RSA SECURID® ACCESS
Implementation Guide

Questetra BPM Suite

Gina Salvalzo, RSA Partner Engineering
Last Modified: March 28, 2018

RSA READY

Solution Summary

Questetra BPM Suite automates various steps like email transmission or PDF generation. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. Questetra BPM Suite does not support user auto-provisioning.

RSA SecurID Access Features Questetra BPM Suite	
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 Questetra BPM Suite 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 – Questetra BPM Suite 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
Questetra BPM Suite SAML Configuration

RSA SecurID Access Server Side Configuration

RSA Cloud Authentication Service Configuration

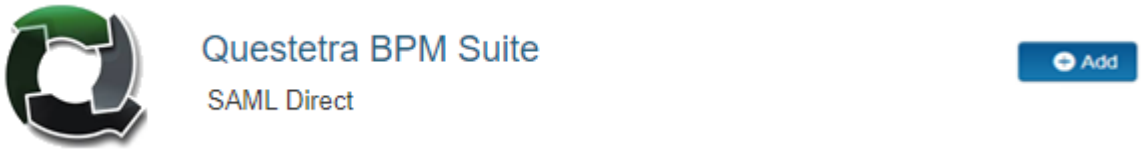
SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Questetra BPM Suite 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

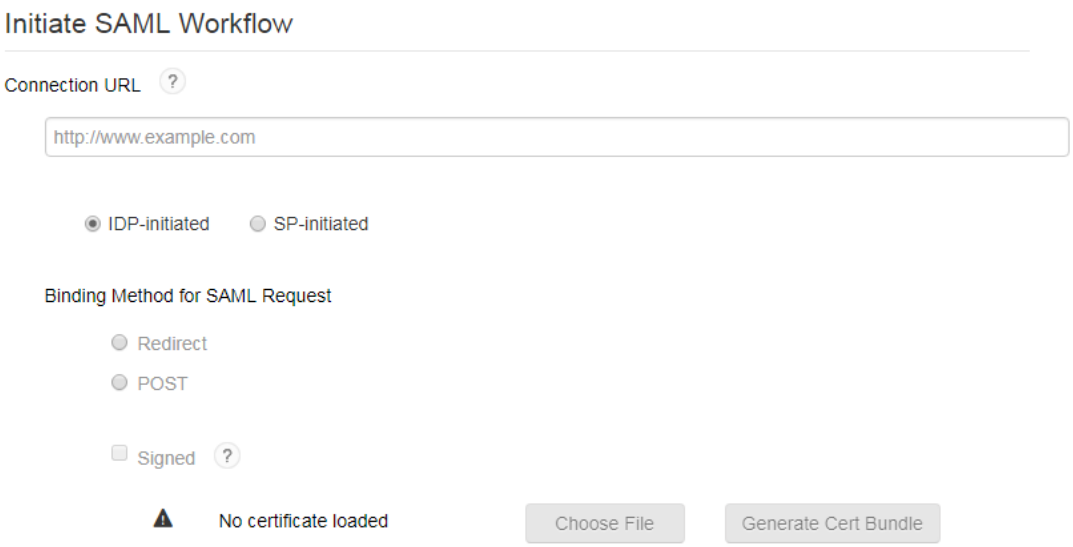
Procedure

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

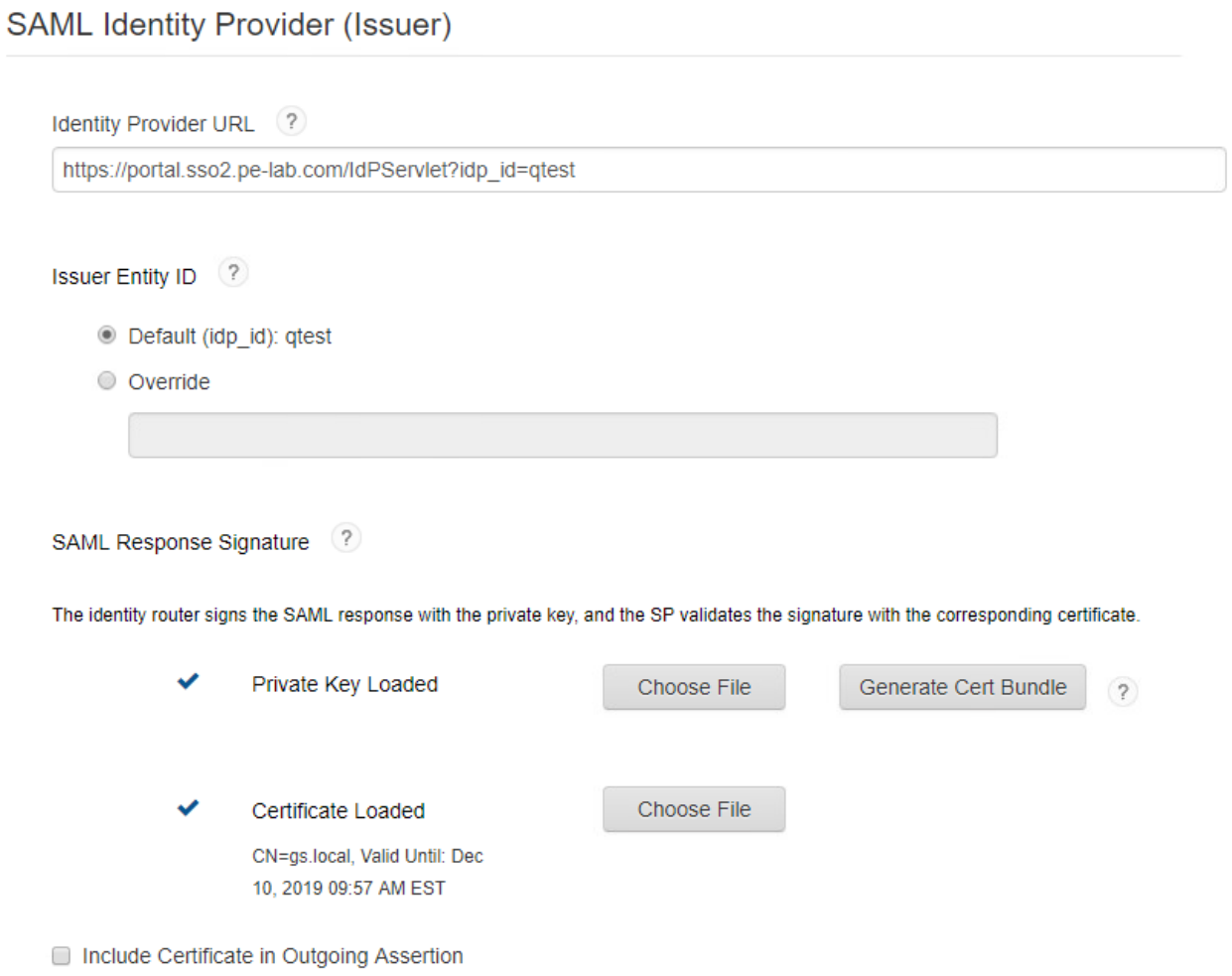


2. Enter a name for the application in the **Name** field on the Basic Information page and click the **Next Step** button.
3. Navigate to Initiate SAML Workflow section.
    a. In the **Connection URL** field, keep the field blank.
    b. Choose **IdP-initiated.**

