

RSA SECURID[®] ACCESS

Implementation Guide

Questetra BPM Suite

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



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

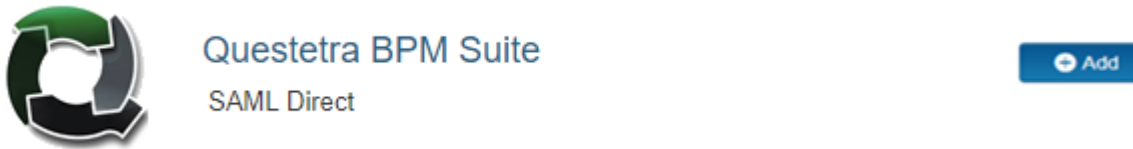
SAML via RSA Identity Router (IdP)

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.

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): qtest

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://<INSTANCE>.questetra.net/saml/SSO/alias/bpm

Audience (Service Provider Entity ID) ?

https://<INSTANCE>.questetra.net/

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.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

10. 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 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.

The screenshot shows the Questetra BPM Suite 11.6 interface. The top navigation bar includes 'Workflow', 'Open Chat', and 'Dashboard'. The left sidebar shows a user profile for 'Gina Salvalzo' and a menu with categories like 'System Summary', 'User/Organization', 'Authorization', 'License', 'Log', 'Security', and 'Google Connectivity'. The 'SSO (SAML)' option is selected. The main content area is titled 'Single Sign-On (SAML)' and contains a message: 'Please refer to the manual for details. [Manual]'. Below this, there are two checkboxes: 'Enable Single Sign-On' (checked) and 'Disable Password Authentication' (unchecked). A 'Save' button is located at the bottom right of the configuration area.



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.

IdP Configuration

* : required

Entity ID*	qtest
Sign-in page URL*	https://portal.sso2.pe-lab.com/IdPServlet?idp_id=qtest
Sign-out page URL	https://portal.sso2.pe-lab.com
NameID format	Email
Digest algorithm	SHA-1
Authentication lifetime	2 Hours
Verification certificate*	<pre> -----BEGIN CERTIFICATE----- MIICpDCCAYygAwIBAgIGAVGMZf+XMA0GCSqGSIb3DQEBCwUAMBxETAPBgNVBAMT CGdzLmxvY2FzMB4XDTE1MTIxMDE0NTc1M1oXDTE1MTIxMDE0NTc1M1owEzERMA8G A1UEAxMIZ3MubG9jYWwvYyEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCx lwDFChHPvUdV8V1V89DbTUuJRWDZ1bwQjRydL/kkyqU3GFXSdaHFMccLdWa7FAnG WJ/+WAPoIZbwNb3gztH4s3dCOZBCCGs12+MunUA3RFggwceyTh6r5gw11SvNBB4e kKw15ndkch56/j6ZF4v/Bji39jCB1qcORYLlwXb3qU0syXYDBKFN1MEqUKHqF5Jr IMtFV2TSKiLDy86u7C3QIOeqJN64gXRvRv8w/dE0V4SdohzxAfjuvv17pK45Qq/G Jnp14BewAETd00WKJQvr+19YqC1DfnN1pEfKRRqMJg3Arp5ZHXchXhoNxFb66014 pJEpgcl2xKHPIj1lrX2jAgMBAAEwDQYJKoZIhvcNAQELBQADggEBADb2PSzcYC6T m0oLi1gr2wOLKOEu63WY0KaF/010Mx91ifgOXLSPyryIjJ95RqQ1e1shtUWMSweC PEFGXCDL1nD5v034t60FC13kE70iyjCQRByI51z0908MEv5GI+gVUH+C7sJvwy7b HK06dCpFW2+jbfnTswDOh5HkeZMDb19t4GaHrgYa4cvbLDWKg9g7fsCNcWg3fr9W XVfFEVGqK3fYC1rU7Q7xRVhkMUyW/Z8aqCjpdTmho5peceqDdzZ1Y9D6ZualZAt9 XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV8SL5113TVwG5L48wCpxwBsoLbM0I5r XeoN8j2YCO0= -----END CERTIFICATE----- </pre>



- 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.

SP Information

Entity ID	https://shijo-karasuma-198.questetra.net/
ACS URL	https://shijo-karasuma-198.questetra.net/saml/SSO/alias/bpm
Single Logout Service URL	https://shijo-karasuma-198.questetra.net/saml/SingleLogout/alias/bpm
Verification certificate	<pre> -----BEGIN CERTIFICATE----- MIIDGjCCAgKgAwIBAgIET7G1gDANBgkqhkiG9w0BAQUFADBPMQswCQYDVQQGEwJK UDEOMAwGA1UECBMFA3lvdG8xDjAMBgNVBAcTBWt5b3RvMRIwEAYDVQQKEw1xdWVz dGV0cmExDDAKBgNVBAMTA2JwbTAeFw0xMjA1MTUwMDM4MjRaFw0yMjA1MTMwMDM4 MjRaME8xCzAJBgNVBAYTAkpQMQ4wDAYDVQQIEwVreW90bzEOMAwGA1UEBxMFa3lvdG8x EjAQBgNVBAoTCXFlZXRyYTEMMAoGA1UEAxMDYnBtMIIBIjANBgkqhkiG 9w0BAQEFAAOCAQ8AMIIBCgKCAQEAOZeQOSGMRYdaDBnCxGV8yG53n5DcS1ZEwJYu 570CpIHrzUx7r41HL7Cx4JOj+nB7e019jz4erJ11w4M3+b7BndIJOERPuxDRC/8J bC7Mdw5NIxT5OvLUDhCXhiSoVmK9EpezQE9JYlggdXaRAHVQE3Hz+iYLQ1SVMYxy Kx8CzXjqXrsWa38QweejYw82V6HXXejAw/cw1oul32UQdqfBbbsLwOM12++Ycddb 10q/+Iuo+/jotkYb7Wp1zNK+re33nS7/PoyGIaIEMI8r4Bk1tn3vPosnb+h50dl7 1ZULdf18WDkR7h16socBNWHV/FUDnvmP035beiOMcUmSHBqN9QIDAQABMA0GCSqG SIb3DQEBBQUAA4IBAQAfS8OzTy7De4iGLP4c2BEodI/aZNbb1DR14eBdh7yKxLkF P6iA2qO7AVdHPx1UHQy/Y17x2aolmn//k4wD1EqCjc2bD3WPqjRGWxSSqs0xu/ma GX2v3eTYM/4hjmQXYVL3bN8TNSMNI1KJoG5AnzpV1IkYDP90JJCg962xHuEXjCo 29DCOARsQdrhasTnfDa2ApHA97k/pAGQKFjhhsdy4JmaL7J579B3Ju2wqY5Xnj1O wUHQ00sMPEtL12P451xTui6DMaci9Tui3LxxZ3BL/4grBY6ppuywT3uxPC1R9MS3 </pre>

Save

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