RSA SecurID Access SAML Configuration for Image Relay

Last Modified: June 12, 2017

Image Relay is the Digital Asset Management system designed with your time in mind. Upload, organize, monitor, manage, and distribute your files from one centralized, secure, easy-to-use spot in the cloud. And if you ever need anything, everything is available at one click to cloud application.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Image Relay.

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

SP Login URL	*https://rsasso.imagerelay.com/*
ACS URL	*https://rsasso.imagerelay.com/sso/consume*
Service Provider Issuer ID	*https://rsasso.imagerelay.com/sso/metadata*

Procedure

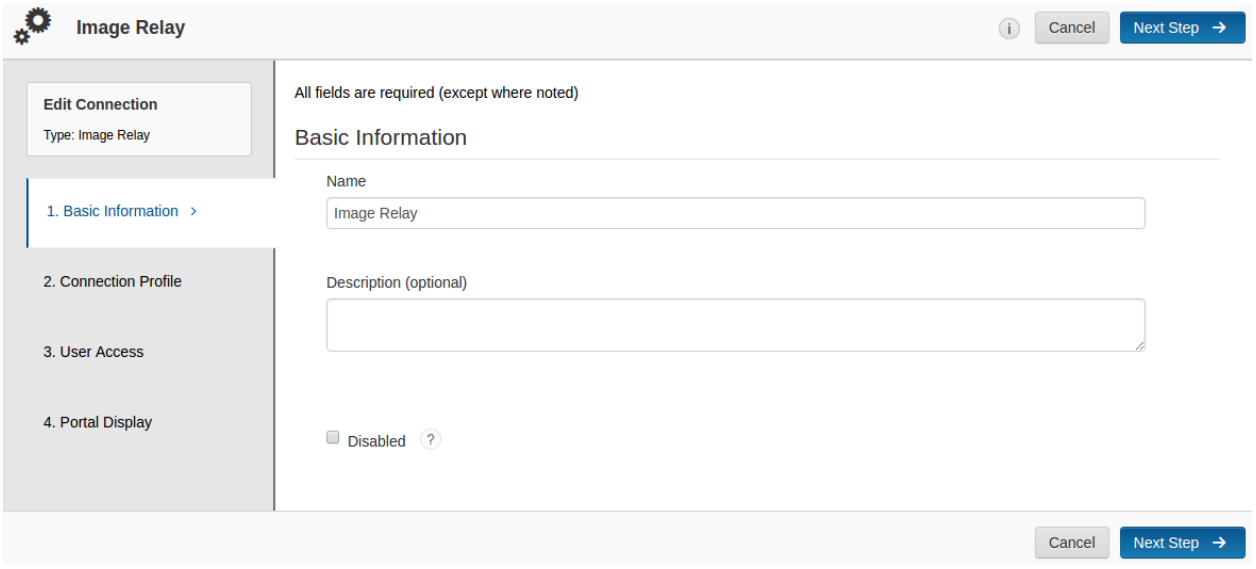
1. Add the Application in RSA SecurID Access
2. Configure Image Relay to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

