

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

**Honey**

Gina Salvazo, RSA Partner Engineering  
Last Modified: May 4, 2018



## Solution Summary

---

Honey is an intuitive social intranet for your company. Built to connect global teams, share resources, simplify team conversations, and support employee workflows. This integration supports single sign on for both SAML SP initiated and IDP initiated work flows. Honey supports user auto-provisioning.

RSA SecurID Access Features	
Honey	
<b>On Premise Methods</b>	
RSA SecurID	✓
On Demand Authentication	✓
Risk-Based Authentication (AM)	-
<b>Cloud Authentication Service Methods</b>	
Authenticate App	✓
FIDO Token	✓
<b>SSO</b>	
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 Honey 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** – Honey 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](#)  
[Honey 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 Honey 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 Honey 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

Choose File

Generate Cert Bundle



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

## SAML Identity Provider (Issuer)

---

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): htest

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 Issuer Entity ID **Override** and paste the Identity Provider URL in that 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**.



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

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://honey.is/org/<COMPANY\_ID>/saml/finalize

Audience (Service Provider Entity ID) ?

https://honey.is/org/<COMPANY\_ID>

6. In the **Assertion Consumer Service (ACS) URL** field, replace <COMPANY\_ID> with your Honey organization ID.
7. In the **Audience (Service Provider Issuer ID)** field, replace <COMPANY\_ID> with your Honey organization ID.
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 **Show Advanced Configuration**.



- In the Attribute Extension section, choose the correct property variables for FirstName, LastName, Department, JobTitle, Location and PhoneNumber.

Attribute Extension ?

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity Sc ▾	FirstName	PE77 ▾	givenName ▾	
Identity Sc ▾	LastName	PE77 ▾	sn ▾	
Identity Sc ▾	Department	PE77 ▾	department ▾	
Identity Sc ▾	JobTitle	PE77 ▾	title ▾	
Identity Sc ▾	Location	PE77 ▾	postalAddre ▾	
Identity Sc ▾	PhoneNumber	PE77 ▾	primaryTele: ▾	

+ ADD

- Verify that **Assertion within response** is selected under Uncommon Formatting.

### Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

- Entire SAML response
  Assertion within response

Signature Algorithm rsa-sha1 ▾

Digest Algorithm sha1 ▾

Encrypt Assertion ?

No certificate loaded

Choose File



14. Click **Next Step**.
15. 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 ▼

16. Click **Next Step**.
17. On the **Portal Display** page, select **Display in Portal**.
18. Click **Save and Finish**.
19. 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 Honey 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 Honey components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### **Honey SAML Configuration**

#### **Procedure**

1. Login to Honey as an administrator. **<https://honey.is/signin>**
2. Navigate to **Admin > SINGLE SIGN-ON**.
3. The ACS URL and Entity ID will be displayed. These will be needed to configure step 6 and 7 on page 6.

#### **Honey SAML Service Provider Details**

##### METADATA URL

<https://honey.is/org/45763/saml/metadata>

##### ASSERTION CONSUMER URL

<https://honey.is/org/45763/saml/finalize>

##### CONSUMER BINDING

urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST

##### NAME ID FORMAT

urn:oasis:names:tc:SAML:1.1:nameid-format:email ▾

##### ATTRIBUTES

FirstName, LastName, JobTitle, Department, Location, PhoneNumber

##### ENTITY ID

<https://honey.is/org/45763>



- 4. Enter the Identity Provider URL from page 5 step 4 into the REMOTE LOGIN URL field.
- 5. Paste the public certificate from page 5 step 4d into the IDENTITY PROVIDER VERTIFICATE window.

**Your SAML Identity Provider Configuration**  
Configure the following details provided by your identity provider.

**REMOTE LOGIN URL**

https://portal.sso2.pe-lab.com/IdPServlet?=hstest

**REMOTE LOGOUT URL (OPTIONAL)**

https://portal.sso2.pe-lab.com/LogoutServlet

**ISSUER URL (OPTIONAL)**

What's your identity provider's issuer URL?

**IDENTITY PROVIDER CERTIFICATE**

```
Jnp14BewAETd00WKJQvr+19YqC1DfnN1pEfKRRqMJg3Arp5ZHXchXhoNx Fb66014
pJEpgclZxKHPIj1irx2jAgMBAAEwDQYJKoZIhvcNAQELBQADggEBADbZPSzcYC6T
m0oLi1gr2wOLKOEU63WY0KaF/010Mx91ifgOXLSPyryIjJ95RqQlelshUWMSwsC
PEFGXCDL1nD5v034t60FC13kE70iyjCQRByI51z0908MEv5GI+qVUH+C7sJvwy7b
HK06dCpFW2+jbfnTsWDOh5HkeZMDb19t4GaHrgYa4cvbLDWKg9g7fsCNcWg3fr9W
XVfFEVGqK3fYC1rU7Q7xRVhkMUyW/Z8aqCjpDTmho5peceqDdzZ1Y9D6Zua1ZAt9
XI8OP0uB6s+gxwRnAJTqXa48/2i8QbPZV8SLe5113TVwGSL48wCpxwBsoLbMOI5r
XeoN8j2YC00=
-----END CERTIFICATE-----
```

**Enable Single Sign-On?**

Single Sign-On should only be enabled after you have configured all the options above.

**SAVE SETTINGS**

- 6. Toggle **Enable Single Sign-on**.
- 7. Click **SAVE SETTINGS**.

