

# **RSA SECURID<sup>®</sup> ACCESS**

## **Implementation Guide**

### **Deputy**

Gina Salvazo, RSA Partner Engineering  
Last Modified: September 5, 2017

## Solution Summary

Deputy is an online HR and employee management system for easy employee scheduling, time, attendance and communication. Deputy delivers a single sign on experience to the user through SAML. This integration supports both IdP initiated and SP initiated authentication flow.

RSA SecurID Access Features	
Deputy	
<b>On Premise Methods</b>	
RSA SecurID	<input checked="" type="checkbox"/>
On Demand Authentication	<input checked="" type="checkbox"/>
Risk-Based Authentication (AM)	<input type="checkbox"/>
<b>Cloud Authentication Service Methods</b>	
Authenticate App	<input checked="" type="checkbox"/>
FIDO Token	<input checked="" type="checkbox"/>
<b>SSO</b>	
SAML SSO	<input checked="" type="checkbox"/>
HFED SSO	<input type="checkbox"/>

Identity Assurance	
Collect Device Assurance and User Behavior	<input checked="" type="checkbox"/>

## Configuration Summary

---

All of the supported use cases of RSA SecurID Access with Deputy 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** – Deputy 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 Deputy SAML Configuration](#)

## RSA SecurID Access Server Side Configuration

### *RSA Cloud Authentication Service Configuration*

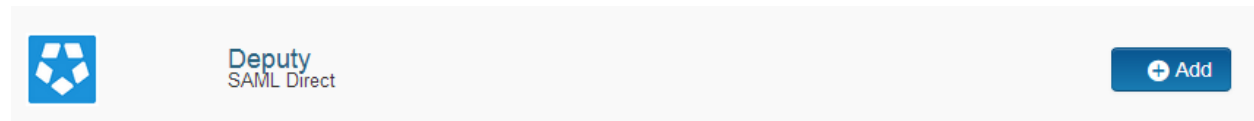
#### SAML via RSA Identity Router (IdP)

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for Deputy 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 Deputy 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 as the value is not required.
  - b. Choose **IDP-initiated**.

 **Note: The following IdP-initiated configuration works for SP-initiated connections 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 ?

https://portal.sso5.pe-lab.com/IdPServlet?idp\_id=1dvkt2gfqe2mv

Issuer Entity ID ?

Default (idp\_id): 1dvkt2gfqe2mv

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

Choose File

Generate Cert Bundle

?

✓ Certificate Loaded

Choose File

CN=gslab.com, Valid Until:  
05/03/2021

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 **Default (idp\_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
- 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**.

# Deputy

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

## Service Provider

Assertion Consumer Service (ACS) URL ?

https://[your-subdomain].[location-code].deputy.com/exec/devapp/samlacs

Audience (Service Provider Entity ID) ?

https://[your-subdomain].[location-code].deputy.com

6. In the **Assertion Consumer Service (ACS) URL** field, provide the value as per received with service provider metadata. Replace [your-subdomain] and [location-code] with your service provider account specific subdomain and location code.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received with service provider metadata. Replace [your-subdomain] and [location-code] with your service provider account specific subdomain and location code.
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

unspecified

Identity Source

AD20

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

9. Click **Next Step**.


# Deputy


10. 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 

11. Click **Next Step**.
12. On the Portal Display page, select **Display in Portal**.
13. Click **Save and Finish**.
14. 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 the Deputy 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 Deputy components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

### Deputy SAML Configuration

#### Procedure

1. Login to your Deputy account.  
[https://\[your-subdomain\].\[location-code\].deputy.com/login](https://[your-subdomain].[location-code].deputy.com/login)
2. Navigate to [https://\[your-subdomain\].\[location-code\].deputy.com/exec/config/system\\_config](https://[your-subdomain].[location-code].deputy.com/exec/config/system_config) then following UI will be displayed.

Workplace/Pay Centre Default Configuration ▾

**Portfolio Settings** Edit  
Portfolio Name

**Language and Locale Settings** Edit  
Regional Settings, Date & Time Format

**Communication Settings** Edit  
Email Configuration, IT support number

**Application Settings** Edit  
Rostering, Time Sheet, Availability, Payroll

**Security Settings** Edit  
Security & Privacy Settings, Password Rules, Session Information

**Advanced Settings** Edit  
SOAP Keys, API Information

**System Config**  
The options chosen here are the defaults for your Deputy installation.  
**Important Information**  
Please be careful as many of these settings affect multiple applications.



3. Click *Edit* button for *Security Settings* then following UI will be displayed.

### Security Settings

**Security Configuration**

Session timeout in minutes  
Period of user inactivity in minutes after which their session times out. Use 0 (zero) for no timeout.

1440

Enable Social Login  
Enable this permission to allow users to log in with Social Network connectors (E.g. Facebook, Google, Twitter, LinkedIn).

ON

OpenSSL Certificate  
SAML SSO Certificate. Generate a self-signing request using pkcs12 and keep your private key secure. Paste the content of certificate here

MIIcPjCCAY6gAwlBAglGAVvNoqX9MA0GC-SqGS1b3DQEBCwUAMBQxEjAQBgNVBAMT CWdzbGFILmNvbTAeFw0xNzA1MDM-wOTI3MjBaFw0yMTA1MDMwOTI3MjBaMBQxEjAQ BgNVBAMTCWdzbGFILmNvbTCCASlWdQYJKoZlhc-NAQEBBQADggEPADCCAQoCggEB AJefJItkysUTDqcnQVt/fqmOsf/qthJlhX2vf-PzRSYB+QGw5Dav2jddQpd4CimcL

Deputy Token to create user on the fly  
If you want SAML insertion to automatically create a user if they do not exist in Deputy, enter the Deputy access token here which will be used to create the user. Get the access token by creating a client [here](#) and get a token

Saml SSO URL  
SAML SSO URL

https://portal.sso5.pe-lab.com/IdPServlet?idp\_id=!

[Save Settings](#)

### System Config

The options chosen here are the defaults for your Deputy installation.

**Important Information**

Please be careful as many of these settings affect multiple applications.

- a) **Session timeout in minutes:** Enter session timeout in minutes.
- b) **Enable Social Login:** Enable this parameter.
- c) **OpenSSL certificate:** Paste content of [public signing](#) certificate used in IdP.
- d) **Deputy Token to create user on the fly:** This is an optional field. This token is used while creating users automatically if log in via SSO is attempted.
- e) **SAML SSO URL:** Enter the Identity Provider URL which can be found in step -4 on page 5. It is of following format : **https://<Your\_Portal\_URL>?idp\_id=<Unique\_IdP\_ID>**
- f) Click on **Save Settings** button to complete the configurations. You may need to log out once to save the settings.

4. Your Deputy account is now enabled for SAML SSO authentication.