

# RSA SecurID Access SAML Configuration for TargetProcess



**Last Modified:** February 13, 2017

TargetProcess is a visual project management software solution that focuses on the agile software development methodology with out-of-the-box support for Scrum, Kanban etc. The software can be customized to support custom project management approaches and workflows. It is available as a SaaS and as a downloadable package.

## Before You Begin

- Acquire an administrator account to both RSA SecurID Access and TargetProcess.
- Obtain SP metadata details from the Service Provider.
- Obtain IdP metadata from IDR portal.

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

<b>SP Login URL</b>	<a href="https://rsa.tpondemand.com/login.aspx">https://rsa.tpondemand.com/login.aspx</a>
<b>ACS URL</b>	<a href="https://rsa.tpondemand.com/api/sso/saml2">https://rsa.tpondemand.com/api/sso/saml2</a>
<b>Service Provider Issuer ID</b>	<a href="https://rsa.tpondemand.com">rsa.tpondemand.com</a>

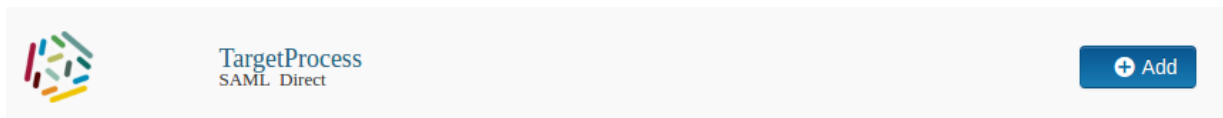
## Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure TargetProcess 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** TargetProcess.



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

4. Navigate to **Initiate SAML Workflow** section.
  - a. In the **Connection URL** field, keep the field blank as the value is not required.
  - b. Choose **IDP-initiated**.

---

 **Note:** The following IdP-initiated configuration works for SP-initiated TargetProcess connections as well.

---

## Initiate SAML Workflow

Connection URL 


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 ?

Issuer Entity ID ?

Default (idp\_id): ijrt7hetvzyv

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=gslab.com, Valid Until:  
11/03/2020

Include Certificate in Outgoing Assertion

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

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

## Service Provider

Assertion Consumer Service (ACS) URL ?

Audience (Service Provider Entity ID) ?

- a. In the **Assertion Consumer Service (ACS) URL** field, insert value as provided by Service Provider.
  - b. In the **Audience (Service Provider Entity ID)** field, insert value as provided by Service Provider.
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 ?

Attribute Hunting ?

NameID Attribute Hunting

8. Click **Next Step**.
9. On the **User Access** page, select **Allow All Authenticated Users** user policy from the drop down list.

## Access Policy

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

Allow All Authenticated Users

Select Custom Policy ?

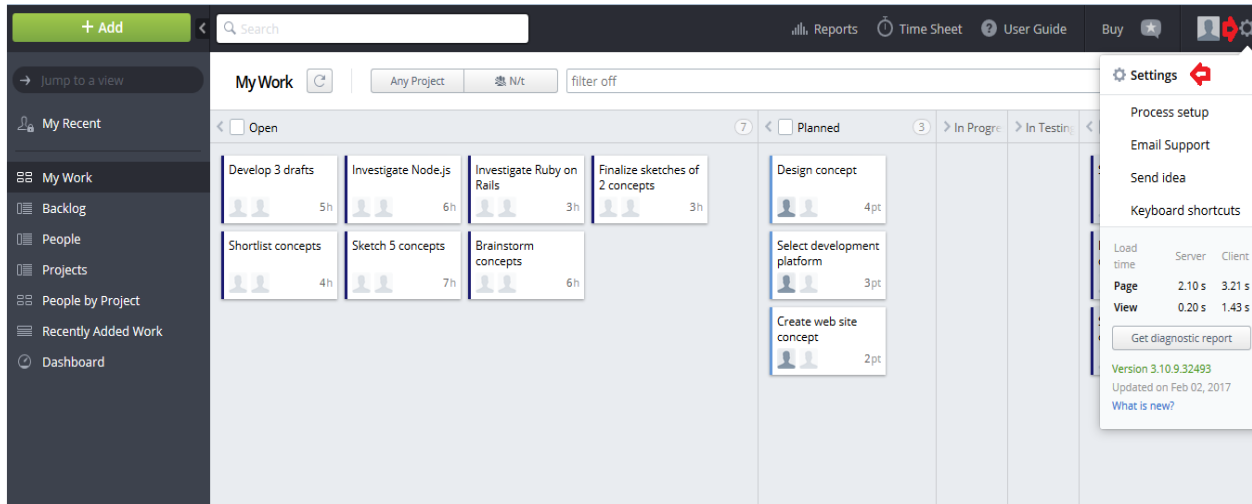
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



