

**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:

<b>SP Login URL</b>	<a href="https://rsasso.imagerelay.com/">https://rsasso.imagerelay.com/</a>
<b>ACS URL</b>	<a href="https://rsasso.imagerelay.com/sso/consume">https://rsasso.imagerelay.com/sso/consume</a>
<b>Service Provider Issuer ID</b>	<a href="https://rsasso.imagerelay.com/sso/metadata">https://rsasso.imagerelay.com/sso/metadata</a>

## 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.



Image Relay  
SAML Direct




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

The screenshot shows the 'Image Relay' configuration interface. At the top, there is a header with a gear icon, the text 'Image Relay', and two buttons: 'Cancel' and 'Next Step →'. Below the header is a sidebar on the left with the following items: 'Edit Connection' (Type: Image Relay), '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' (text input with 'Image Relay'), 'Description (optional)' (text area), and a 'Disabled' checkbox with a help icon. At the bottom right of the main area are 'Cancel' and 'Next Step →' buttons. A note at the top of the main 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 Image Relay 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>.imagerelay.com/sso/consume

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.imagerelay.com/sso/metadata

- 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.

## 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.

[Publish Changes](#)

Status:  Changes Pending

# Configure Image Relay to Use RSA SecurID Access as an Identity Provider

## 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*.

The screenshot shows the 'Single Sign On Settings' page in the Image Relay application. The page has a navigation bar at the top with 'Account Settings' selected. On the left, there is a sidebar with 'Single Sign On Settings' highlighted. The main content area is titled 'SAML Settings' and contains several configuration fields, each with a red arrow icon indicating a required or important field:

- Sign In URL (SSO)**: A text input field containing the URL `https://portal.sso5.pe-lab.com/ldpServlet?idp_id=crqpg9zz45sh`.
- Sign Out URL (SLO) (optional)**: A text input field containing the URL `https://rsasso.imagerelay.com/`.
- Redirect URL - User is redirected here after logging out of IR (optional)**: A text input field containing the URL `https://rsasso.imagerelay.com/`.
- Name Id Format**: A radio button selection with two options: `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress` (selected) and `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`.
- Binding Options for Requests from the Service Provider (Image Relay)**: A radio button selection with two options: `Redirect Binding` (selected) and `POST Binding`.
- Authn Context (Optional)**: A dropdown menu showing the selected value `urn:oasis:names:tc:SAML:2.0:ac:classes:Passwo`.

- 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>](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.

Image Relay  
SAML Service  
Provider Details

**x.509 Certificate**

```
/AJRUJPzcza+7dkU  
nBizdStBm5OGO66AbQfsbBPezHHie2EZSRri5HTJhn831VO  
/33Hwz94U/kpLbBgg  
TF2G60jL9z66lrW0fbjhQAFg7eU  
/9h2CD4eEafGMkq1YerweQGwYMs8z7ZoDRmR  
EGkT+GW8Qo0PsRsiHL8yzQYODqk4XypwXn9Rz2+b6wdj9MyD  
/Jj912rqzpZrXeB  
HeOF1lbZ1wml  
/N5VshaWBr5yfTGK5Q6ZiIsxsei+opLPXOSZc4z2iNmKFxzxbiKs  
ACp2zdoVFpyKssLYxnqjMBMCAwEAATANBgkqhkiG9w0BAQsFAAO  
CAQEASVErg9WL  
fK5eEUDzulDEu7O3yBSyym0RqfZMOal0kN86emlzCBEIe4GGtZh9  
3od6NJF31Hna  
v2QuRCuThoogjyNTk+ppTd8i6NvCPTZvDp7  
/h+jDneTNZuvzbGySoE3EL6VZ88aD  
RgggkBZncM+F2j/aPSSwqrjasNxEIF4Sqz8sHXjPuhp  
/n7gzGN4WLM+ixZeFnLHX  
QNxrlo+JtGX6+JD1Vgj  
/kPafElocAVm0T1scobfGof8uHcMLLcT1uKy0b60u0W
```

**Metadata URL**

<https://rsasso.imagerelay.com/sso/metadata>

**SAML Version**

2.0

**Assertion Consumer URL (Send your SAML Responses Here)**

<https://rsasso.imagerelay.com/sso/consume>

- 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.

