property
unspecified	AD20	mail

□ Attribute Hunting

8. Click on **Show Advanced Configuration**.

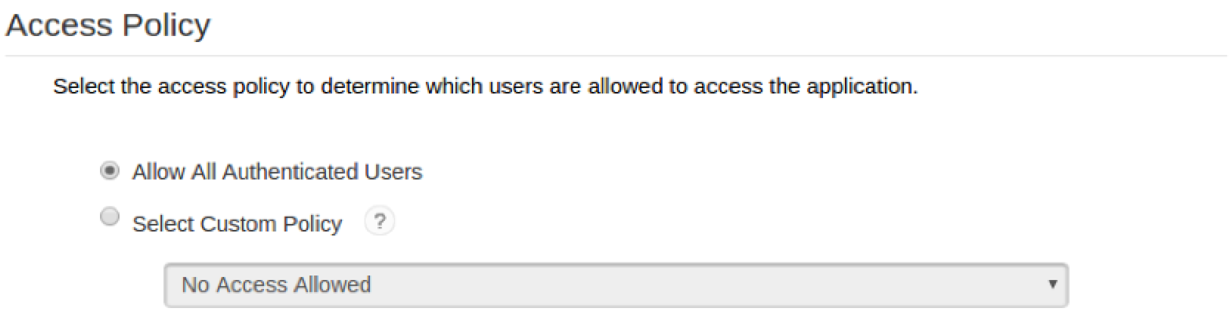
9. In the **Attribute Extension** section, add **TargetID, fname**,**lname**, **Email**. These are mandatory provisioning attributes needs to be forwarded at the time of SSO.



Attribute Extension ?

Attribute Source	Attribute Name Manage	Identity Source	Property
Identity So	TargetID	AD20	mail
Identity So	fname	AD20	givenName
Identity So	lname	AD20	sn
Identity So	Email	AD20	mail

10. Click **Next Step**.
11. On the **User Access** page, select **Allow All Authenticated Users** user policy from the available options.



Access Policy

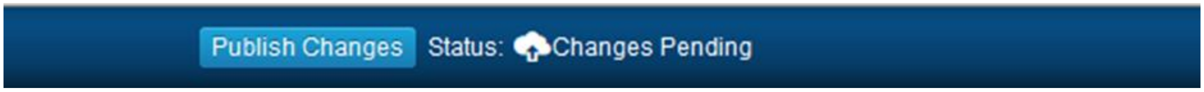
Select the access policy to determine which users are allowed to access the application.

● Allow All Authenticated Users

○ Select Custom Policy ?

No Access Allowed ▾

12. Click **Next Step**.
13. On the **Portal Display** page, select **Display in Portal**.
14. Click **Save and Finish**.
15. Click **Publish Changes**. Your application is now enabled for SSO.

