

# **RSA SECURID® ACCESS**

## **Implementation Guide**

### **ClearSlide**

Gina Salvazo, RSA Partner Engineering  
Last Modified: June 7, 2018



## Solution Summary

---

ClearSlide is a complete platform for Sales Enablement and Engagement that integrates content, communications and actionable insights. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. ClearSlide does support user auto-provisioning.

RSA SecurID Access Features	
ClearSlide	
<b>On Premise Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	✓
<b>SSO</b>	
SAML SSO	✓
HFED SSO	-
Identity Assurance	
Collect Device Assurance and User Behavior	✓



## Configuration Summary

---

The following supported use case of RSA SecurID Access with ClearSlide require both server-side and client-side configuration changes. This section of the guide includes links to the appropriate sections for configuring both sides for each use case.

**RSA Cloud Authentication Service** – ClearSlide can be integrated with RSA Cloud Authentication Service in the following way:

SAML via RSA Identity Router (IdP)

[Cloud Authentication Service – Identity Router IdP Configuration](#)  
[ClearSlide SAML Configuration](#)

## RSA SecurID Access Server Side Configuration

### *RSA Cloud Authentication Service Configuration*

#### SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for ClearSlide in the RSA SecurID Access Console. During configuration of the IdP you will need some information from the SP. This information includes (but is not limited to) Assertion Consumer Service URL and Service Provider Entity ID.

#### Configure RSA Identity Router SAML IdP

##### Procedure

1. Logon to the RSA SecurID Access console and browse to **Applications > Application Catalog**, search for ClearSlide and click **+Add** to add the connector.



2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
  - a. In the **Connection URL** field, leave the field blank.
  - b. Choose **IDP-initiated**.

**Note: The following IDP-initiated configuration works for SP-initiated as well.**

#### Initiate SAML Workflow

Connection URL

IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

No certificate loaded

4. Scroll down to SAML Identity Provider (Issuer) section.

## SAML Identity Provider (Issuer)

---

Identity Provider URL ?

Issuer Entity ID ?

- Default (idp\_id): ctest  
 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=gs.local, Valid Until: Dec  
10, 2019 09:57 AM EST

Include Certificate in Outgoing Assertion

- a. Make a note of Identity Provider URL field value, as it will be needed later to configure the service provider configuration.
- b. Select **Choose File** and upload the private key.
- c. Select **Choose File** to import the public signing certificate.
- d. Select the checkbox for **Include Certificate in Outgoing Assertion**.



5. Scroll down to the Service Provider section.

### Service Provider

Assertion Consumer Service (ACS) URL ?

https://www.clearslide.com/auth/saml\_login\_tx?tm=<TEAM\_ID>

Audience (Service Provider Entity ID) ?

<TEAM\_ID>

6. In the **Assertion Consumer Service (ACS) URL** field, replace <TEAM\_ID> with your ClearSlide Team ID for your account.
7. In the **Audience (Service Provider Issuer ID)** field, replace <TEAM\_ID> with your ClearSlide TEAM ID for your account.
8. 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

PE77

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attribute name **email** with the correlating value from your Identity source.

### Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc	email	PE77	mail	
+ ADD				

11. Click **Next Step**.



12. 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 ▼

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

**Publish Changes**

Status:  Changes Pending

## Partner Product Configuration

---

### ***Before You Begin***

This section provides instructions for configuring ClearSlide with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

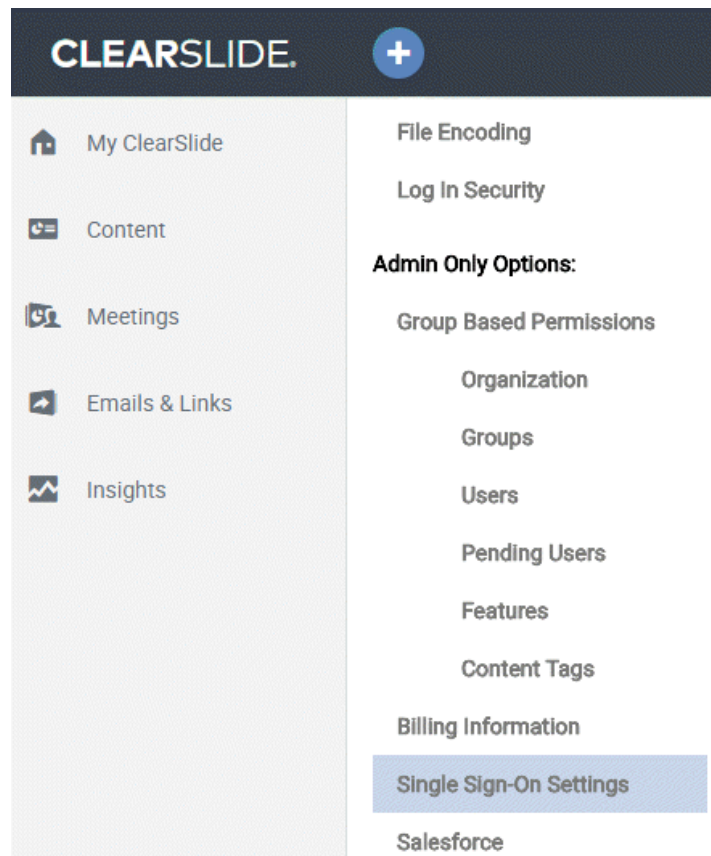
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All ClearSlide components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### **ClearSlide SAML Configuration**

#### **Procedure**

1. Contact ClearSlide and request SAML be enabled on your account.
2. Login to ClearSlide as an administrator.
3. Navigate to your account icon in the upper right and select **My Account**.
4. Under Admin Only Options, select **Single Sign-On Settings**.