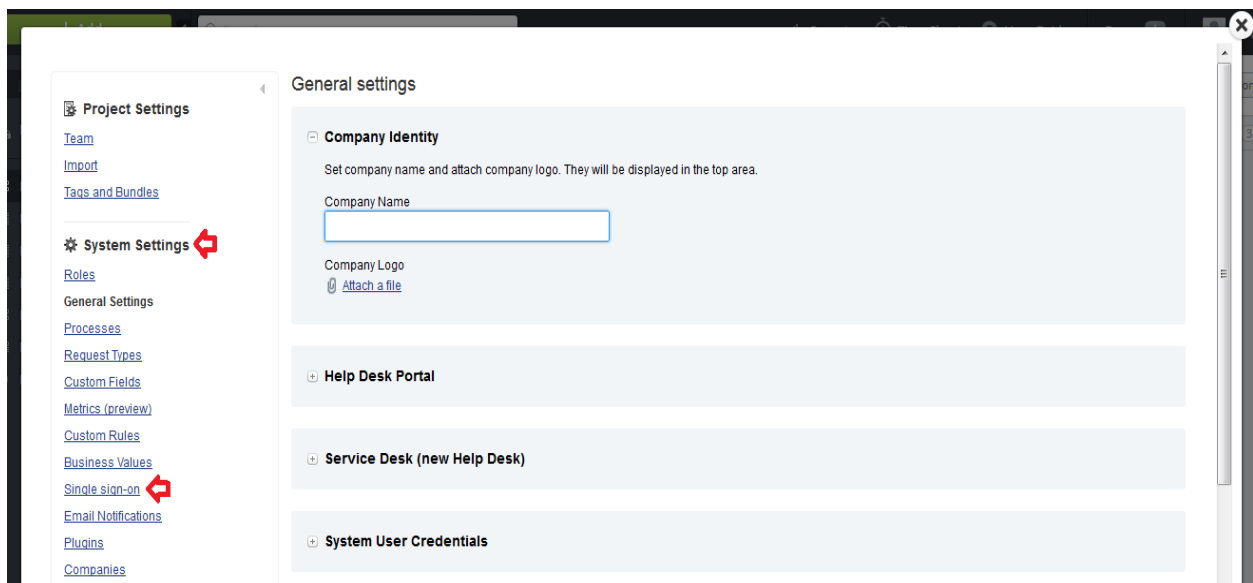
# Configure TargetProcess to Use RSA SecurID Access as an Identity Provider

## Procedure

1. Login to your TargetProcess account. (<https://www.targetprocess.com/login/>)
2. Following page will be displayed. Click on the gear icon available at top-right corner of the page followed by **Settings** option.



3. Following pop-up will be displayed. Click on **Single sign-on** option available under **System Settings** tab.



4. Following UI will appear.

General Settings  
Processes  
Request Types  
Custom Fields  
Metrics (preview)  
Custom Rules  
Business Values  
Single sign-on  
Email Notifications  
Plugins  
Companies  
System Log  
Audit History  
License  
Mashups  
Cleanup Sample Data

**TARGETPROCESS INFORMATION**  
Use these values to configure a connector in your identity provider settings:  
Assertion Consumer URL: <https://rsa.tpondemand.com/api/sso/saml2>

Enable Single Sign-on

Sign-on URL:

Certificate: 

```
-----BEGIN CERTIFICATE-----  
MIICpJCCAY6gAwIBAgIGAVgp4T9kMA0GCSqGSIb3DQEBCwUAMBQxEjAQBgNVBAMT  
CWdzbGFILmNvbTAeFw0xNjExMDMxMTA5MzdaFw0yMDE5MDMxMTA5MzdaMBQxEjAQ  
BgNVBAMTCWdzbGFILmNvbTCCASlwdQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB  
AJoUHRNu+TFz94saWXzKjWb5zhkYw8dGAOAPi6C/m7dO1ID/AlRUJPzcca+7dkU  
-----END CERTIFICATE-----
```

Enable JIT Provisioning  
 Disable login form

Exceptions list — allow these users to log in with their logins and passwords (the form is available at <https://rsa.tpondemand.com/login.aspx?login=form>):

Save

- Note** the **Assertion Consumer URL** provided under **TARGETPROCESS INFORMATION** section. It will be required while configuring Identity Provider SAML settings.
- Click on the **Enable Single Sign-on** checkbox.
- Sign-on URL** : Provide IdP endpoint URL value. Refer to page 3..  
[https://<Your IdP Portal URL>?idp\\_id=<Unique IdP ID>](https://<Your IdP Portal URL>?idp_id=<Unique IdP ID>)
- Certificate** : Paste IdP public certificate. Refer to page 3.
- Keep rest of the fields to their default values.

- Click on **Save** button to save SAML configurations.
- Your TargetProcess account is now enabled for SAML SSO authentication.