

Last Modified: January 6th, 2017

CloudLock is a Cybersecurity-as-a-Service provider, protecting enterprises from compromised accounts, cloud malware, and data breaches in the cloud. CloudLock focuses on providing enterprise class security solution for data in the cloud.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and CloudLock.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of this manual.

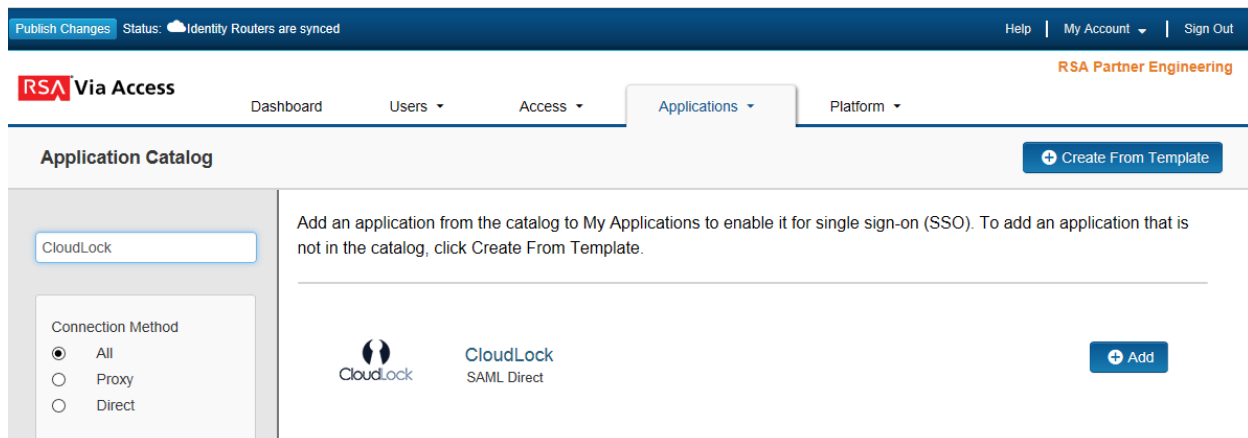
Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure CloudLock 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** for the SAML application that you wish to add.



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

 **Note:** The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.

4. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed

 No certificate loaded

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

SAML Identity Provider (Issuer)

Identity Provider URL

Issuer Entity ID

Default (idp_id): cloudlock

Override

Certificate Bundle

The certificate bundle is required to ensure a secure transaction.

Private Key Loaded

Certificate Loaded


CN=gs.local, Valid Until:
12/10/2019

Include Certificate in Outgoing Assertion

- a. Select **Choose File** and upload the RSA SecurID Access private key.
- b. Select **Choose File** and upload the RSA SecurID Access public certificate.
- c. 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>/gate/saml/sso/<your_domain>

Audience (Service Provider Entity ID) 

https://<domain>/gate/saml/sso/<your_domain>

- a. In the **Assertion Consumer Service (ACS) URL** field, replace **<domain>** with the CloudLock domain and **<your_domain>** with your SSO domain name. Example: <https://platform.cloudlock.com/gate/saml/sso/pe-lab.com>
 - b. In the **Audience (Service Provider Entity ID)** field, replace **<domain>** with the CloudLock domain and **<your_domain>** with your SSO domain name. Example: <https://platform.cloudlock.com/gate/saml/sso/pe-lab.com>
7. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

User Identity

Name ID

Identifier Type

Email Address 

User Store

PE_AD 

Property

mail 

Attribute Hunting

NameID Attribute Hunting

8. Click **Next Step**.

9. On the **User Access** page, select the desired user policy from the drop down list.

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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

Next Steps

[Configure CloudLock to Use RSA SecurID Access as an Identity Provider](#)

