RSA SecurID Access SAML Configuration for ITRP

Last Modified: April 10, 2017

ITRP is a premium service management application service. It is the service management solution that tracks both end-to-end SLAs and the SLAs with external service providers. ITRP also offers an intuitive user interface and delivers fast response time for organizations that operate globally. ITRP does not support auto-provisioning of the user.

Before You Begin

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

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

SP Login URL	*https://gslab.itrp.qa/access/normal*
ACS URL	*https://gslab.itrp.qa/access/saml/consume*
Service Provider Issuer ID	*https://gslab.itrp.qa/*

Procedure

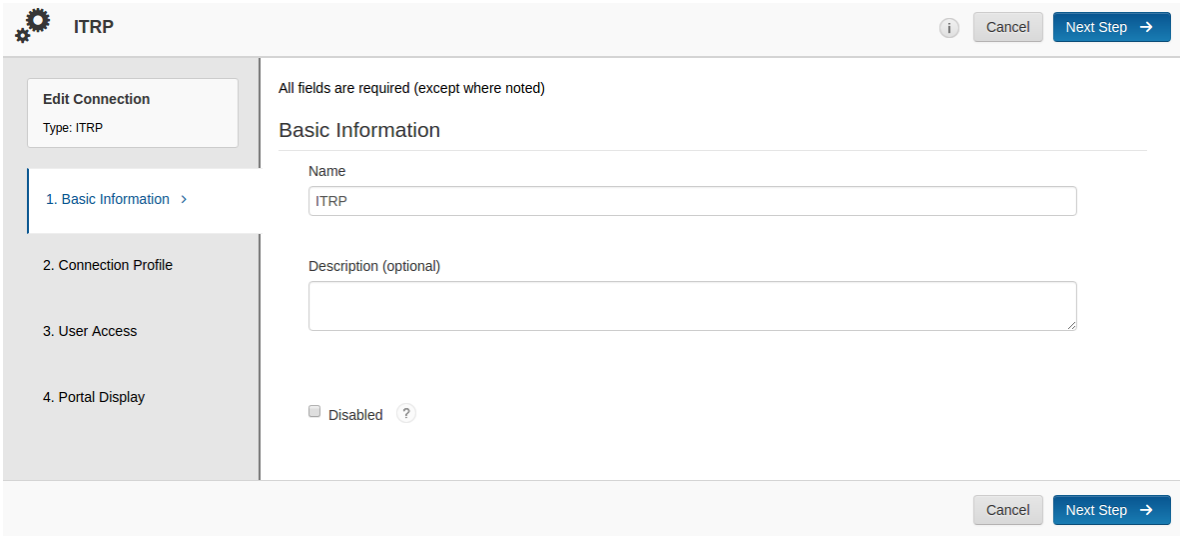
1. Add the Application in RSA SecurID Access
2. Configure ITRP to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

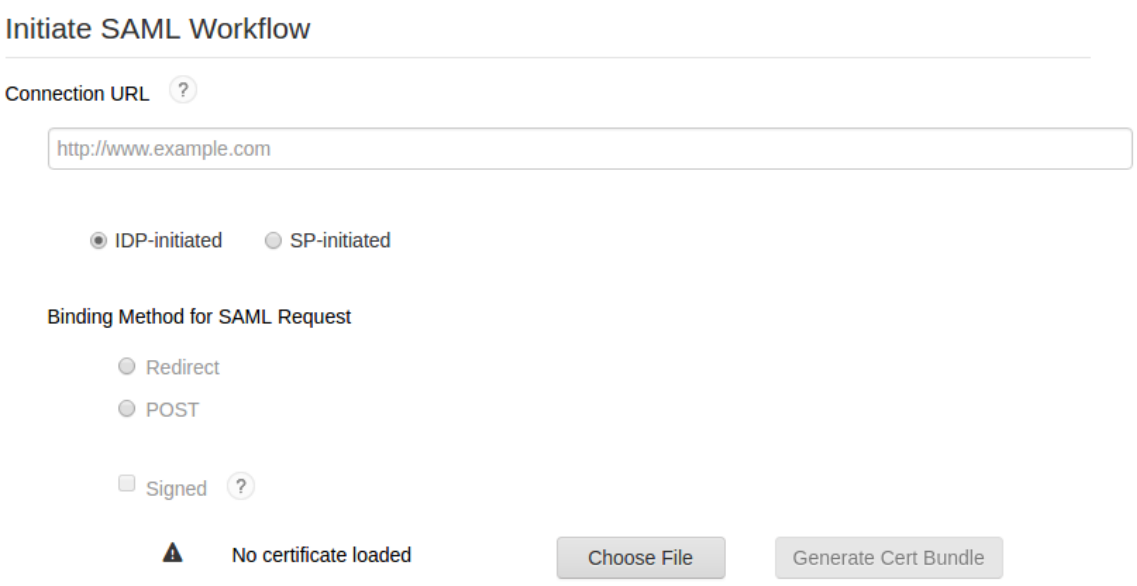
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** ITRP.

