

Configure Pacific Timesheet for Single Sign-On

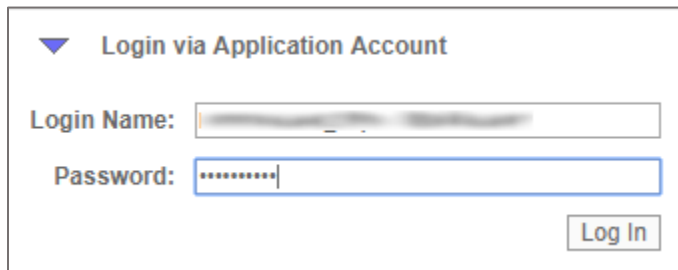
Configuring Pacific Timesheet for single sign-on (SSO) enables administrators to manage users of Citrix ADC. Users can securely log on to Pacific Timesheet by using the enterprise credentials.

Prerequisite

Browser Requirements: Internet Explorer 11 and above

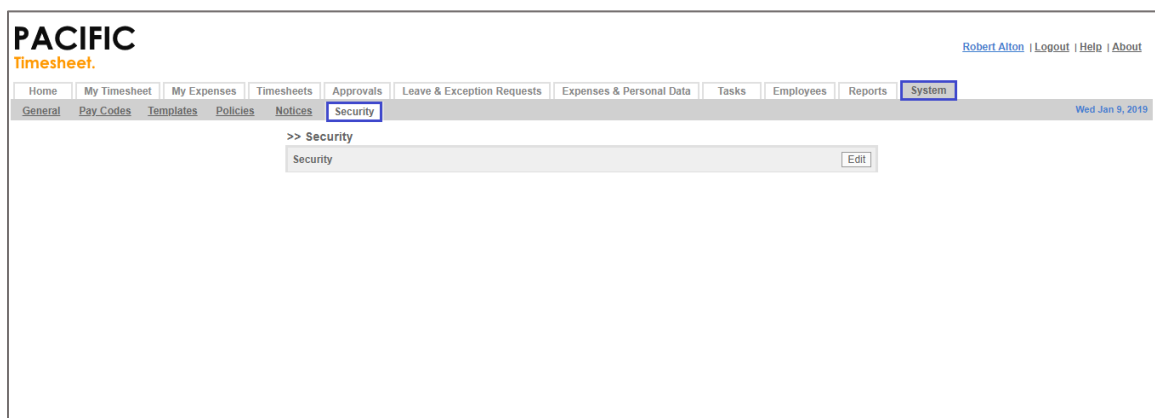
To configure Pacific Timesheet for SSO by using SAML:

1. In a browser, type <https://<customer domain>.pacifictimesheet.com/timesheet/home.do> and press **Enter**.
2. Click **Login via Application Account** in the left pane.
3. Type your Pacific Timesheet admin account credentials (**Login Name** and **Password**) and click **Log In**.



The screenshot shows a login form titled "Login via Application Account". It contains two input fields: "Login Name:" and "Password:". The "Login Name" field has a blurred value. The "Password" field contains several asterisks. A "Log In" button is located at the bottom right of the form.

4. In the dashboard page, click **System > Security**.



The screenshot shows the Pacific Timesheet dashboard. The top navigation bar includes "Home", "My Timesheet", "My Expenses", "Timesheets", "Approvals", "Leave & Exception Requests", "Expenses & Personal Data", "Tasks", "Employees", "Reports", and "System". The "System" menu is expanded, showing "General", "Pay Codes", "Templates", "Policies", "Notices", and "Security". The "Security" page is selected, showing a "Security" entry with an "Edit" button. The dashboard also displays the user name "Robert Alton", "Logout", "Help", and "About" in the top right corner, and the date "Wed Jan 9, 2019" in the bottom right corner.

5. In the **Security** page, click **Edit**.

6. In the pop-up window, enter the values for the following fields:

Required Information	Description
Authentication Type	Select SAML 2.0 SSO from the drop-down list.
Name	Citrix Netscaler
Issuer URL	IdP Issuer URL
SAML 2.0 Endpoint (HTTP)	IdP logon URL
Certificate (Primary)	<p>Copy and paste the IdP certificate. The IdP certificate must begin and end with -----Begin Certificate----- and -----End Certificate-----</p> <p>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</p>

>> Security

Security OK Cancel

Authentication Type: SAML 2.0 SSO

Note: Use the following URL to connect to Pacific Timesheet when setting up your application link in your identity provider:
[https://\[redacted\].pacifictimesheet.com/timesheet/home.do](https://[redacted].pacifictimesheet.com/timesheet/home.do)
(This is sometimes referred to as the Single Sign On URL, Destination URL or Recipient URL)

Name: Citrix Netscaler
This is the name used in the login button on the login page.

Issuer URL: [redacted]
For example: https://app.onelogin.com/saml/metadata/439734

SAML 2.0 Endpoint (HTTP): [redacted]
For example: https://app.onelogin.com/trust/saml2/http-post/ssa/439734

Certificate (Primary): [redacted]
The primary X.509 security certificate

Certificate (Secondary): [redacted]
The secondary or backup X.509 security certificate

Logging: Log authentication errors for troubleshooting

Expire idle sessions after: 30 Minutes

7. Select the **Log authentication errors for troubleshooting** check box.
8. Finally, scroll up and click **OK**.