

Configure TalentLMS for Single Sign-On

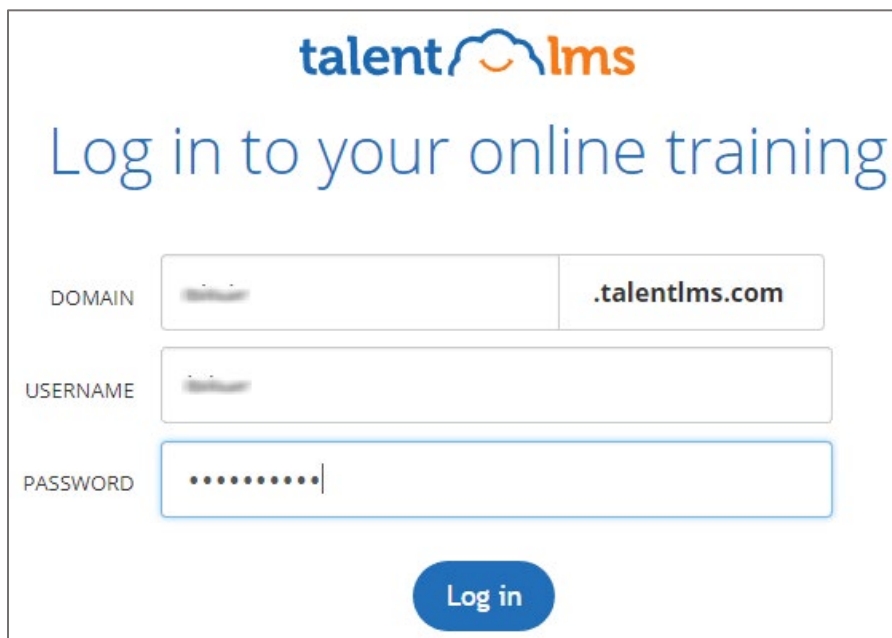
Configuring TalentLMS for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to TalentLMS by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

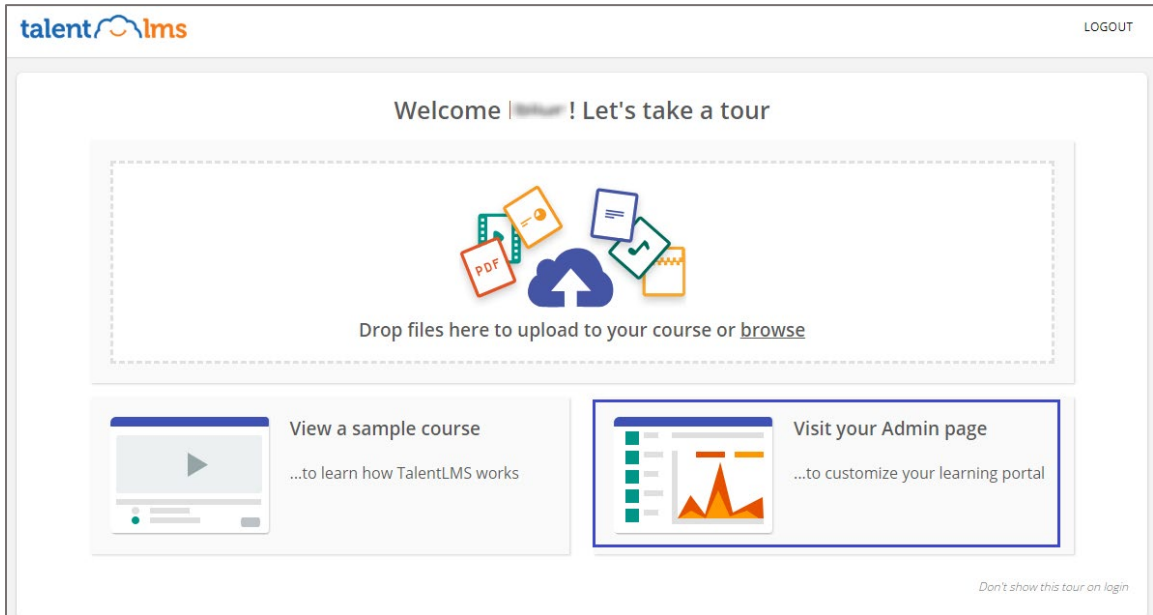
To configure TalentLMS for SSO by using SAML:

1. In a browser, type <https://app.talentlms.com/login> and press **Enter**.
2. Type your TalentLMS admin account credentials (**DOMAIN**, **USERNAME**, and **PASSWORD**) and click **Log in**.