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

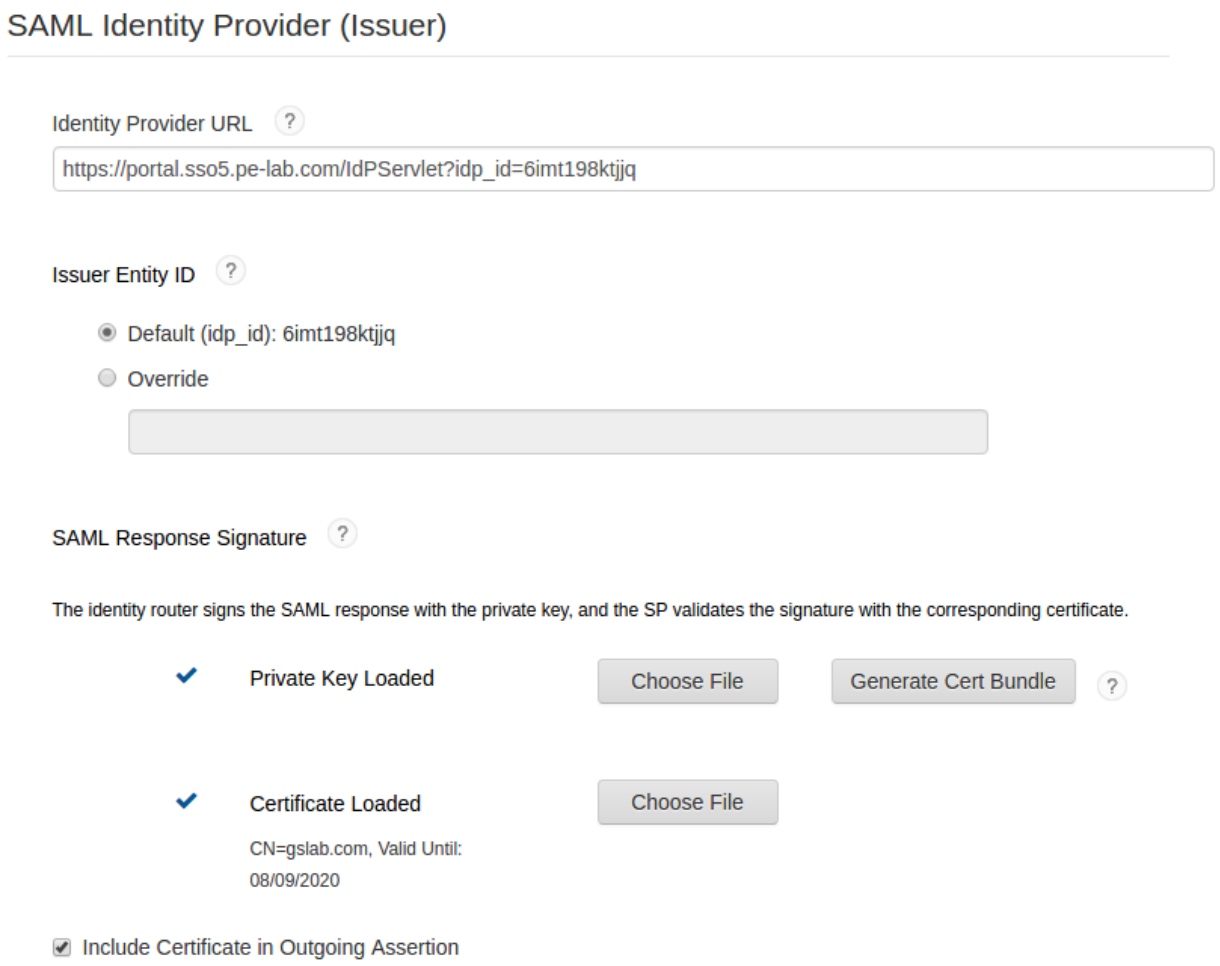


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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