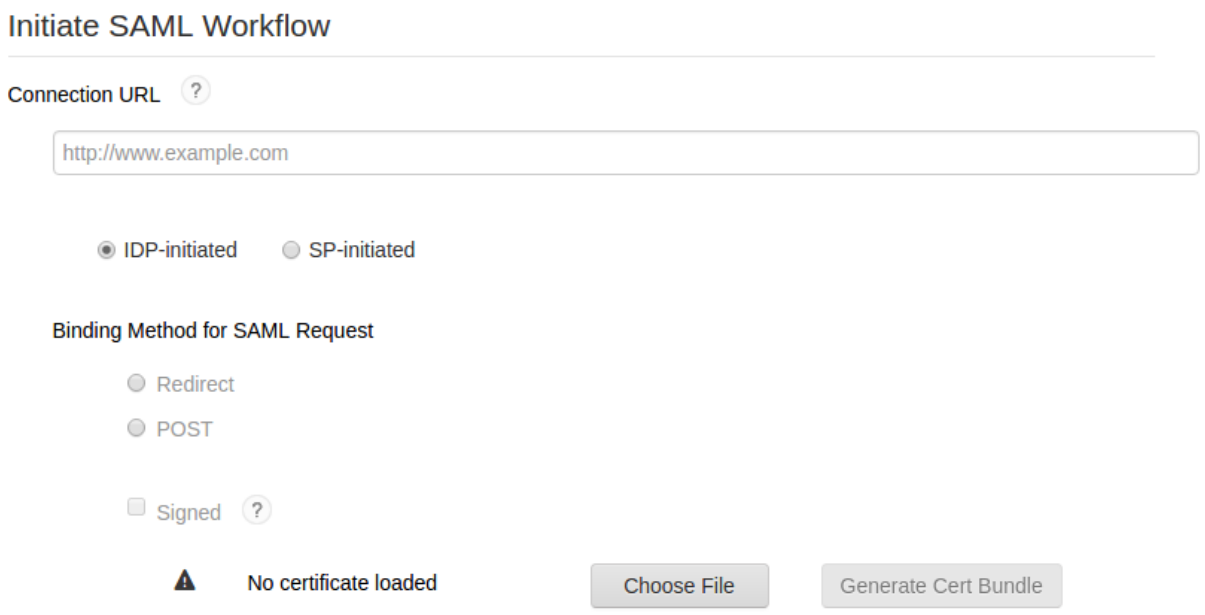
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** Image Relay.

