




# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

### **FileCloud**

Gina Salvazo, RSA Partner Engineering  
Last Modified: January 25, 2018



## Solution Summary

---

FileCloud is the leading, self-hosted file sharing, sync and mobile access for Businesses. This integration supports both SP-initiated authentication as well as IDP-initiated flow. FileCloud supports auto-provisioning of users.

<b>RSA SecurID Access Features</b>	
<b>FileCloud</b>	
<b>On Premise Methods</b>	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
<b>Cloud Authentication Service Methods</b>	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
<b>SSO</b>	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

<b>Identity Assurance</b>	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with FileCloud 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** – FileCloud 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](#)  
[FileCloud 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 FileCloud 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 FileCloud 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 and choose **SP-initiated**.
4. In Connection URL field, replace **<YOUR\_DOMAIN>** with your domain, for example **http://pelab.filecloudonline.com/authsamlssso.php**.

 **Note:** The following SP-initiated configuration works for IdP-initiated FileCloud connections as well.

#### Initiate SAML Workflow


Connection URL 

IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

Choose File

Generate Cert Bundle

# FileCloud

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

## SAML Identity Provider (Issuer)

---

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): fctest

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

- Take note of the Identity Provider URL.
- Click **Override**, under Issuer Entity ID and paste the Identity Provider URL in this field.
- 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**.

# FileCloud

6. Scroll down to the **Service Provider** section.

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://<YOUR\_DOMAIN>/simplesaml/module.php/saml/sp/saml2-acis.php/default-sp

Audience (Service Provider Entity ID) ?

https://<YOUR\_DOMAIN>/simplesaml/module.php/saml/sp/metadata.php/default-sp

7. In the Assertion Consumer Service (ACS) URL field, replace **<YOUR\_DOMAIN>** with your domain; for example **https://pelab.filecloudonline.com/simplesaml/module.php/saml/sp/saml2-sca.php/default-sp**.
8. In the Audience (Service Provider Issuer ID) field, replace **<YOUR\_DOMAIN>** with your domain.
9. Scroll down to the **User Identity** section. Verify the settings are correct for your environment. In this example the username to be presented in unspecified format and the user account will be validated against the User Store selected.

## User Identity ?

NameID

Identifier Type

unspecified

Identity Source

PE77

Property ?

sAMAccountName










Attribute Hunting ?

NameID Attribute Hunting

# FileCloud

10. Click **Show Advanced Configuration**.
11. Under the Attribute Extension section, enter values for **givenname, surname, uid, email**.

## Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	givenname	PE77 ▾	givenName ▾	 
Identity Sc ▾	surname	PE77 ▾	sn ▾	 
Identity Sc ▾	uid	PE77 ▾	userPrincipa ▾	 
Identity Sc ▾	email	PE77 ▾	mail ▾	 
 ADD				

12. Click **Next Step**.
13. 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 ▾

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

**Publish Changes**

Status:  Changes Pending

# FileCloud

18. Navigate to **Applications > My Applications**.

19. Locate **FileCloud** in the list and from the **Edit** option, select **Export Metadata**.




FileCloud

Created From: FileCloud

SAML Direct

Edit ▼

 Edit

 Export Metadata

 Delete



# FileCloud

## ***Before You Begin***

This section provides instructions for configuring FileCloud 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 FileCloud components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## **FileCloud SAML Configuration**

### **Procedure**

1. Log into your FileCloud application web account as company administrator.  
**https://<YOUR\_DOMAIN>/ui/admin/index.html**
2. Navigate to **Settings > SSO**.
3. From the Default SSO Type pull down select **SAML**.
4. Enter the **Identity Provider URL** from page 5 in the IdP End Point URL field.
5. Enter **uid** in the IdP Username Parameter field.
6. Enter **mail** in the IdP Email Parameter field.
7. Enter **givenname** in the IdP Given Name Parameter field.
8. Enter **sn** in the IdP Surname Parameter field.
9. Copy the whole [RSA SecurID Access metadata](#) into the **Identity Provider (IDP) Metadata** window.

- HOME
  - Dashboard
- USERS/GROUPS
  - Users
  - Groups
  - Admins
- MANAGE
  - Team Folders
  - Network Folders
  - User Shares
  - Folder Permissions
- DEVICES
  - Devices
- MISC.
  - Audit
  - User Locks
  - Workflows
  - Reports
- SETTINGS
  - Settings
- CUSTOMIZATION
  - Customization

## Manage Settings

Reset All

- Server
- Storage
- Authentication
- Admin
- Email
- Endpoint Backup
- License
- Policies
- SSO**
- Team Folders
- Misc

### Single Sign On (SSO) Settings

Reset to defaults

Default SSO Type  Specify the Single Sign On Type

### SAML Settings

IdP End Point URL  URL of the Identity Provider that the Service Provider must contact.

IdP Username Parameter  Username Parameter Name in Identity Provider

IdP Email Parameter  Email Parameter Name in Identity Provider

IdP Given Name Parameter  Given Name Parameter Name in Identity Provider

IdP Surname Parameter  Surname Parameter Name in Identity Provider

IdP Meta Data

10. Check the **User login token expiration match IdP token expiration** box if you want to force expiration specified by Identity Provider.

Enable ADFS  Specify if IdP is Active Directory Federation Service (ADFS)

User login token expiration match IdP token expiration  If enabled, user authentication token will expire as specified by Identity Provider.