RSA SECURID® ACCESS
Implementation Guide

FileCloud

Gina Salvalzo, 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.

RSA SecurID Access Features	
FileCloud	
On Premise Methods	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
Cloud Authentication Service Methods	
Authenticate App	✓
FIDO Token	✓
SSO	
SAML SSO	✓
HFED SSO	-

Identity Assurance	
Collect Device Assurance and User Behavior	✓

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.

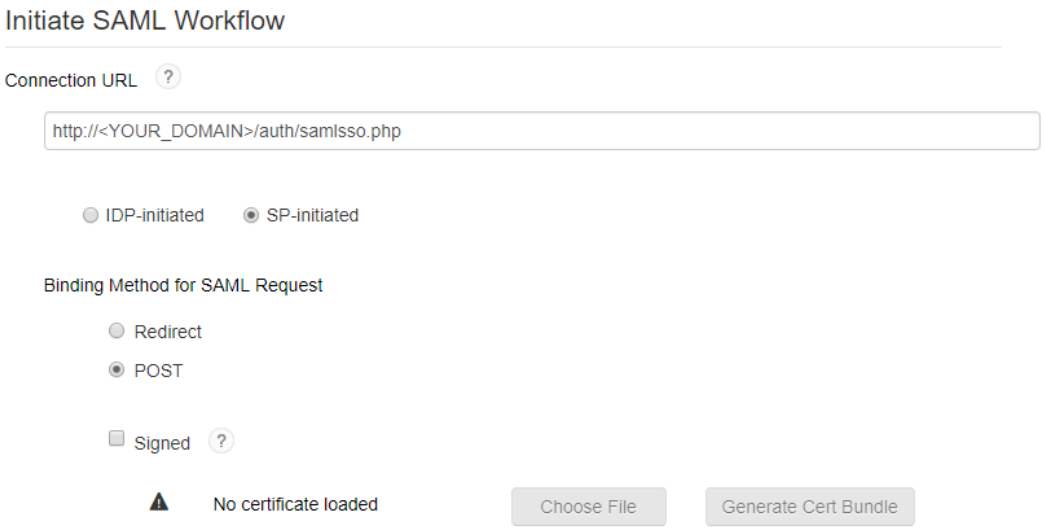
Configure RSA Identity Router SAML IdP

Procedure

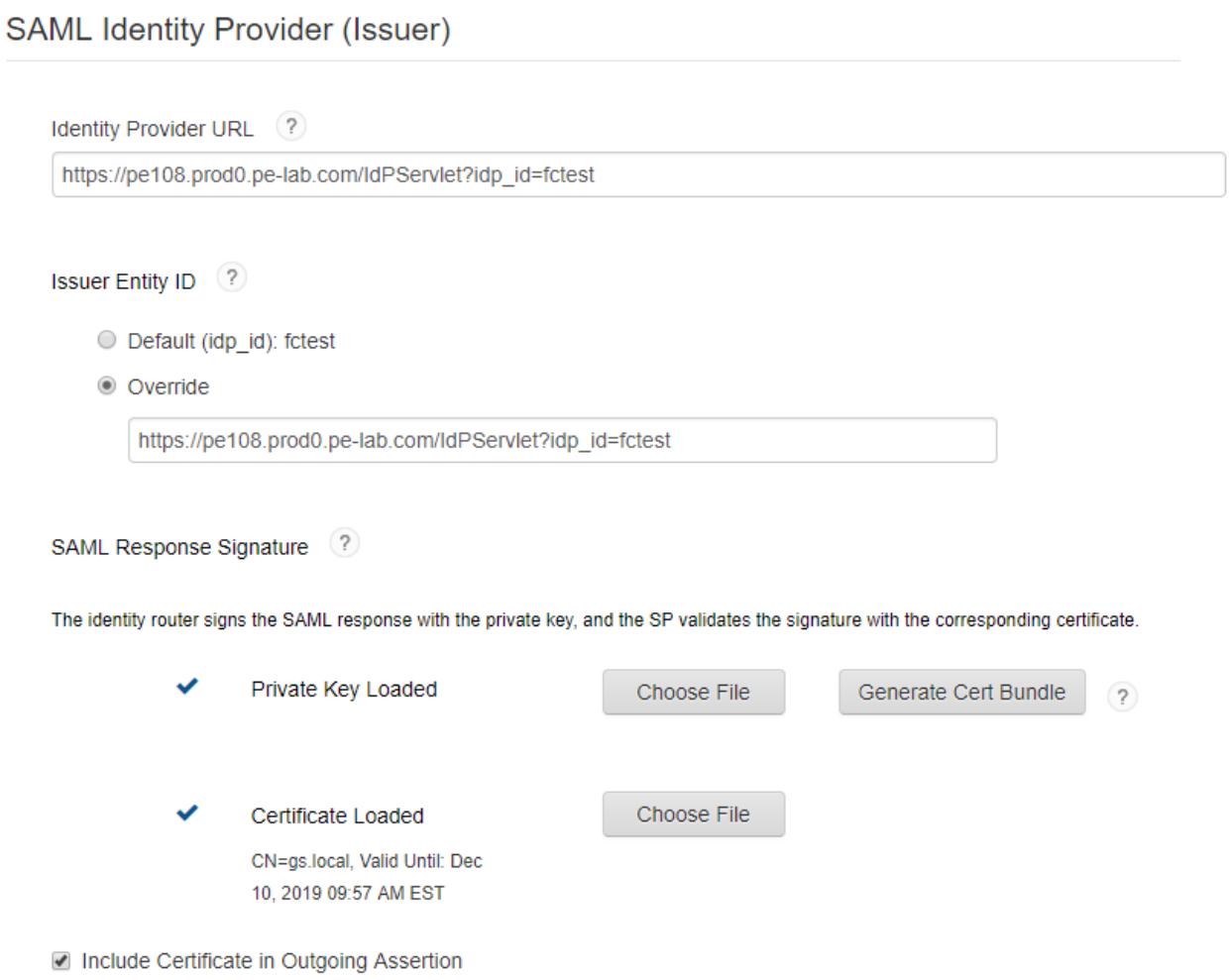
1. Logon to the RSA SecurID Access console and browse **to Applications > Application Catalog**, search for FileCloud and click **+Add** to add the connector.