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

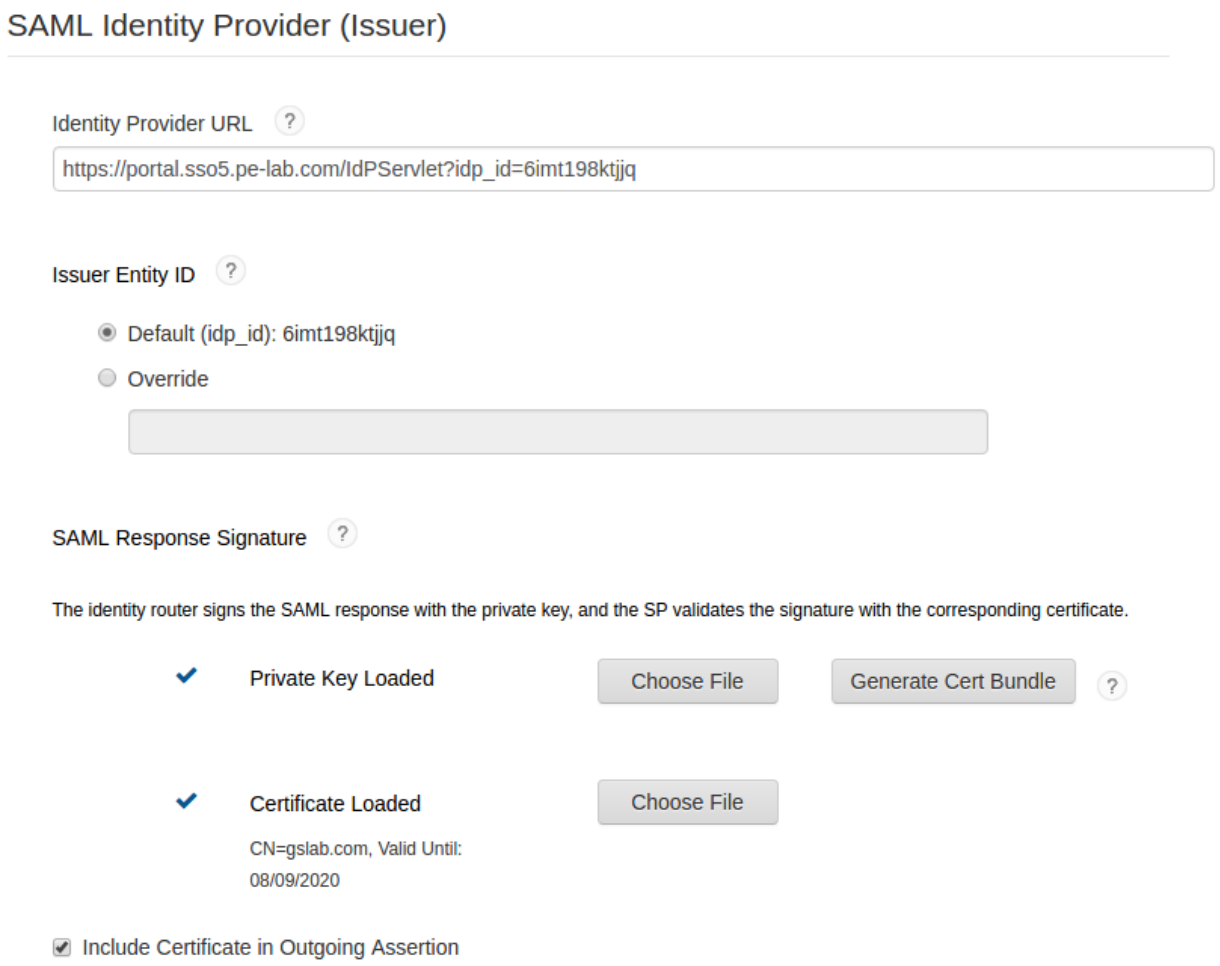


4. Navigate to **Initiate SAML Workflow** section.
   a. In the **Connection URL** field, keep the field blank as the value is not required.
   b. Choose **IDP-initiated.**

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



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

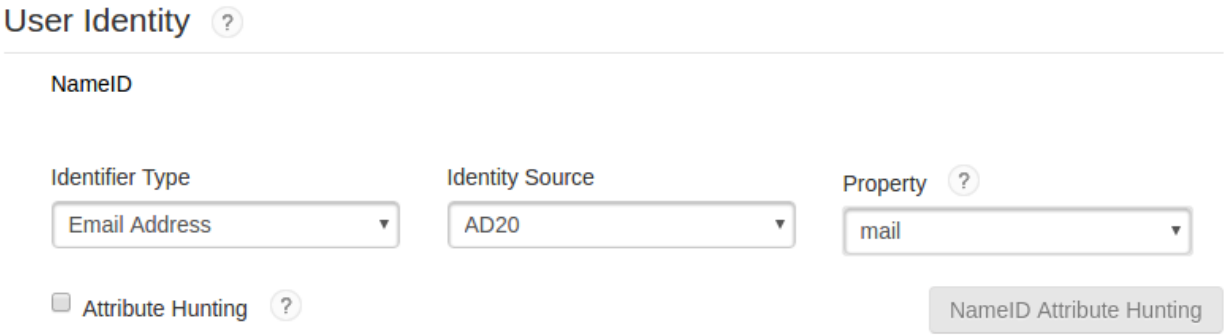


a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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.

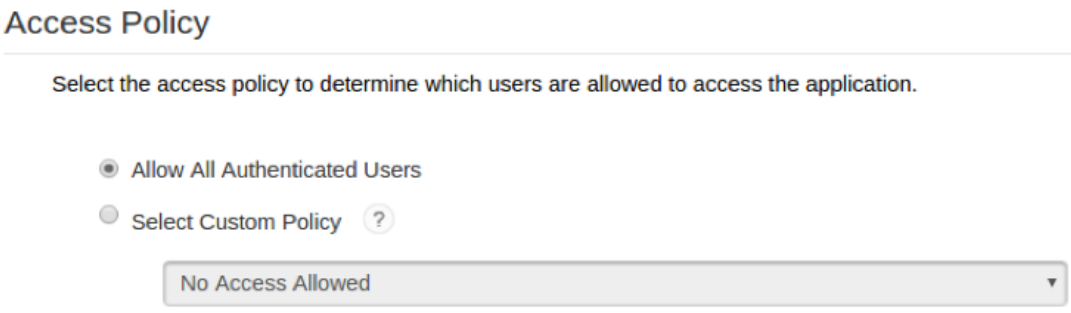
   a. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your organization domain name.
   b. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your organization domain name.