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

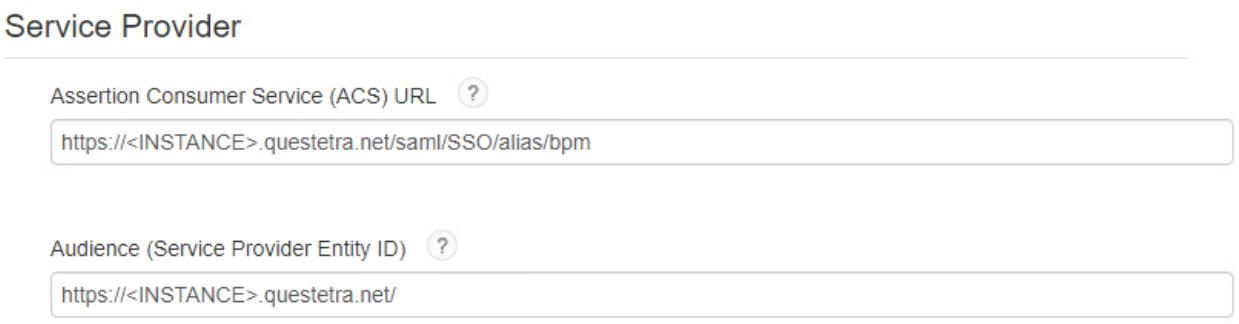


4. Scroll down to SAML Identity Provider (Issuer) section.

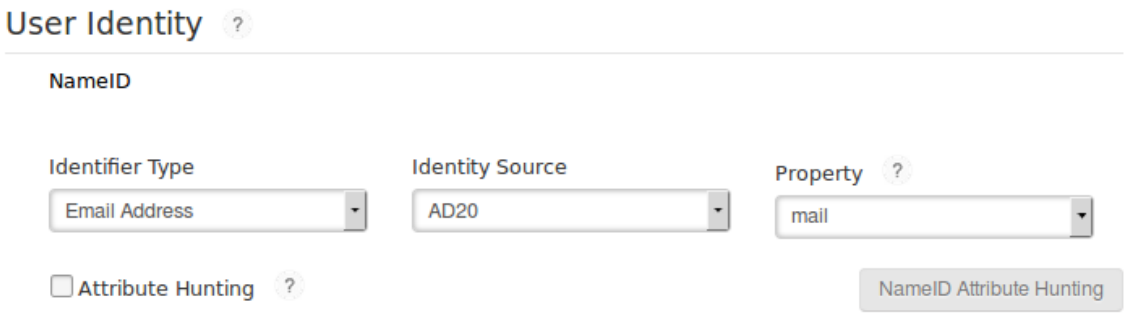


a. Make a note of Identity Provider URL field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Choose File** and upload the private key.
c. Select **Choose File** to import the public signing certificate.
d. Select the checkbox for **Include Certificate in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

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

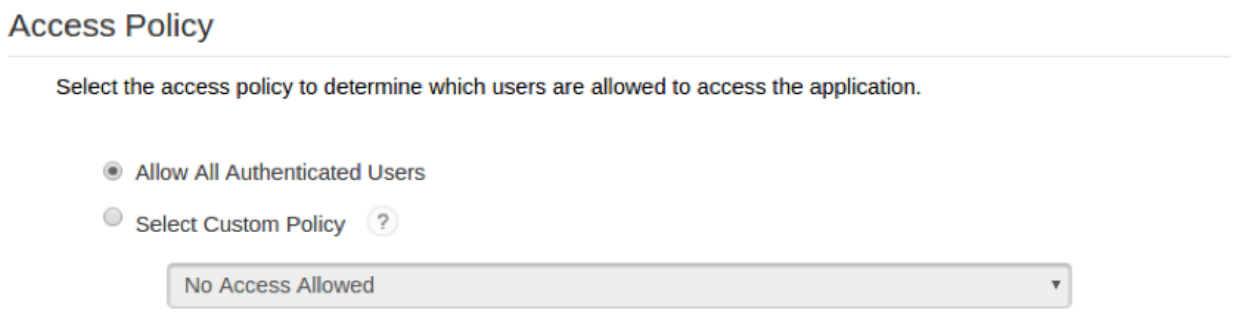


6. In the **Assertion Consumer Service (ACS) URL** field, replace <INSTANCE> with your Questetra BPM Suite stage instance.
7. In the **Audience (Service Provider Issuer ID)** field, i replace <INSTANCe> with your Questetra BPM Suite staged instance.
8. Scroll down to the **User Identity** section. Verify 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.

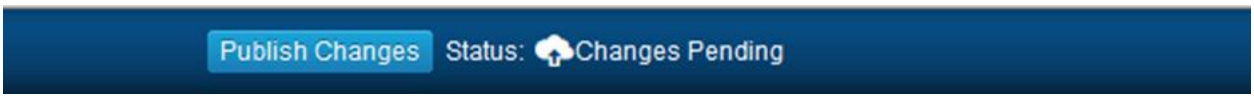


10. Click **Next Step**.

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 Questetra BPM Suite with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

