

Configure TimeLive for Single Sign-On

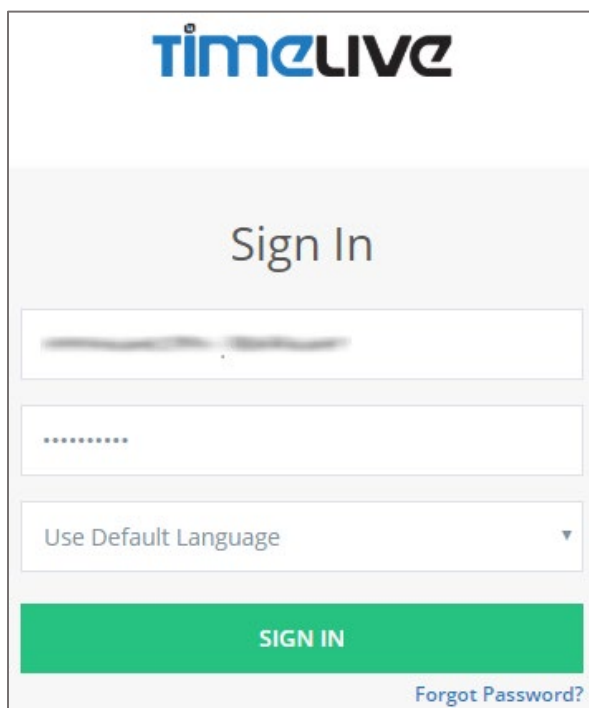
Configuring TimeLive for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to TimeLive by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

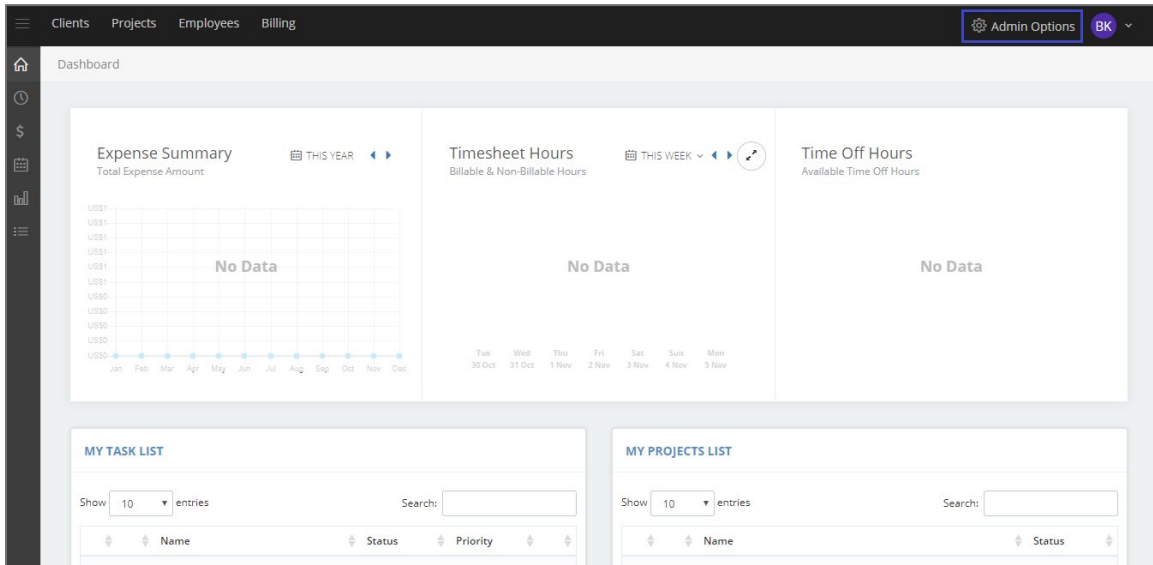
To configure TimeLive for SSO by using SAML:

1. In a browser, type <https://timelive.livetecs.com/> and press **Enter**.
2. Type your TimeLive admin account credentials (**Username** and **Password**) and click **SIGN IN**.