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.

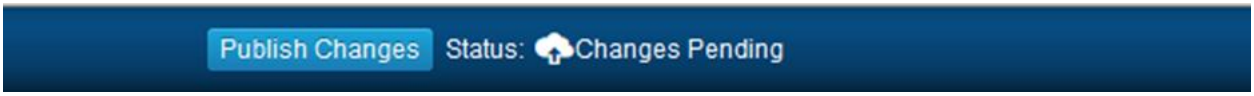


8. Click **Next Step**.

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

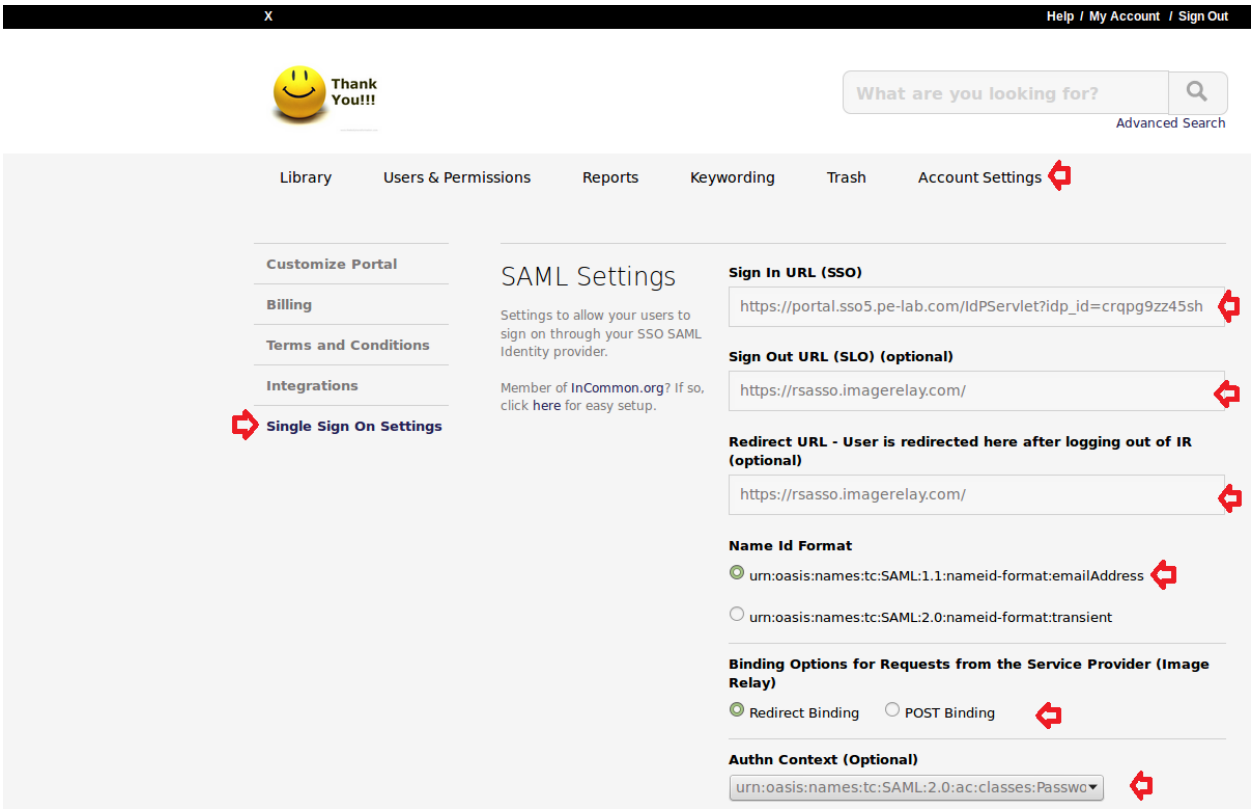


10. Click **Next Step**.
11. On the **Portal Display** page, select **Display in Portal**.
12. Click **Save and Finish**.
13. Click **Publish Changes**. Your application is now enabled for SSO.



