

RSA SECURID[®] ACCESS

Implementation Guide

Fog Creek Software

Manuscript

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



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.**

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): mtest

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://<DOMAIN>.manuscript.com/auth/SAML2/POST

Audience (Service Provider Entity ID) ?

https://<DOMAIN>.manuscript.com/saml-sp

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.

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 **FogBugzEmail** with the correlating email value from your Identity source.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc	FogBugzEmail	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 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**.

Site Configuration

Mail | **Authentication** | **Regional** | **Advanced**

Authentication Mode: SAML Authentication
Users will log in using a SAML 2.0 compliant identity provider.

Identity Provider URL: https://pe108.prod0.pe-lab.com/IdPServlet?idp_id=n
The URL where Manuscript should redirect unauthenticated users.

Public x509 Signing Certificate:
PEFGXCDL1nD5v034t60FC13ke70IyjCQRB
yI5lz09O8MEv5GI+qVUH+C7sJvwy7b
HK06dCpPW2+jbfnTsWDOh5HkeZMDbl9t
4GaHrgYa4cvbLDWKg9g7fsCNcWg3fr9W
XVfFEVGqK3fYC1rU7Q7xRVhkMUyW/Z8aq
CjpDTmho5peceqDdzZlY9D6ZualZAt9
XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV
8SLe5I13TVwG5L48wCpxwBsoLbM0I5r
XeoN8j2YC00=
-----END CERTIFICATE-----
The public x509 certificate used by your identity provider to sign requests.

Community Users: On Off
Community users are enabled. Community users are free and have access to discussion groups and wikis.

Community Users Control: Only admins can create community users

OK Cancel



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.