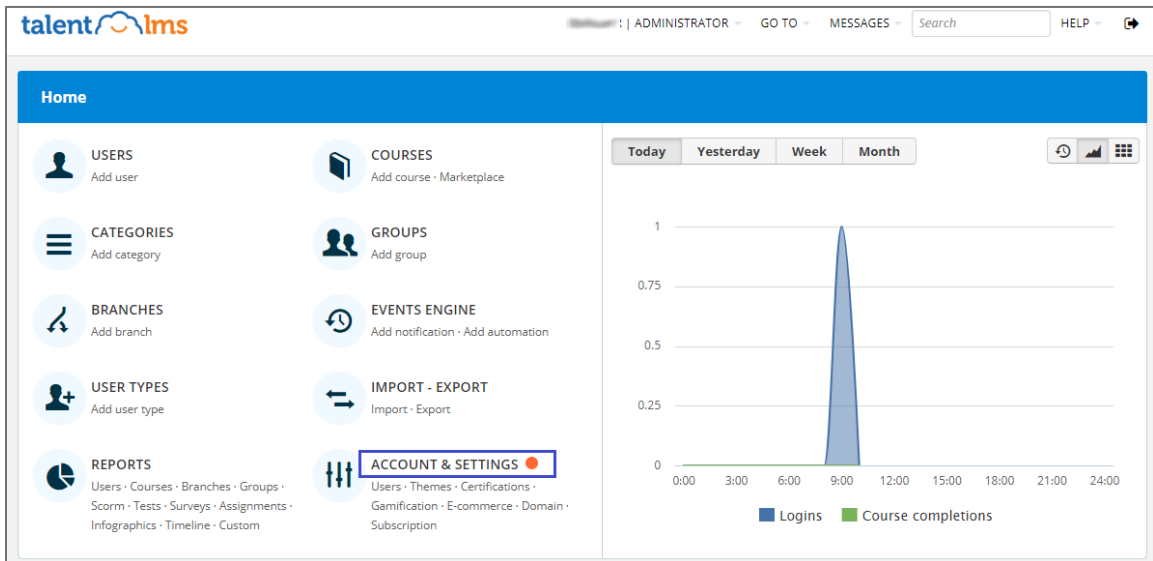


The screenshot shows the TalentLMS login interface. At the top, the logo "talentlms" is displayed in blue and orange. Below the logo, the text "Log in to your online training" is written in blue. The login form consists of three input fields: "DOMAIN" with a dropdown menu showing ".talentlms.com", "USERNAME" with a text input field, and "PASSWORD" with a masked input field (dots). A blue "Log in" button is located at the bottom center of the form.

3. In the dashboard page, click the **Visit your Admin page** tile.



4. In the **Home** page, click **ACCOUNT & SETTINGS**.



- In the **Account & Settings** page, click the **Users** tab.

Home / **Account & Settings**

Basic settings **Users** Themes Certifications Gamification E-commerce Domain Subscription

Signup

Default user type

Default group ⓘ

🔒 Password settings

📄 Terms of Service

👤 Visible user format

🗣️ Social options

Single Sign-On (SSO) **SAML2.0**

Save or cancel

- Click **Single Sign-On (SSO)** and enter the values for the following fields:

Required Information	Description
SSO integration type	Select SAML2.0 from the drop-down list.
Identity provider (IdP)	IdP URL
Certificate fingerprint	The certificate fingerprint is generated after pasting the SAML certificate.
SAML certificate	Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate----- Note: The IdP metadata is provided by Citrix and can be accessed from the link below. The link is displayed while configuring SSO settings for your app. <a href="https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml">https://gateway.cloud.com/idp/saml/<citrixcloudcust_id>/<app_id>/idp_metadata.xml
Alternative certificate fingerprint	Same as certificate fingerprint.
Remote sign-in URL	IdP logon URL
TargetedID	Username
First name	FirstName
Last name	LastName
Email	Email

SSO integration type: SAML2.0

Identity provider (IdP): [redacted] Type: Azure AD

Certificate fingerprint: [redacted]; or paste your SAML certificate (PEM format)

SAML certificate: paste your SAML certificate (PEM format)

Alternative certificate fingerprint: [redacted] or paste your SAML certificate (PEM format)

Remote sign-in URL: [redacted]

Remote sign-out URL: [redacted]

TargetedID: Username

First name: FirstName

Last name: LastName

Email: Email

Group: [redacted] 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

The Entity ID is: [redacted]

The Assertion Consumer Service (ACS) URL is: [redacted]

The Single Logout Service URL is: [redacted]

SP Metadata XML: [redacted]

SSO login screen: Login page + IdP login link

Save or cancel

7. Click **Save and check your configuration**.

Note: Note down the Entity ID, Assertion Consumer Service (ACS) URL, Single Logout Service URL, and SP Metadata XML for IdP configuration.

8. Finally, click **Save**.