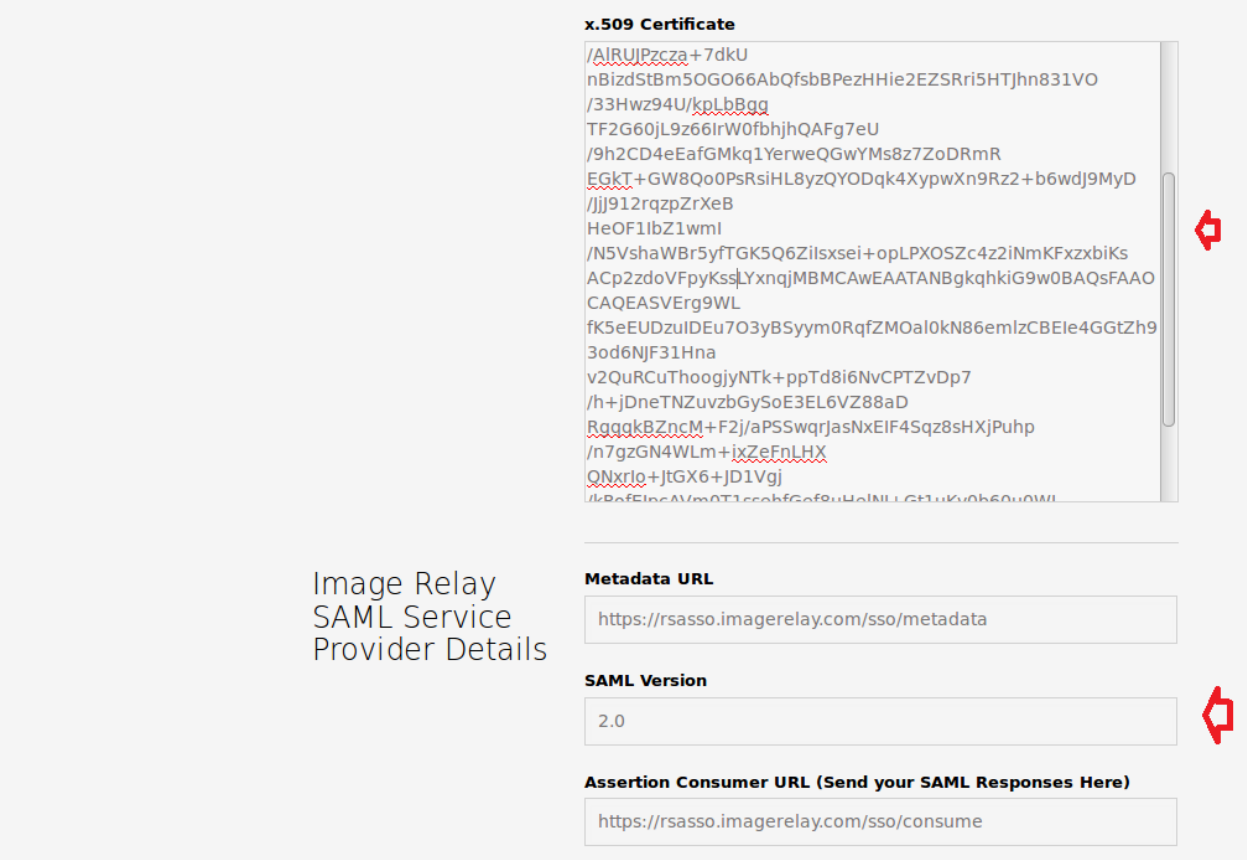
Procedure

1. Login to your Image Relay application web account. (https://rsasso.imagerelay.com)
2. Following UI will be displayed. Go to *Account Settings → Single Sign on Settings*.



