RSA SECURID® ACCESS
Implementation Guide

Fog Creek Software
Manuscript

Gina Salvalzo, RSA Partner Engineering
Last Modified: June 12, 2018

RSA READY

Solution Summary

Fog Creek Software Manuscript is a purpose-built project management tool for software teams. This integration supports single sign-on for both SAML SP initiated and IDP initiated work flows. Manuscript does support user auto-provisioning.

RSA SecurID Access Features	Manuscript
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

The following supported use case of RSA SecurID Access with Manuscript 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 – Manuscript 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
Manuscript 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 Manuscript 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.

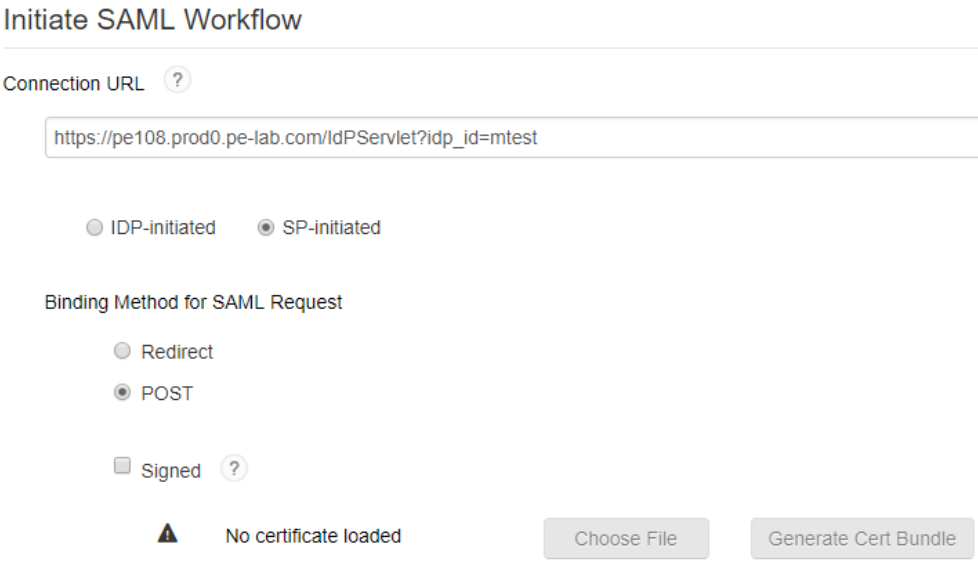
Configure RSA Identity Router SAML IdP

Procedure

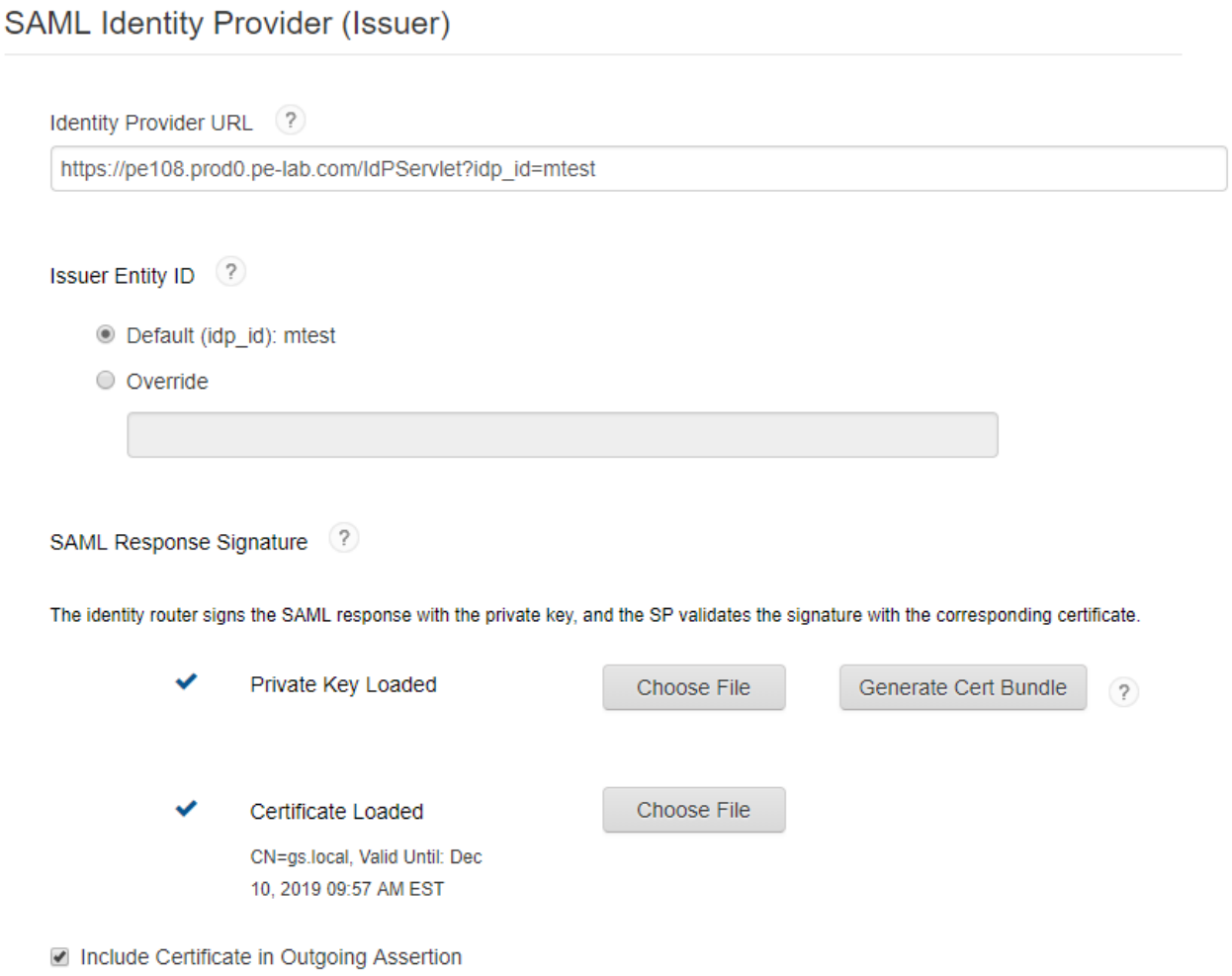
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Manuscript and click **+Add** to add the connector.