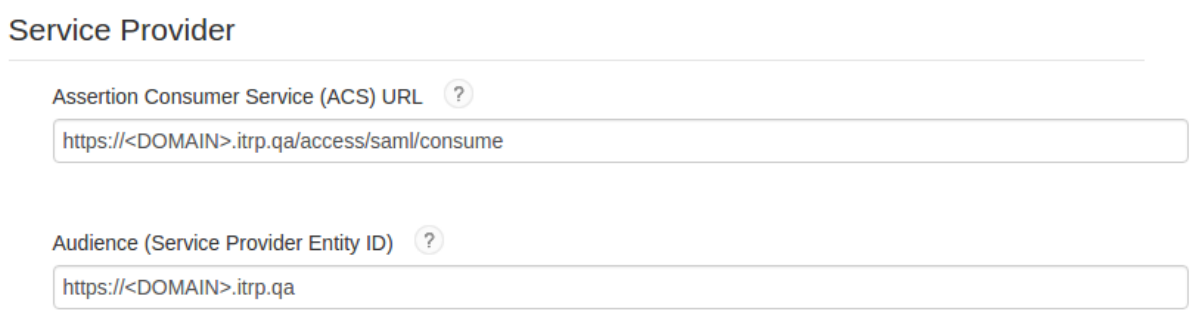


5. Scroll down to **SAML Identity Provider (Issuer)** section.

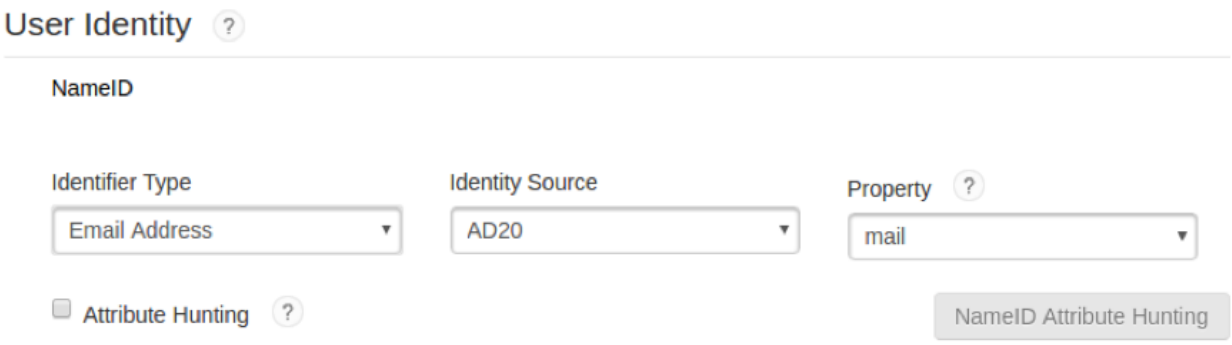


   a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
   b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
   c. Select **Choose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

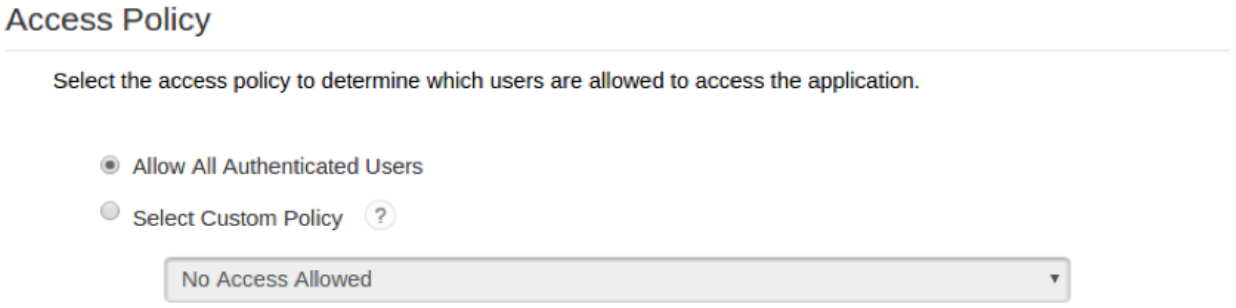
6. Scroll down to the **Service Provider** section.