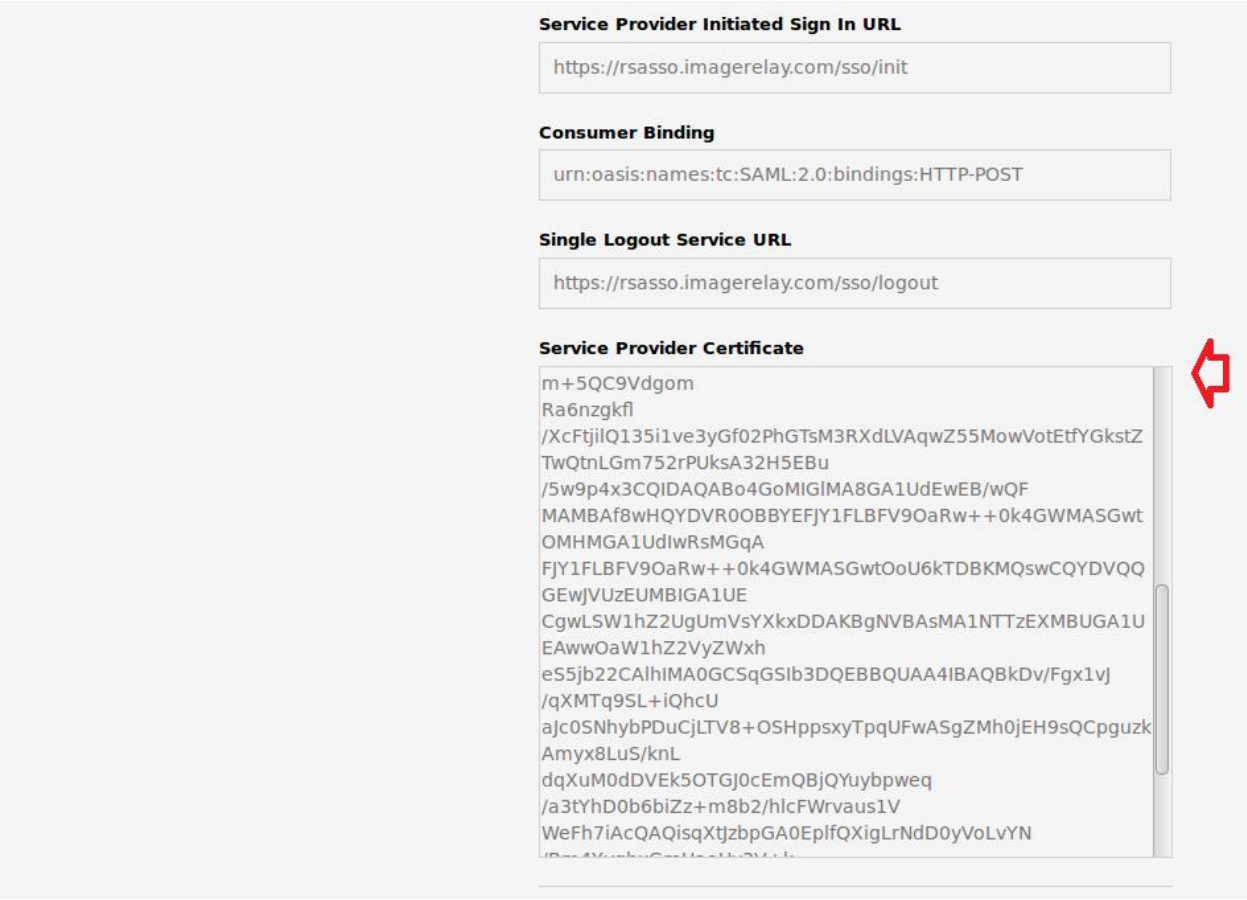
   a. **Sign In URL (SSO)** : Enter the Identity Provider URL found in *step – 5* on page - 3. It is of following format - https://<Your_Portal_URL>?idp_id=<Unique_IdP_ID>
   b. **Sign Out URL (SLO)** is the optional field. Provide here value of your choice Identity Provider specific.
   c. **Redirect URL** is the optional field. This value will be the URL where you will get redirected after logging out from the account.
   d. **Name Id Format** : Choose appropriate name id format as per your Identity Provider specific.
   e. Choose appropriate binding for **Service Provider initiated** login.
   f. **Auth Context** is the optional field. Choose appropriate authentication context Identity Provider specific.