**Service Provider Initiated Sign In URL**

https://rsasso.imagerelay.com/sso/init

**Consumer Binding**


urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

**Single Logout Service URL**

https://rsasso.imagerelay.com/sso/logout

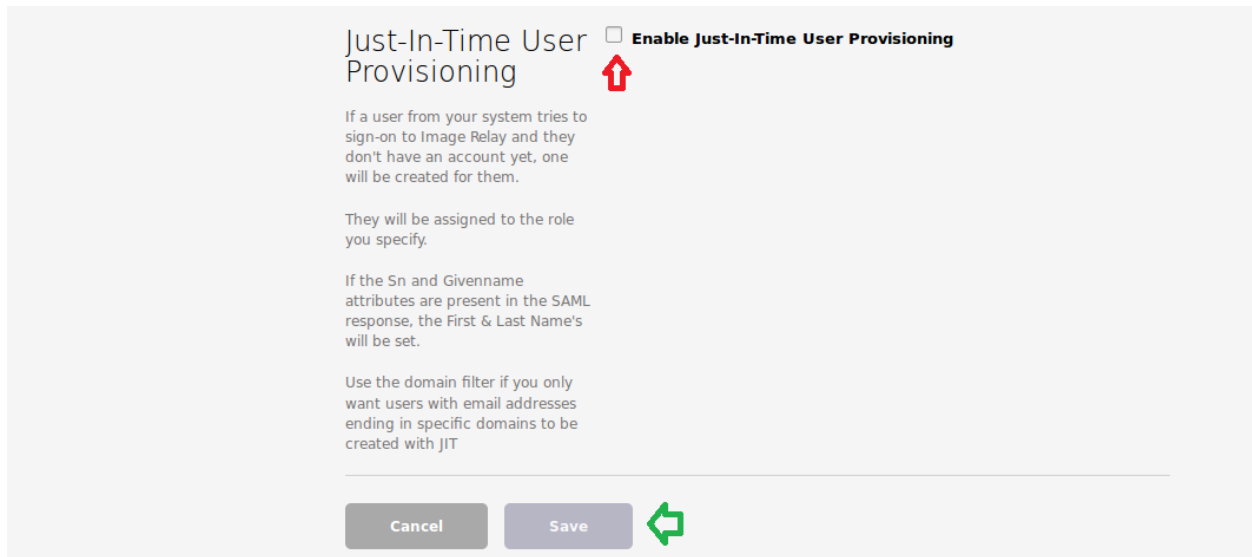
**Service Provider Certificate**

```
m+5QC9Vdgom
Ra6nzgkfl
/XcFtjilQ135i1ve3yGf02PhGTsM3RXdLVAqwZ55MowVotEtFYGkstZ
TwQtnLGm752rPUksA32H5EBu
/5w9p4x3CQIDAQABo4GoMIGIMA8GA1UdEwEB/wQF
MAMBAf8wHQYDVR0OBByEFJY1FLBFV9OaRw++0k4GWMASGwt
OMHMGA1UdlwRsMGqA
FJY1FLBFV9OaRw++0k4GWMASGwtOoU6kTDBKMQswCQYDVQQ
GEwJVUzEUMBIGA1UE
CgwLSW1hZ2UgUmVsYXkxDDAKBgNVBAsMA1NTTzEXMBUGA1U
EAwwOaW1hZ2VyZWxh
eS5jb22CAIhMA0GCSqGSIb3DQEBBQUAA4IBAQBkDv/Fgx1Vj
/qXMTq9SL+iQhcU
ajc0SNhybPDUcJLTV8+OSHppsxyTpqUFwASgZMh0jEH9sQCpguzk
Amyx8LuS/knL
dqXuM0dDVEk5OTGj0cEmQBjQYuybpweq
/a3tYhD0b6biZz+m8b2/hlcFWrvaus1V
WeFh7iAcQAQisqXtjzbpGA0EplfQXigLrNdD0yVoLVYN
-----BEGIN-----
```





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.