

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/

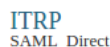
Procedure

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**.

The screenshot shows the 'Edit Connection' page for an ITRP connection. The page title is 'ITRP'. On the left, there is a sidebar with a list of steps: '1. Basic Information >', '2. Connection Profile', '3. User Access', and '4. Portal Display'. The main content area is titled 'Basic Information' and contains the following fields: 'Name' (with the value 'ITRP'), 'Description (optional)' (empty), and a 'Disabled' checkbox which is unchecked. At the top right and bottom right of the main content area, there are 'Cancel' and 'Next Step' buttons. A message at the top of the main content area states 'All fields are required (except where noted)'.

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.

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): 6imt198ktjjq

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:
08/09/2020

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 ?

https://<DOMAIN>.itrp.qa/access/saml/consume

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.itrp.qa

- 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.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

8. Click **Next Step**.
9. 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 ?

No Access Allowed

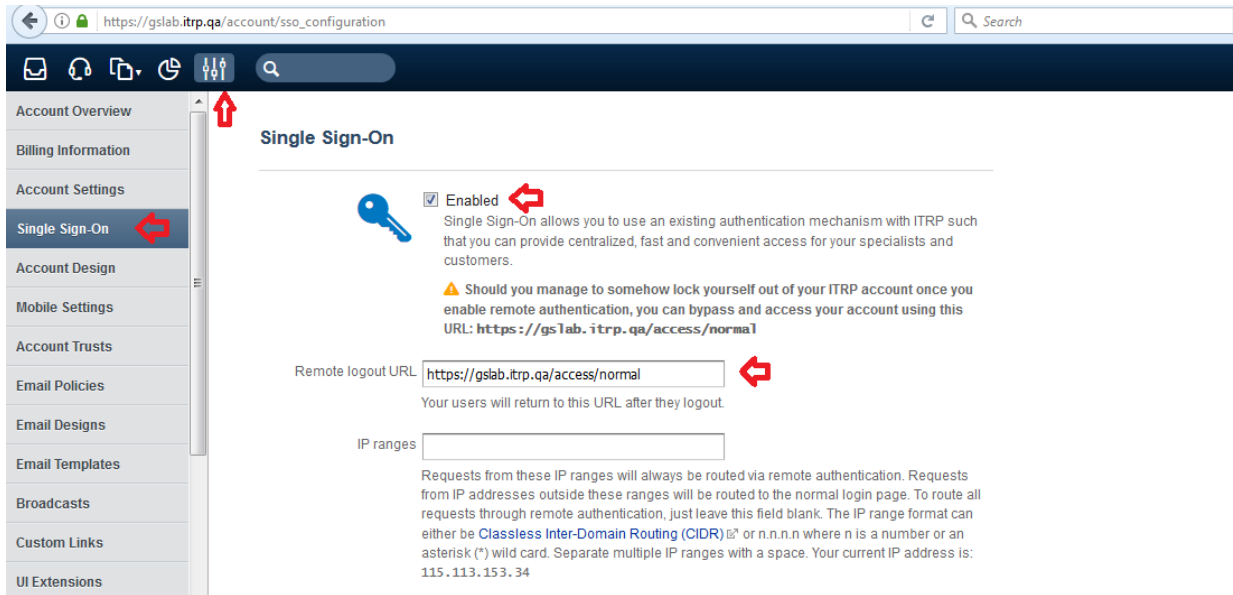
10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



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.

requests through remote authentication, just leave this field blank. The IP range format can either be **Classless Inter-Domain Routing (CIDR)** or n.n.n.n where n is a number or an asterisk (*) wild card. Separate multiple IP ranges with a space. Your current IP address is: 115.113.153.34

SAML

SAML SSO URL

This is the URL that ITRP will invoke to redirect users to your Identity Provider.

Note that our Assertion Consumer Service (ACS) URL is:
<https://gs1ab.itrp.qa/access/saml/consume>

To assist with troubleshooting, our SAML 2.0 metadata is located at:
<https://gs1ab.itrp.qa/access/saml/metadata>

Certificate fingerprint

The SHA1 fingerprint of the SAML certificate. Obtain this from your SAML identity provider.

Secondary fingerprint

The SHA1 fingerprint of the secondary SAML certificate, used for certificate rollover purposes. Obtain this from your SAML identity provider.

- 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>
- Certificate fingerprint** : Provide fingerprint of the RSA SecurID Access IdP public certificate here.
- Keep the **Secondary fingerprint** field blank.
- Once sure of changes, click on **Save** button to complete configuration.

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