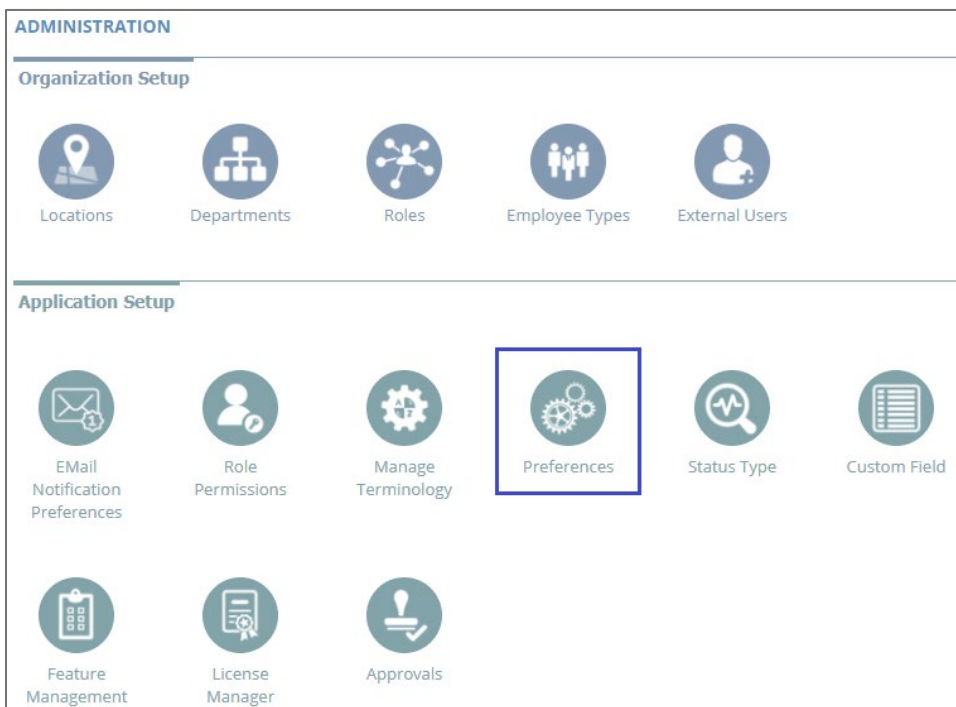


The screenshot shows the TimeLive Sign In page. At the top is the TimeLive logo. Below it is a grey header with the text "Sign In". There are two input fields: the first is for the username and the second is for the password, with the password field masked with dots. Below the password field is a dropdown menu labeled "Use Default Language" with a downward arrow. At the bottom is a green button labeled "SIGN IN" and a link labeled "Forgot Password?".

3. In the dashboard page, click **Admin Options**.



4. In the **ADMINISTRATION** page, click **Preferences**.



- In the **APPLICATION PREFERENCES** page, click the **Security** tab.
- Select the **Enable Single sign-on (SSO)** check box and enter the values for the following fields:

Field Name	Description
Sign in using Single Sign-On (SSO) with	Select SAML from the drop-down list.
SAML SSO URL	IdP logon URL
logout URL	IdP logout URL
X.509 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

The screenshot shows the 'APPLICATION PREFERENCES' page with the 'Security' tab selected. Under the 'Authentication Information' section, the following settings are visible:

- Enable Google Apps Authentication
- Enable Password Complexity
- Password Expiry Period: 0 Days (0 = No Expiry)
- Enable Single sign-on (SSO)
- Sign in using Single Sign-On (SSO) with: SAML
- SAML SSO URL
- logout URL
- X.509 Certificate: [Text area containing a blurred certificate string starting with -----BEGIN CERTIFICATE-----]

At the bottom right, there are two buttons: 'Update Preferences' and 'Cancel'.

- Finally, click **Update Preferences**.