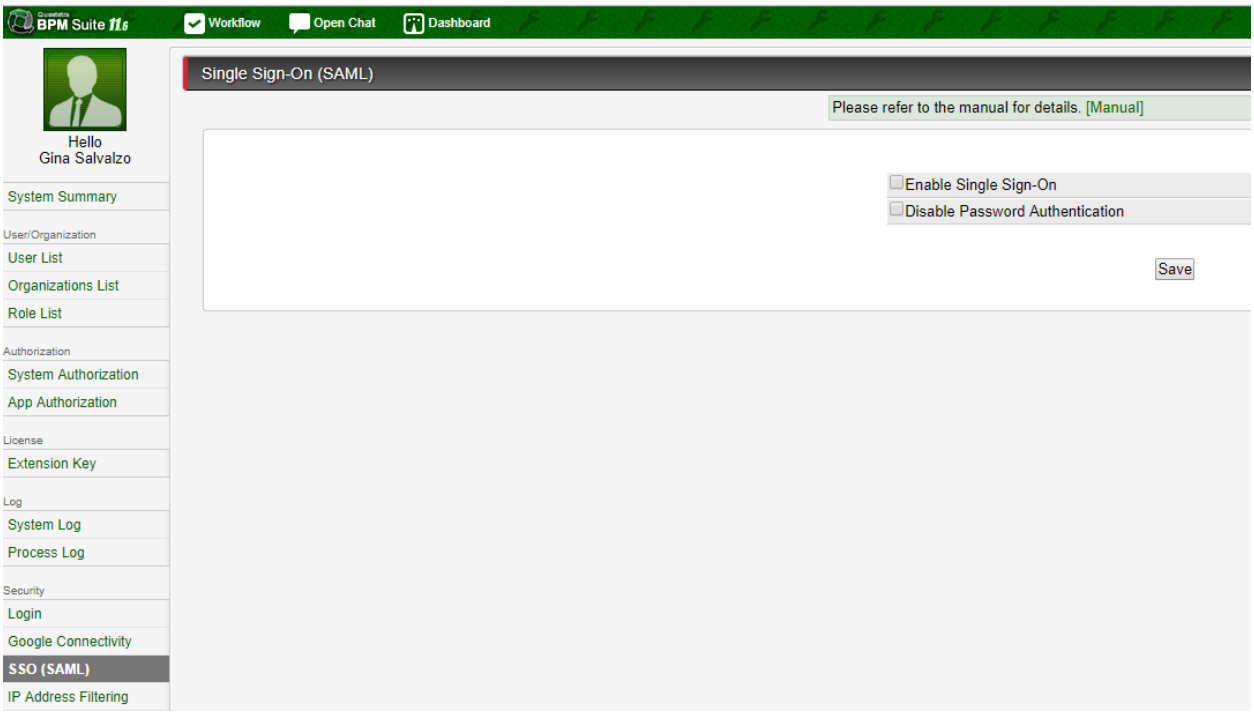
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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