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/authsamlsso.php**.

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

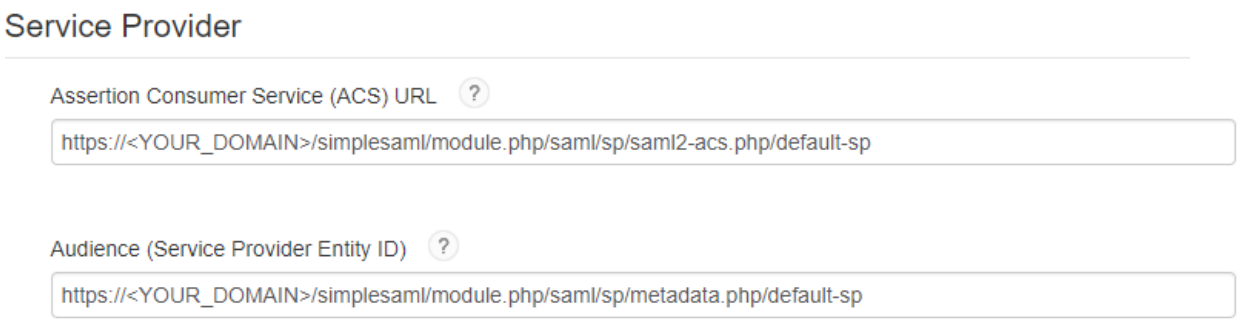


5. Scroll down to SAML Identity Provider (Issuer) section.

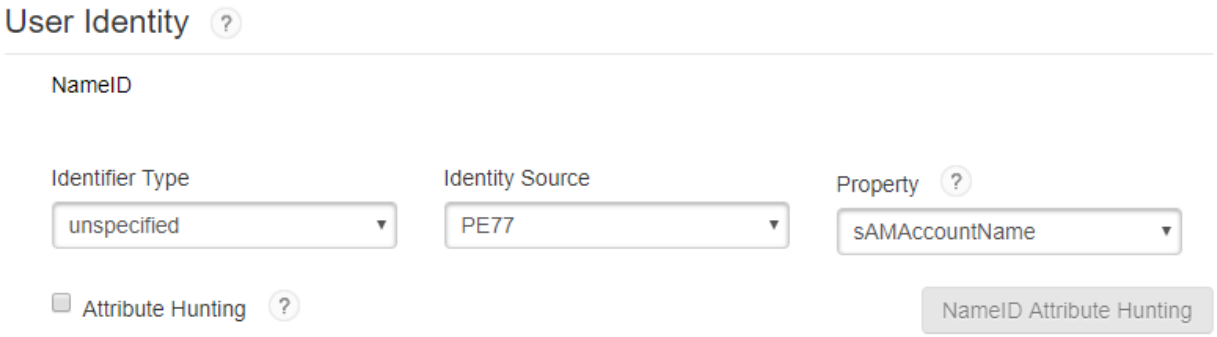


a. Take note of the Identity Provider URL.
b. Click **Override**, under Issuer Entity ID and paste the Identity Provider URL in this field.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