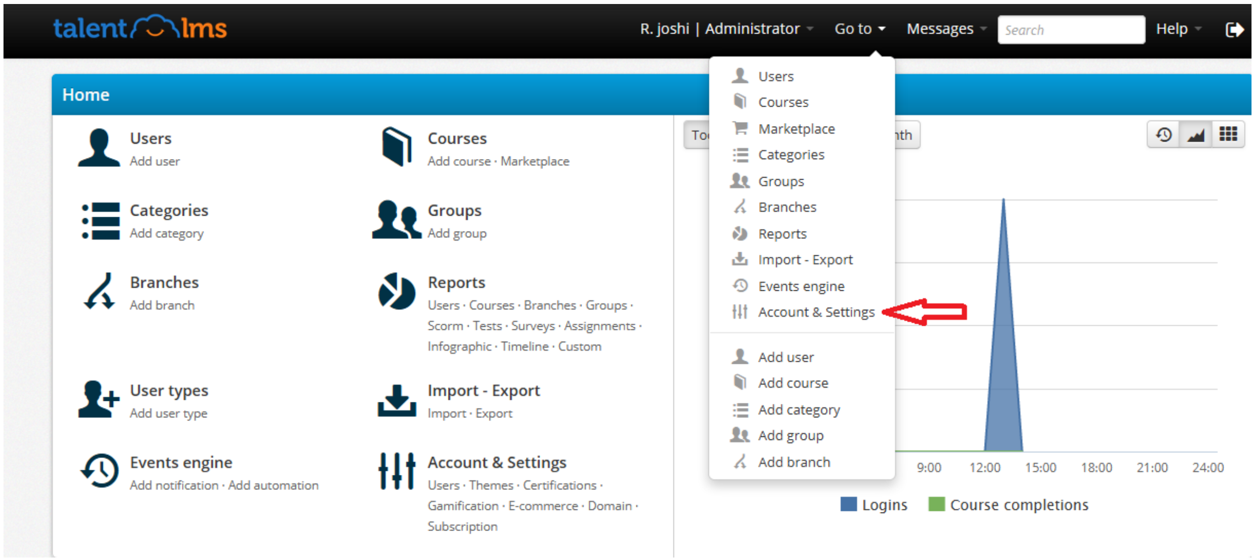


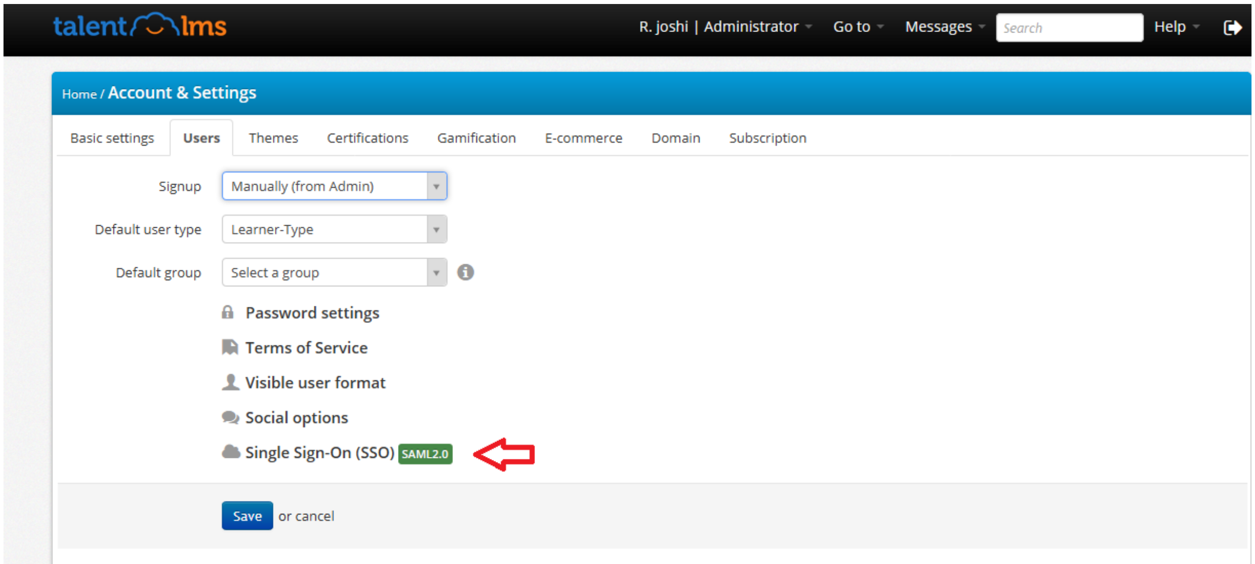
Status: Changes Pending

Configure TalentLMS to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your TalentLMS domain as a super-admin and in *Go to* → *Account & Settings* → *Users* → *Single Sign-On(SSO)*. (https://www.talentlms.com/login)