3. Moving down on same page following UI will be displayed.

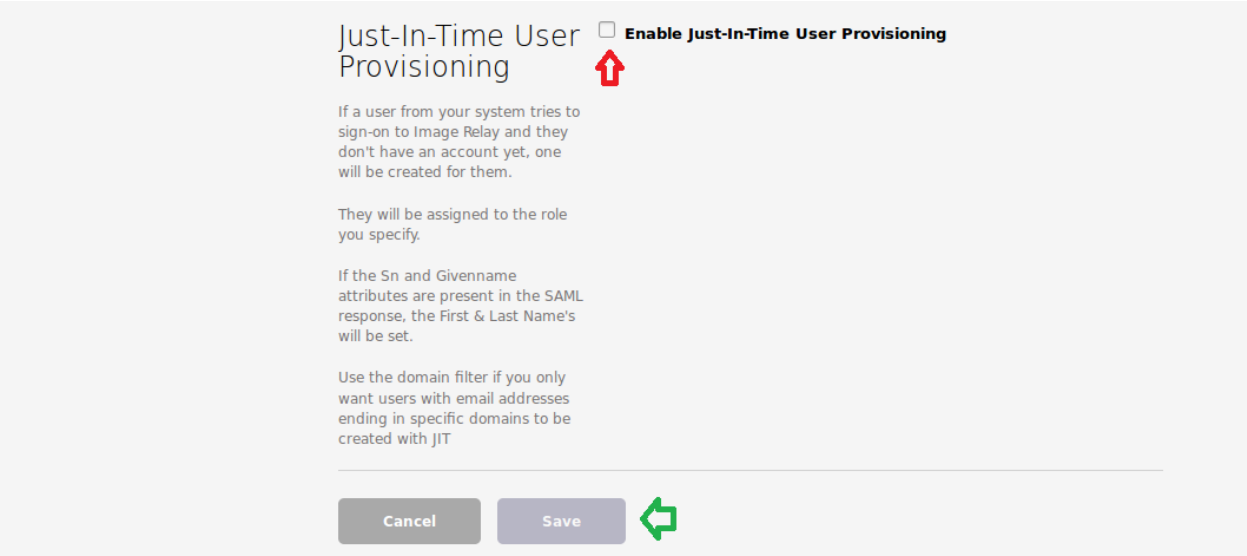


a. **x.509 Certificate** : Provide the RSA SecurID Access IdP public certificate here.
b. Make a note of service provider metadata details. These will come handy during identity provider side configurations.

4. Moving down on same page following UI will be displayed. Make a note of service provider metadata details. These will come handy during identity provider side configurations.



5. Moving down on same page following UI will be displayed.



   a. Click on **Enable Just-In-Time User Provisioning** option if you wish to auto-provision users whose account is not yet exist on Image Relay. Users will get created on the fly at the time of SSO if this option is enabled. By default, this field is optional.
   b. Once sure of all changes, click on **Save** button to complete configuration.

6. Your Image Relay account is now enabled for SAML authentication.

RJ