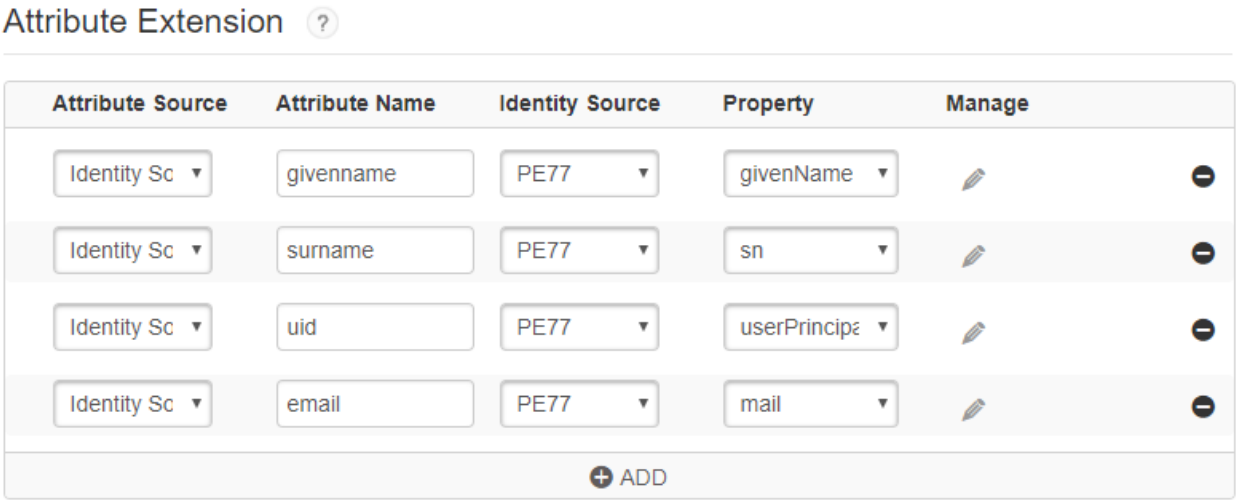
6. Scroll down to the **Service Provider** section.



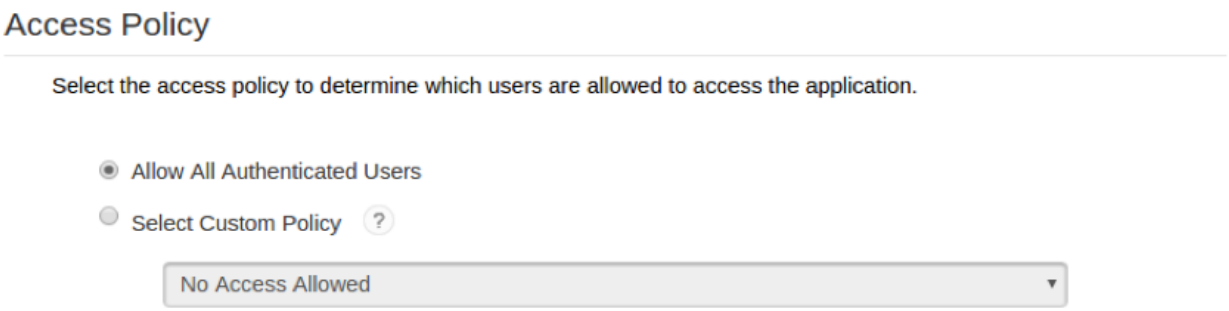
7. In the Assertion Consumer Service (ACS) URL field, replace **<YOUR_DOMAIN>** with your domain; for example **https://pelab.filecloudonline.com/simplesaml/module.php/saml/sp/saml2-sca.php/default-sp**.
8. In the Audience (Service Provider Issuer ID) field, replace **<YOUR_DOMAIN>** with your domain.
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.