Create the RSA SecurID Access Metadata file

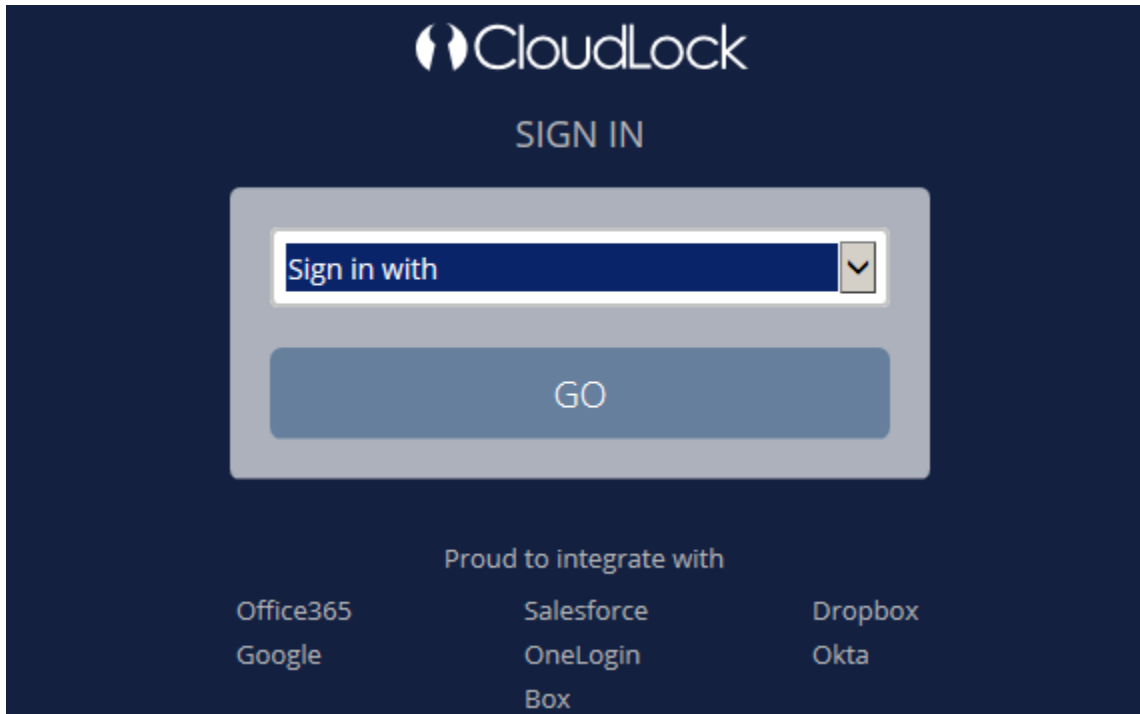
1. Modify the highlighted lines in the example below with your environment information.
2. When inserting the cert.pem file **do not** include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----lines.

```
<?xml version="1.0" encoding="UTF-8"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="cloudlock"><md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor
use="signing"><ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<!-- public saml cert -->
<ds:X509Data><ds:X509Certificate>CHANGE_ME_TO_PUBLIC_SAML_CERT_CONTENT
</ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:NameIDForm
at>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.
1:nameid-format:unspecified</md:NameIDFormat><md:SingleSignOnService
Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://pe110.prod1.pe-lab.com/IdPServlet?idp_id=cloudlock"/>
<md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://pe110.prod1.pe-lab.com/IdPServlet?idp_id=cloudlock"/>
</md:IDPSSODescriptor>
</md:EntityDescriptor>
```

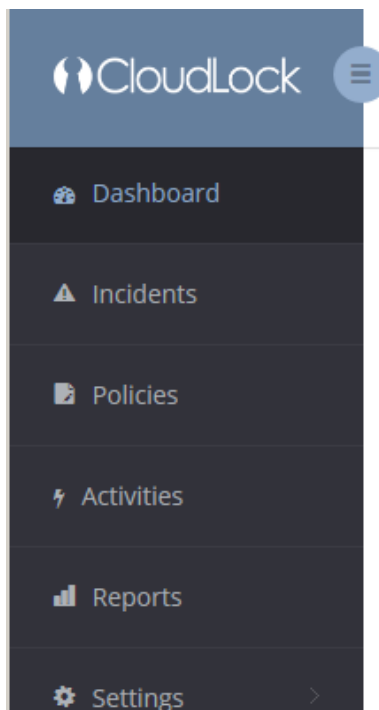
Configure CloudLock to Use RSA SecurID Access as an Identity Provider

Procedure


1. Login to CloudLock with an administrator account. In this example we used a Google account.
<https://platform.cloudlock.com>

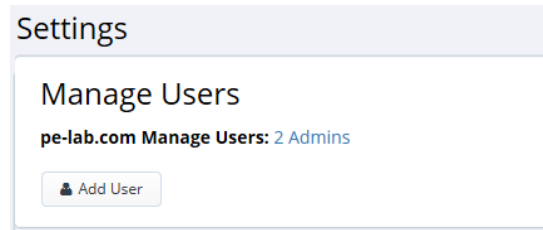


2. From the **Sign in with** pull down, select **Google** and enter your gmail credentials.
3. From the left side menu, select **Settings**.