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, enter the Identity Provider URL.
    b. Choose **SP-initiated.**
    c. Choose **POST.**

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



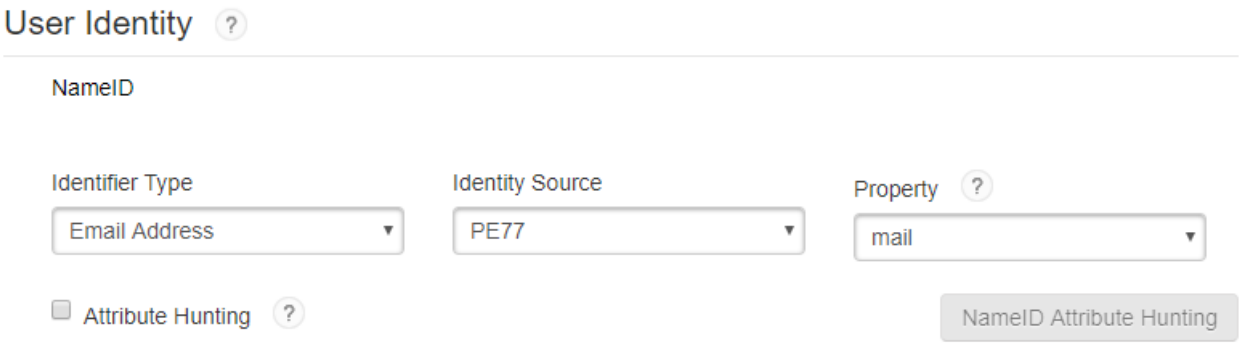
4. Scroll down to SAML Identity Provider (Issuer) section.



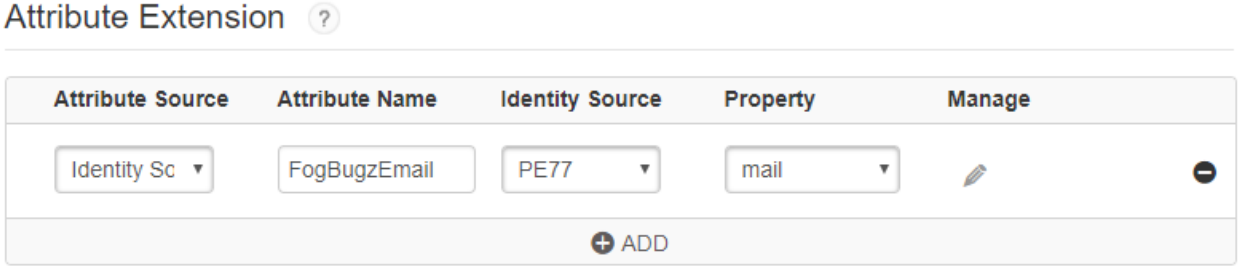
a. Make a note of Identity Provider URL field value, as it will be needed later to configure the service provider configuration.
b. Select **Choose File** and upload the private key.
c. Select **Choose File** to import the public signing certificate.
d. Select the checkbox for **Include Certificate in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

5. Scroll down to the Service Provider section.

6. In the **Assertion Consumer Service (ACS) URL** field, replace <DOMAIN> with your Manuscript site name.
7. In the **Audience (Service Provider Issuer ID)** field, replace <DOMAIN> with your Manuscript site name.
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.