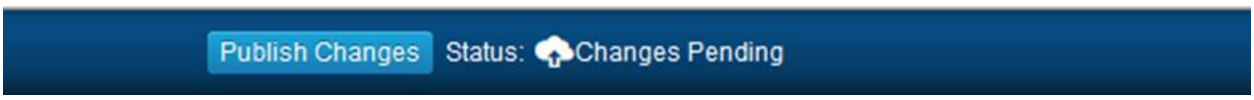
10. Click **Show Advanced Configuration**.
11. Under the Attribute Extension section, enter values for **givenname, surname, uid, email**.



12. Click **Next Step**.
13. On the User Access page, select **Allow All Authenticated Users** user policy from the available options.



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.



18. Navigate to **Applications** > **My Applications**.
19. Locate **FileCloud** in the list and from the **Edit** option, select **Export Metadata**.

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.

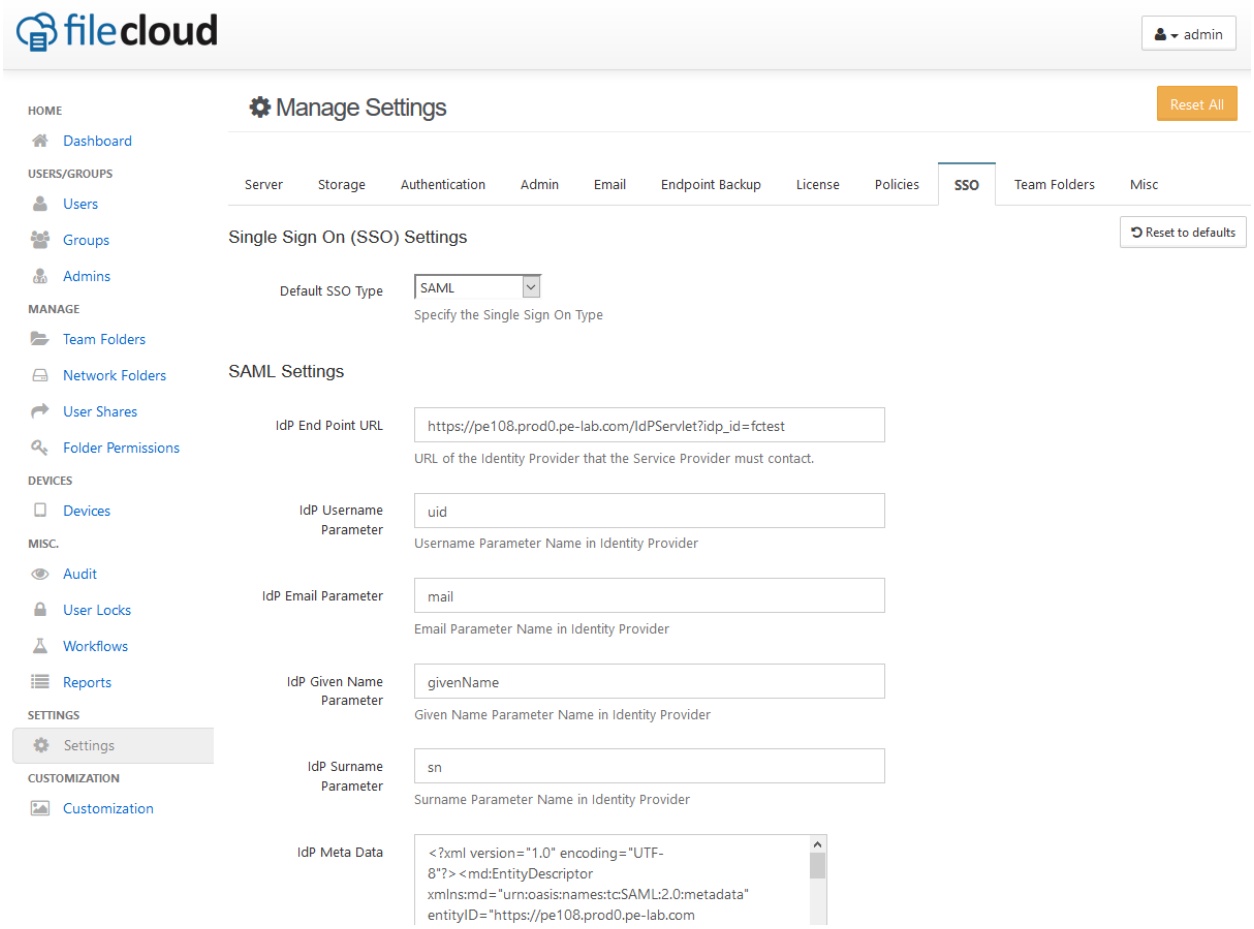
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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.



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