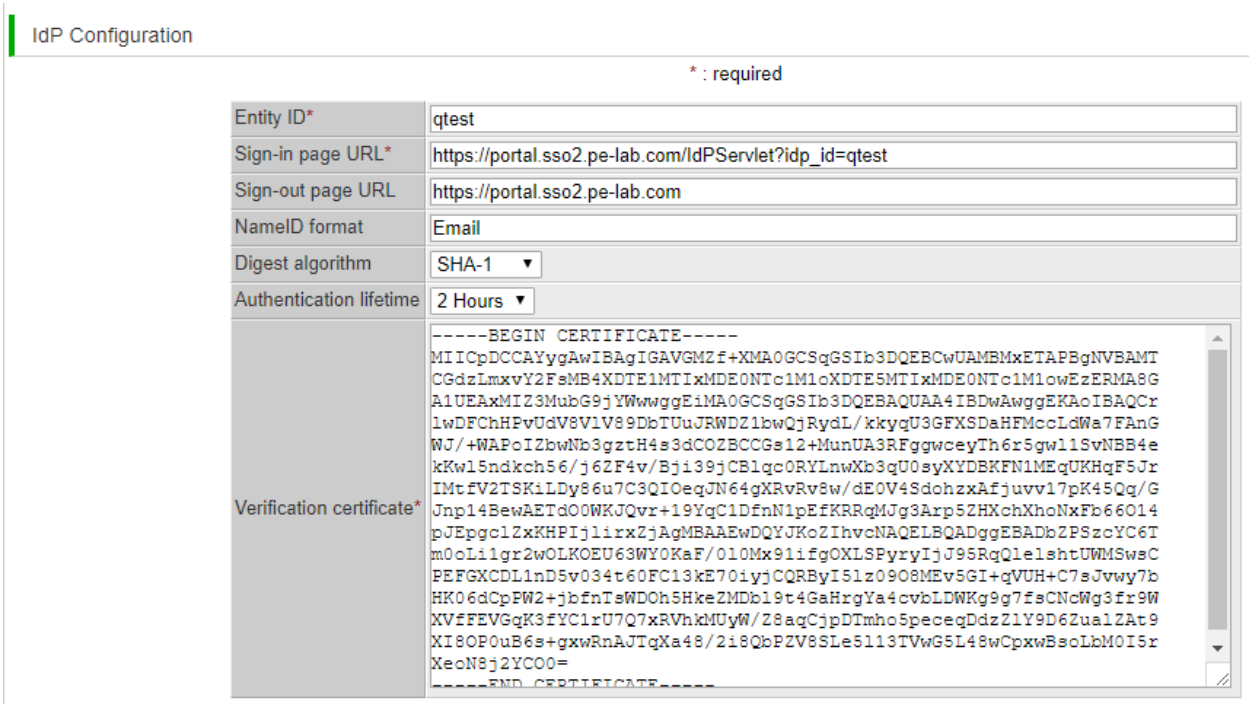
Questetra BPM Suite SAML Configuration

Procedure

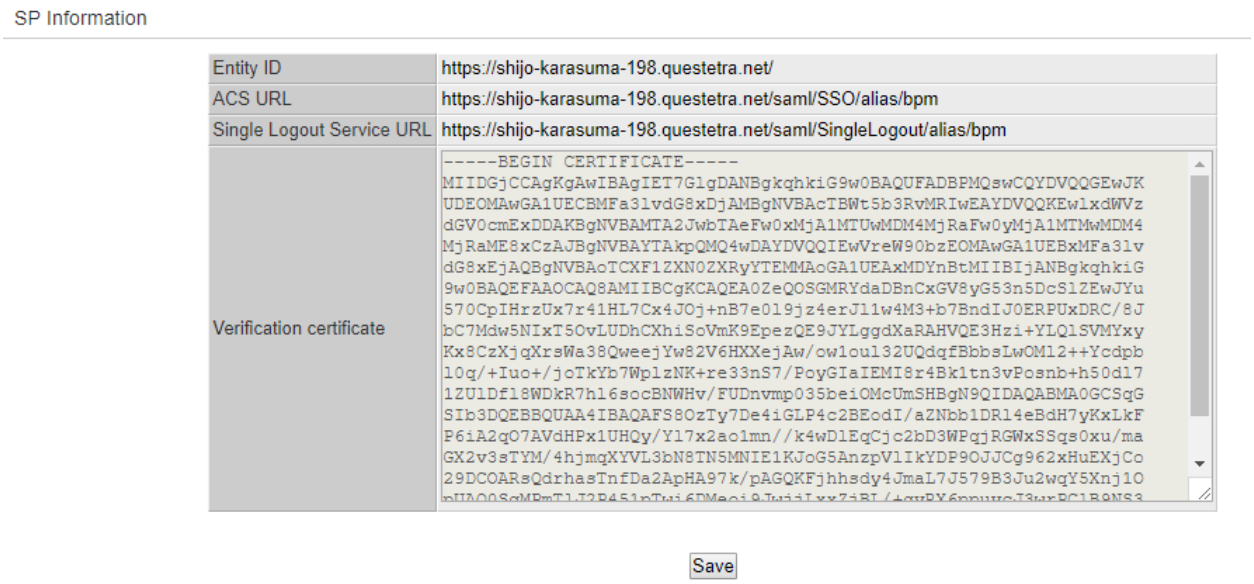
1. Login to Questetra BPM Suite as an administrator.
   https://<instance>.questetra.net/Login_show
2. Under the username select **System Settings > SSO (SAML)**.
3. Check **Enable Single Sign-On** and make sure Disable Password Authentication is unchecked.



4. Enter the **Entity ID** from page 5 step 6.
5. Enter the Identity Provider URL in the **Sign-in page URL** field.
6. Enter **Email** in the NameID format field.
7. Paste the public certificate into the **Verification certificate** field.



8. Take note of the Entity ID and ACS URL in the SP Information section. This will be needed to configure the IdP in steps 5 and 6 on page 6.



9. Click **Save**.
10. For SP initiated login, go to **https://<intance>.questetra.net/saml/SSO/alias/bpm**.