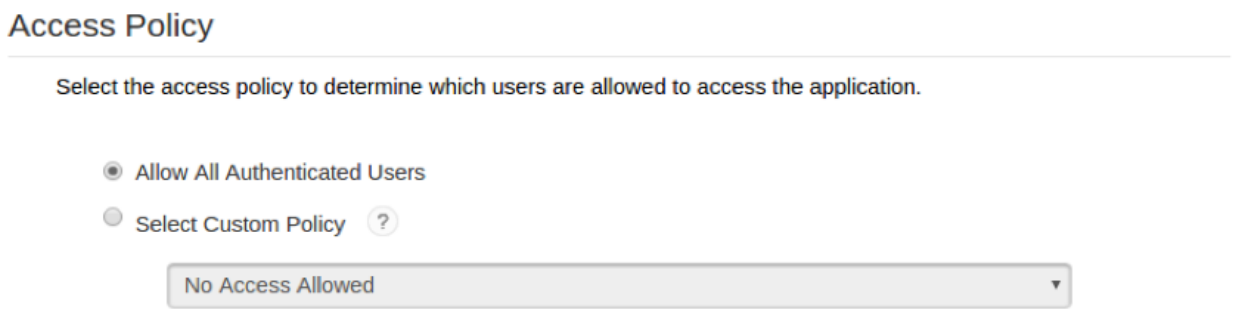


9. Click **Show Advanced Configuration**.
10. Under Attribute Extension, enter attribute name **FogBugzEmail** with the correlating email value from your Identity source.

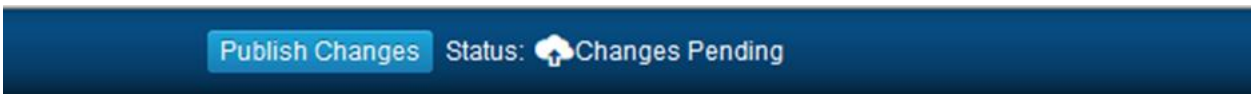


11. Click **Next Step**.

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



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.



Partner Product Configuration

Before You Begin

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

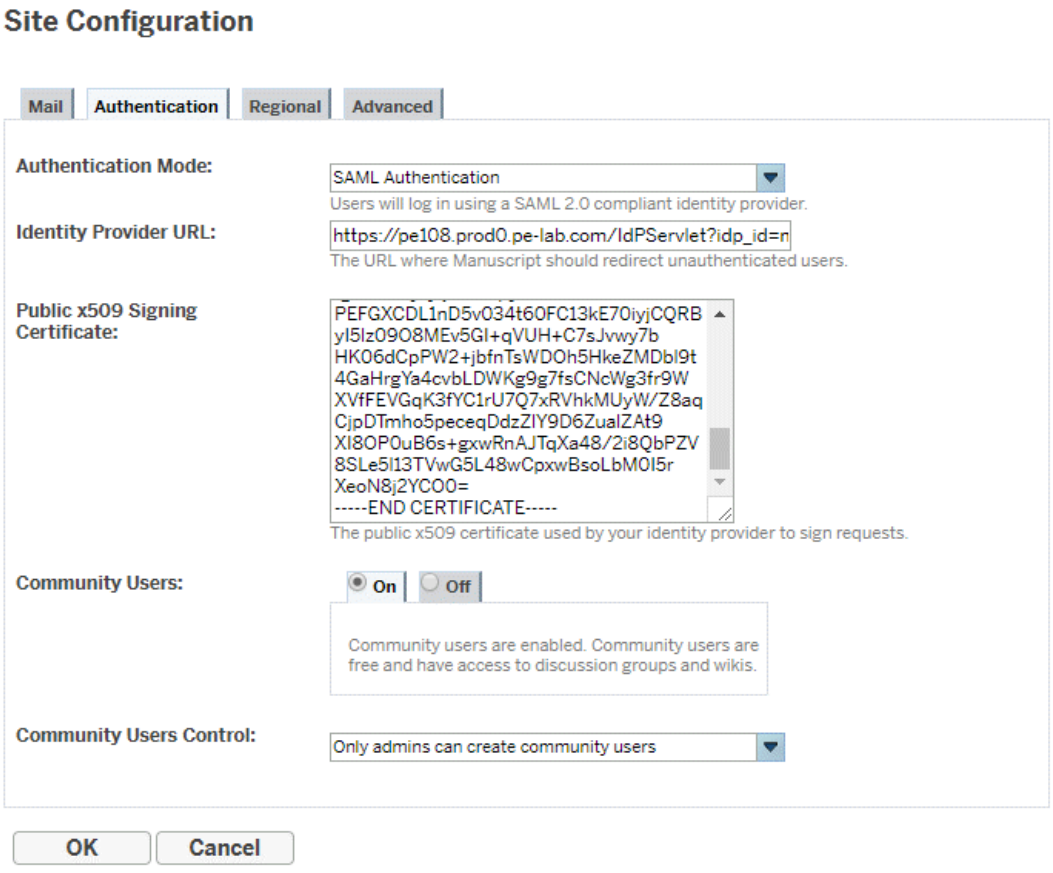
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

Manuscript SAML Configuration

Procedure

1. Login to Manuscript as an administrator.
2. Navigate **Site Configuration > Authentication**.
3. From the Authentication Mode pulldown select either **Username and Password or SAML Authentication** or **SAML Authentication**.



4. Copy and paste the Identity Provider URL from step 4a. on page 5 into the Identity Provider URL field.
5. Paste the public certificate used in step 4c. on page 5 into the X.509 Certificate field.
6. Click **OK**.

Note: User's email address must match user created in Manuscript.