

RSA SECURID[®] ACCESS

Implementation Guide

Pacific Timesheet

Gina Salvazo, RSA Partner Engineering
Last Modified: January 3, 2019



Solution Summary

Pacific Timesheet offers a cloud platform to consolidate and standardize your time tracking systems. Pacific Timesheet supports multi-factor authentication through SAML 2.0 via the service-provider login page or the RSA identity provider portal.

SAML 2.0 integrations have two specific use cases:

1. When integrated with Identity Router (IDR IDP), RSA provides single sign-on authentication and multi-factor authentication to Pacific Timesheet via SP or IDP initiated login. JIT provisioning is not supported.
2. Cloud IDP/ Relying Party, which is not supported by Pacific Timesheet at this time.

| RSA SecurID Access Features | |
|---|---|
| Pacific Timesheet | |
| On Premise Methods | |
| RSA SecurID | ✓ |
| On Demand Authentication | ✓ |
| Risk-Based Authentication (AM) | - |
| Cloud Authentication Service Methods | |
| Authenticate App | ✓ |
| FIDO Token | ✓ |
| SSO | |
| SAML SSO | ✓ |
| HFED SSO | - |
| Identity Assurance | |
| Collect Device Assurance and User Behavior | ✓ |



Configuration Summary

All of the supported use cases of RSA SecurID Access with Pacific Timesheet require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

RSA Cloud Authentication Service – Pacific Timesheet can be integrated with RSA Cloud Authentication Service in the following ways:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration](#)

[Pacific Timesheet SAML Configuration](#)



RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Pacific Timesheet in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

Configure RSA Identity Router SAML IdP

Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for Pacific Timesheet and click **+Add** to add the connector.



Pacific Timesheet
SAML Direct

+ Add

2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
 - a. In the **Connection URL** field, enter **IDP Provider URL**.
 - b. Choose **SP-initiated**.

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

Initiate SAML Workflow

Connection URL ?

IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed ?

No certificate loaded

Choose File

Generate Cert Bundle



4. Scroll down to SAML Identity Provider (Issuer) section.

SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp_id): pttest

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 Loaded



✓ Certificate Loaded

CN=gs.local, Valid Until: Dec
10, 2019 09:57 AM EST

Include Certificate in Outgoing Assertion

- a. Select **Choose File** and upload the private key.
- b. Select **Choose File** to import the public signing certificate.
- c. Select the checkbox for **Include Certificate in Outgoing Assertion**.



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

Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

6. In the Assertion Consumer Service (ACS) URL field replace **<DOMAIN>** with your site domain.
7. In the Audience (Service Provider Entity ID) field replace **<DOMAIN>** with your site domain.
8. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the NameID is set to format **unspecific** with the value of **mail**.

User Identity ?

NameID

Identifier Type Identity Source

Attribute Hunting ?

9. Click **Next Step**.
10. 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 ?

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

Status: Changes Pending



Partner Product Configuration

Before You Begin

This section provides instructions for configuring Pacific Timesheet with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Pacific Timesheet components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

Pacific Timesheet SAML Configuration

Complete the steps in this section to integrate Pacific Timesheet with RSA SecurID Access using SAML authentication protocol.

Procedure

1. Login into the Pacific Timesheet administration console. https://your_domain.pacifictimesheet.com.
2. Select **System > Security**.

PACIFIC Timesheet.

[Robert Alton](#) | [Logout](#) | [Help](#) | [About](#)

The screenshot shows the Pacific Timesheet administration console. The top navigation bar includes: Home, My Timesheet, My Expenses, Timesheets, Approvals, Leave & Exception Requests, Expenses & Personal Data, Tasks, Employees, Reports, and System (selected). Below this is a sub-menu for System: General, Pay Codes, Templates, Policies, Notices, and Security (selected). The Security page displays the following configuration:

- Authentication Type: Standard
- Maximum invalid login attempts before lockout:
- Maximum password age, in days:
- Maximum password history:
- Minimum password length: 5
- Minimum lower case characters:

An 'Edit' button is visible in the top right corner of the configuration box.

3. Click **Edit**.
4. From the Authentication Type pulldown select **SAML 2.0 SSO**.



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://eval28.pacifictimesheet.com/timesheet/home.do>
 (This is sometimes referred to as the Single Sign On URL, Destination URL or Recipient URL)

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

Issuer URL: `https://pe110.prod1.pe-lab.com/IdPServelet?idp_id=pfest`
For example: https://app.onelogin.com/saml/metadata/439734

SAML 2.0 Endpoint (HTTP): `https://pe110.prod1.pe-lab.com/IdPServelet?idp_id=pfest &`
For example: https://app.onelogin.com/trust/saml2/http-post/ssa/439734

Certificate (Primary):

```

MIIEAjEAMiZ3MubG99VWwwoEiMA0GCsAgSjB3DQERACQuAA4IBDw3wqaEKaQlBAQCr
byDEChHPVudV8V99bTUuJRWDZ1bwQjRvdlKkvtU3GFXSdAhFMccl.d/wa7FAnG
WU/+WApolZbWb3qzH4s3dCQZBCCGs12+MunUA3RFggwcyvTh6r5qwt1SvNRR4e
kkwi5ndkch56I6ZF4w/Bj39CBloc0RYLvwXb3qL0sy2XYDBKFN1MEqUKHqE5Jr
IMfV2TISKILDv88u7C3QIQepJN64nXBvRv9wIdEQV4Sdohcx8Afwv17nK45Qg/G
Jnp14BewAETdQWkJQvr+19YqC1DfnN1pEKRBBMjg3Arp5ZHxchXhoNxFb66Q14
pJFggciZxKHPWwz2i8qMR8AEwDQYJkqZihvCAQELR9AdDgeERAdDzbZPSccYC6T
m0aL1Iqr2wOLKQEU183WY0KqE910Mx91IqOXLSPyviU95RqQleahUW3SwcC
PEFGXCDL1nD5v034t60FC13kE70iVCQBByIS-09O8MEv5GI+qVUH+C7sJwwz7q
HK06dCoPW2+JbnTaWDQh5HkeZMDh9H4GaHroYa4cyblDWWKq9g7fscNsWn3fr9W
XVIFEVGgK3fY.C1rdU7Q7xRVhkmUyW/Z8agCamDImboSpeeenOdzZY9D6ZualZAR
X18QP0u86s+pmwRnAJTqXa48/2l8QhPZV8SLe5H3TVyG5L48vCpww8s0Lbm015r
XcoN6ZYCO0=
-----END CERTIFICATE-----
    
```

The primary X.509 security certificate

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

Logging: Log authentication errors for troubleshooting

Expire idle sessions after: 30 Minutes





5. In the **Name** field, enter a name that you want to appear as the SSO button on the login page.
6. In the **Issuer URL** field, enter the Identity Provider URL.
7. In the SAML 2.0 Endpoint (HTTP), enter the Identity Provider URL followed by &.
8. In the Certificate (Primary) field, paste the public certificate including the ---BEGIN and END statement.
9. Click **OK** to save.
10. Select the Employees tab and add a SSO user with the same email address as in RSA.

Timesheet.

Home My Timesheet My Expenses Timesheets Approvals Leave & Exception Requests Expenses & Personal Data Tasks Employees

Employees Groups

>> Employees >> New Employee

Employee Edit OK OK / Add Cancel

*Login Name:

*Password:

*Confirm Password:

First Name:

*Last Name:

ID:

*Status:

First Day:

Last Day:

Photograph: No file chosen