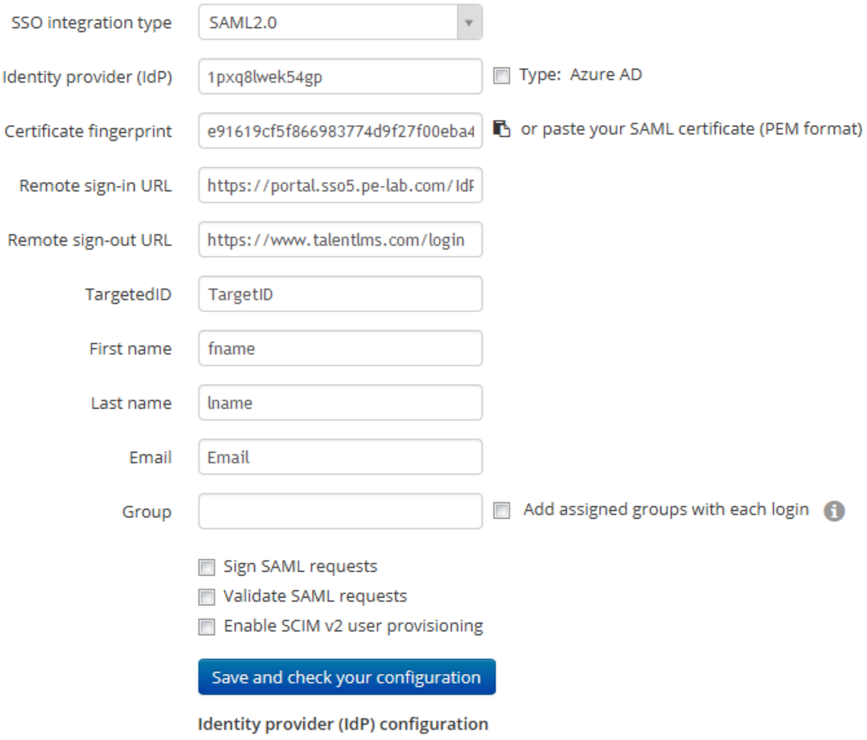


Signup: Manually (from Admin)

Default user type: Learner-Type

Default group: Select a group

2. Following UI will be displayed.



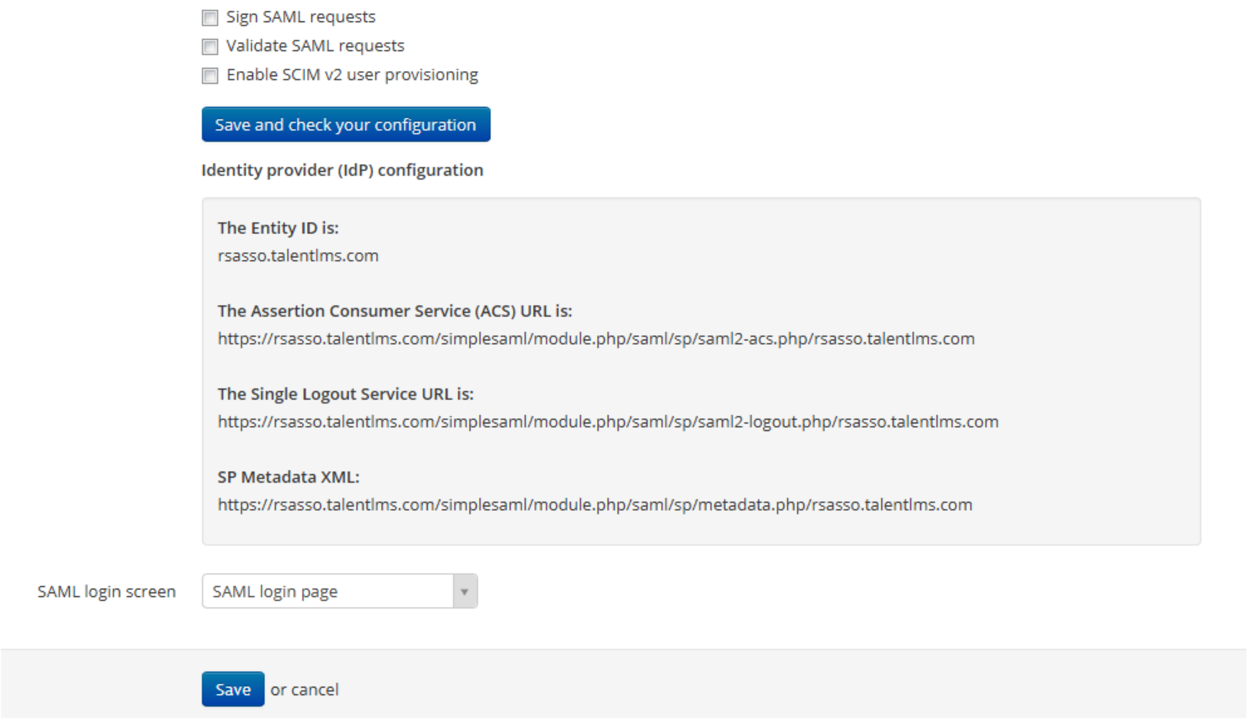
SSO integration type	SAML2.0	
Identity provider (IdP)	1pxq8lwek54gp	☐ Type: Azure AD
Certificate fingerprint	e91619cf5f866983774d9f27f00eba4	or paste your SAML certificate (PEM format)
Remote sign-in URL	https://portal.sso5.pe-lab.com/IdF	
Remote sign-out URL	https://www.talentlms.com/login	
TargetedID	TargetID	
First name	fname	
Last name	lname	
Email	Email	
Group		☐ Add assigned groups with each login