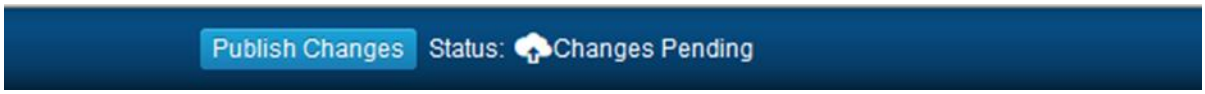
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> value with your organization account value.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> value with your organization account value.
7. Scroll down to the **User Identity** section. Verify the 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.



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



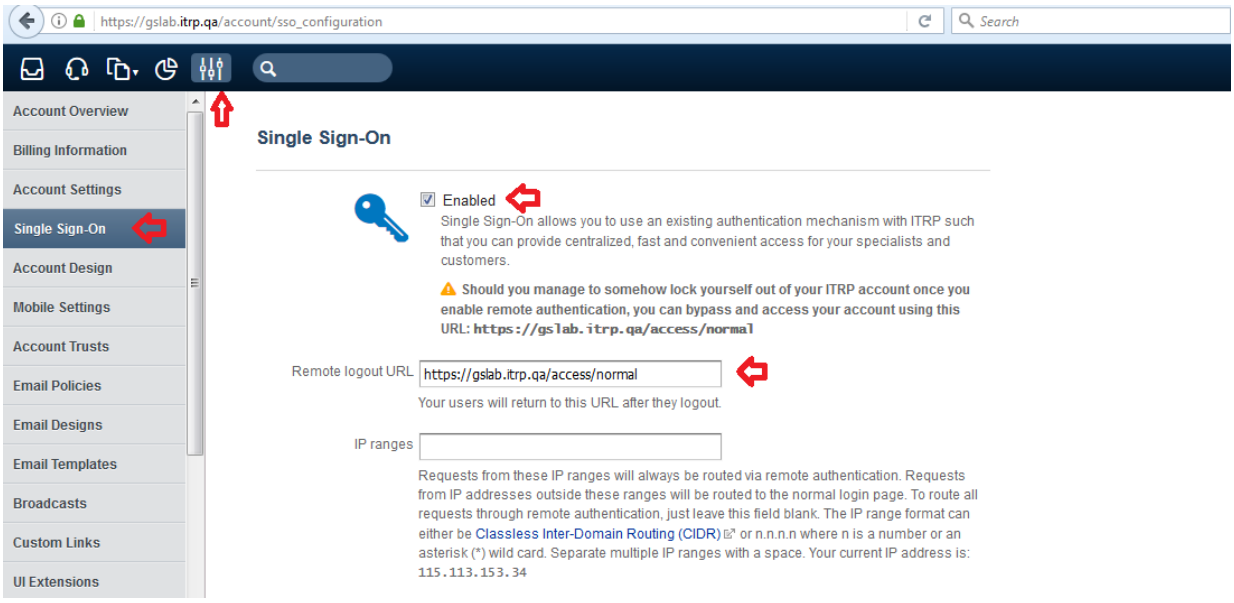
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



Configure ITRP to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to your ITRP application web account. (https://gslab.itrp.qa/access/normal)
2. Following UI will be displayed. Go to *Settings (symbol)* -> *Single Sign-On.*



   a. Click on **Enabled** checkbox to enable SAML SSO flow.
   b. **Remote logout URL**: Provide URL here where user will be redirected after logging out from the account.
   c. Keep the **IP ranges** field blank.

3. Move below on the same page.

   a. **SAML SSO URL** : Enter the Identity Provider URL found on page 3 step 5. It is of following format : https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>
   b. **Certificate fingerprint** : Provide fingerprint of the RSA SecurID Access IdP public certificate here.
   c. Keep the **Secondary fingerprint** field blank.
   d. Once sure of changes, click on **Save** button to complete configuration.

4. Your ITRP account is now enabled for the SAML authentication.

RJ