- Use the Single Sign-On Provider pull down and select **SAML 2.0 Provider**.

Single Sign-on Settings

Single Sign-On Provider:

None

None

Google OAuth 2.0

**SAML 2.0 Provider**

- Check **Automatically create user accounts**.
- Check **Require Single Sign-On for all users**.

### Single Sign-on Settings

Single Sign-On Provider:

SAML 2.0 Provider

Automatically create user accounts

If checked, ClearSlide accounts will automatically be created when a new user logs in through your SSO provider. Note: this can affect your billing

Require Single Sign-On for all users

If checked, users will only be able to login to ClearSlide with their SSO credentials. If not, they can also use a ClearSlide account.

Custom Login URL:

<https://www.clearslide.com/login/> pe\_lab

Create a user-friendly URL that your team can use or bookmark to login to ClearSlide with Single Sign-On.

Single Sign-Out URL:

<https://pe108.prod0.pe-lab.com/LogoutServlet>

After logging out of ClearSlide, users will be presented with this URL, a shortcut to logging out of the account associated with your SSO provider.

Your ClearSlide SAML Settings

---

Your SAML provider will need this data

SAML Consumer URL:

[https://www.clearslide.com/auth/saml\\_login\\_tx?tm=22D744CA4B762ECF](https://www.clearslide.com/auth/saml_login_tx?tm=22D744CA4B762ECF)

This URL should be configured in your SAML provider and is the location where SAML posts are sent. It is sometimes called the 'destination URL' or 'post URL'.

ClearSlide Team ID:

22D744CA4B762ECF

This is sometimes required by your SAML provider. This is your unique Team ID in ClearSlide for Single Sign-On.

- The Custom Login URL is the url that users will use to login to ClearSlide with Single Sign-On.
- Take note of the Single Sign-On URL this is the Assertion Consumer Service URL configured in step 6 page 6.
- Take note of the Team ID as it is the Service Provider Entity ID configured in step 7 page 6.



11. Paste the public certificate used in step 4c. on page 5 into the X.509 Certificate field.
12. Click **Save**.

## Your SAML Provider Configurations

You will need to collect this data from your SAML provider  
IDP Metadata URL to fetch the data below:

Fetch IDP Data

We can automatically fill in the next three fields with the correct data if you have an IDP Metadata URL

SAML Provider Endpoint:

Your SAML provider should have given you this URL, which Clearslide will redirect to in order to begin the SAML authentication process

SAML Provider Entity ID:

The optional identify provider issuer if given to you by your SAML provider.

X.509 Certificate:

```
IwDFChHPvUdV8VIV89D6tUuJRWDZ1bwQjRydL/kkyqU3GFXSdaHFMccLdWa7FAnG
WJ/+WAPoIzBwNb3gztH4s3dCOZBCCGs12+MunUA3RFggwceyTh6r5gw11SvNBB4e
kKwl5ndkch56/j6ZF4v/Bjj39jCBlqc0RYLnwXb3qU0syXYDBKFN1MEqUKHqF5Jr
IMtfV2TSkiLDy86u7C3QIOeqJN64gXRvRv8w/dE0V4SdohzxAfjuv17pK45Qq/G
Jnp14BewAETd00WKJQvr+19YqC1DfnN1pEfKRRqMJg3Arp5ZHXchXhoNxFb66014
pJEpgclZxKHPiljrxZjAgMBAAEwDQYJKoZIhvcNAQELBQADggEBAdbZPSzcYC6T
m0oLi1gr2wOLKOEu63WY0KaF/0l0Mx91ifgOXLSpyryljJ95RqQlelshUWMSwS
PEFGXCDL1nD5v034t60FC13kE70iyjCQRByI5lz0908MEv5GI+qVUH+C7sJvwy7b
HK06dCpPW2+jbfnTsWDOh5HkeZMDbl9t4GaHrgYa4cvbLDWKg9g7fsCNcWg3fr9W
XVfFEVGqK3fYC1rU7Q7xRVhkMUyW/Z8aqCjpDTmho5peceqDdzZiY9D6ZualZAt9
XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV8SLe513TVwG5L48wCpxwBsolbM0l5r
XeoN8j2YCO0=
-----END CERTIFICATE-----
```

The optional identify provider issuer if given to you by your SAML provider.

Save