- Open the Manage Users tab and click **Add user** to add any additional administrators to your account.

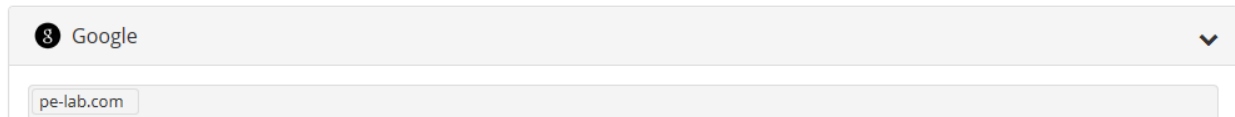
 **Note:** If the user role is enabled then the user will be assigned the role “superadmin”. Refer to CloudLock documentation for further information.



- Open the Platforms tab and add your company domain.

Domains

Box, Dropbox, Office365 and Google domains internal to your organization are defined here. Sharing with users outside these domains is considered external exposure. These internal domains apply only to Box, Dropbox, Office365 and Google.



- Open the CloudLock Data and APIs tab, and slide the SAML Login button to **ON**.
- Paste the RSA SecurID Access Metadata file into the Identity provider metadata window.

SAML Configuration

SAML Login ON

Identity provider metadata

```
<?xml version="1.0" encoding="UTF-8"?><md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
entityID="cloudlock"><md:IDPSSODescriptor WantAuthnRequestsSigned="true"
protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><md:KeyDescriptor use="signing"><ds:KeyInfo
xmlns:ds="http://www.w3.org/2000/09/xmldsig#"><ds:X509Data><ds:X509Certificate>MIICpDCCAyAgAwIBAgIGAVGMZf+XMA0GCS
qGS1b3DQEBChUAMBMAQCBAMT
CGdzLmxvY2FsMB4XDTE1MTIxMDE0NTc1M1oXDTE5MTIxMDE0NTc1M1owEzERMA8G
A1UEAxMIZ3MubG9jYXVwZG9iEiMA0GCSqGSIb3DQEBBAQAA4IBDwAwggEKAoIBAQCc
lwDFChHPvUdV8VIV89DbTUujRWDZ1bwQJRYdL/kkyqU3GFXSdaHFMcclDwa7FAnG
WJ/+WAPolZbwNb3gztH4s3dCOZBCCGs12+MunUA3RfgwceyTh6r5gwI15vNBB4e
kKwI5ndkch56/j6ZF4v/Bji39jCBIqc0RYLnwXb3qU0syXYDBKFN1MEqUKHqF5Jr
IMtFV2TSKILdy86u7C3QIOeqjN64gXRvRv8w/dE0V4SdohzxAfjuv17pK45Qq/G
Jnp14BewAETdO0WKJQvr+19YqC1DfnN1pEfKRRqMjg3Arp5ZHxchXhoNxhFb66O14
pJEpgclZxKHPjIirxZjAgMBAAEwDQYJKoZIhvcNAQELBQADggEBADbZP5zcYC6T
m0oLi1gr2wOLKOEUE63WY0KaF/010Mx91ifgOXLSPyryljj95RqQlelshUWMSwsC
PEFGXCDL1nD5v034t60FC13ke70iyjCQRByl5lz09O8MEv5GI+qVUH+C7sjvwy7b
HK06dCpPW2+JbfnTsWDOh5HkeZMDbl9t4GaHrgYa4cvbLDWKg9g7fsCncWg3fr9W
XVfFEVGqK3fYc1rU7Q7xRVhKMUjW/Z8aqCjPDTmho5peceqDdzZY9D6ZualZat9
XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV85Le5113TVwG5L48wCpxwBsoLbM0I5r
XeoN8j2YCO0=
</ds:X509Certificate></ds:X509Data></ds:KeyInfo></md:KeyDescriptor><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:namei
d-format:emailAddress</md:NameIDFormat><md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:unspecified</md:NameIDFormat><md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://pe-lab.com/IdPService?idp_id=cloudlock"/></md:SingleSignOnService
```

Submit

- Click **Submit**.

GLS