☐ Sign SAML requests
☐ Validate SAML requests
☐ Enable SCIM v2 user provisioning

Save and check your configuration
Identity provider (IdP) configuration

- **SSO integration type:** Choose SAML2.0 from the drop-down list
- **Identity provider (IdP):** type the Identity Provider's (IdP) URL
- **Certificate fingerprint:** fill-in the SHA-1 SAML certificate fingerprint provided by your IdP. Alternatively, you can download the SAML certificate in PEM format from your IdP, open it with your favorite text editor, and transfer its contents in the text area that will appear when you click on the "**paste your SAML certificate (PEM format)**" link. The SHA-1 SAML Certificate fingerprint will be computed when you click on the **Save** button. Keep in mind that TalentLMS will only work with RSA certificates. DSA certificates are not supported.
- **Remote sign-in URL:** fill-in the remote sign-in URL of your IdP. This is the URL where TalentLMS will redirect your users for signing-in. (refer to page 3 step 5)
- **Remote sign-out URL:** fill-in the remote sign-out URL of your IdP. This is the URL that TalentLMS will redirect your users when they sign-out.
- **TargetedID:** Specify 'TargetID' as value, this value will be supplied from IDP.
- **First name:** Specify 'fName' as value, this value will be supplied from IDP.
- **Last Name:** Specify 'lName' as value, this value will be supplied from IDP.
- **Email:** Specify 'Email' as value, this value will be supplied from IDP.

3. Click **Save** button



□ Sign SAML requests

□ Validate SAML requests

□ Enable SCIM v2 user provisioning

Identity provider (IdP) configuration

The Entity ID is:
rsasso.talentlms.com

The Assertion Consumer Service (ACS) URL is:
https://rsasso.talentlms.com/simplesaml/module.php/saml/sp/saml2-acs.php/rsasso.talentlms.com

The Single Logout Service URL is:
https://rsasso.talentlms.com/simplesaml/module.php/saml/sp/saml2-logout.php/rsasso.talentlms.com

SP Metadata XML:
https://rsasso.talentlms.com/simplesaml/module.php/saml/sp/metadata.php/rsasso.talentlms.com

SAML login screen: SAML login page