




# **RSA SECURID<sup>®</sup> ACCESS** **Implementation Guide**

**HelpScout**

Gina Salvazo, RSA Partner Engineering  
Last Modified: November 7, 2017



## Solution Summary

---

Help Scout is a help desk software company headquartered in Boston, Massachusetts. The company provides an email-based customer support platform, knowledge base tool, and an embeddable search/contact widget for customer service professionals.

RSA SecurID Access Features	
HelpScout	
<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 HelpScout 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** – HelpScout 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 HelpScout SAML Configuration](#)

## RSA SecurID Access Server Side Configuration

### *RSA Cloud Authentication Service Configuration*

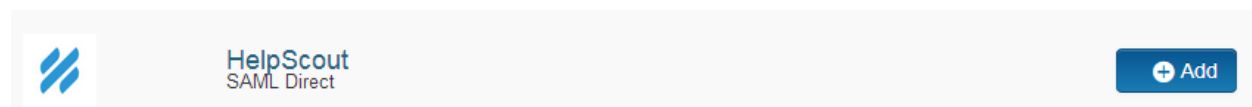
#### **SAML via RSA Identity Router (IdP)**

To configure a SAML Service Provider in RSA Identity Router, you must deploy the connector for HelpScout 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 HelpScout 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 and choose **IDP-initiated**.

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

#### Initiate SAML Workflow

Connection URL 


IDP-initiated  SP-initiated

Binding Method for SAML Request

Redirect

POST

Signed 

 No certificate loaded

# HelpScout

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

## SAML Identity Provider (Issuer)

Identity Provider URL ?

Issuer Entity ID ?

Default (idp\_id): 16wti8gc1x39h

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

?

cert.pem

Certificate valid until: Mon  
Aug 16 06:45:13 UTC 2021

Include Certificate in Outgoing Assertion

- a. Take note of the Identity Provider URL.
- b. Take note of the Issuer Entity ID.
- 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**.

# HelpScout

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

## Service Provider

Assertion Consumer Service (ACS) URL [?](#)

https://helpscout.auth0.com/login/callback?connection=<Company>-<CompanyID>-sso-saml

Audience (Service Provider Entity ID) [?](#)

urn:auth0:helpscout:<Company>-<CompanyID>-sso-saml

6. In the Assertion Consumer Service (ACS) URL field, replace **<Company>** with your company and **<CompanyID>** with your CompanyID.
7. In the Audience (Service Provider Issuer ID) field, replace **<Company>** with your company and **<CompanyID>** with your CompanyID.
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

9. Click the **Show Advance** button.
10. Under the Attribute Extension section, enter the attribute **Email** and the mapped Active Directory attribute for this value.

## Attribute Extension [?](#)

Attribute Source	Attribute Name	Identity Source	Property	Manage
Identity So	Email	AD20	mail	 
<a href="#">+</a> ADD				

11. Click **Next Step**.

# HelpScout

- 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 ▼

- Click **Next Step**.
- On the Portal Display page, select **Display in Portal**.
- Click **Save and Finish**.
- Click **Publish Changes**. Your application is now enabled for SSO.

**Publish Changes**

Status:  Changes Pending

- Navigate to **Applications > My Applications**.
- Locate **HelpScout** in the list and from the **Edit** option, select **Export Metadata**.




HelpScout

Created From: HelpScout-SAML2-Direct  
SAML Direct

Edit ▼

 Edit

 Export Metadata

 Delete

# HelpScout

## ***Before You Begin***

This section provides instructions for configuring HelpScout 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 HelpScout components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

## **HelpScout SAML Configuration**

### **Procedure**

1. Log into your HelpScout application web account as company administrator.  
<https://secure.helpscout.net/members/login/>
2. Navigate to **Manage -> Company -> Authentication**.
3. On Single Sign On tab, select **Use SAML SSO**.
4. Click **Enable SAML**.
5. In the Single Sign On URL field enter the [Identity Provider URL](#) from step 4a on page 5.
6. In the X.509 Certificate field click **Upload Certificate** and use the [public certificate](#) use in step 4d on page 5.
7. In the Email Domains field enter your organization's email domains. You can enter more than one if needed separated by comma.
8. Use the Force SAML Sign-on only if you want to force users to use SAML Sign-on only.
9. Click **Save**.

The screenshot shows the HelpScout configuration page for SAML. On the left is a sidebar with 'EMC' and navigation options: 'Edit Company', 'Authentication' (highlighted), 'Features', 'Import Data', 'Office Hours', and 'Spam Filtering'. The main content area has tabs for 'Single Sign-On', 'IP Restrictions', and 'Two-Factor Authentication'. Under 'Single Sign-On', there are two buttons: 'Use SAML SSO' (selected) and 'Use Google SSO'. Below these are several settings:

- Enable SAML:** A toggle switch that is turned on.
- Single Sign-On URL:** A text input field containing 'https://portal.sso5.pe-lab.com/IdPServlet?idp\_ic' with an information icon.
- X.509 Certificate:** A button labeled 'Upload Certificate' with an information icon. Below it, the text 'cert - Copy.pem.cer previously uploaded' is displayed.
- Email Domains:** A text input field containing 'emc.com, rsa.com' with an information icon.
- Force SAML Sign-on:** A toggle switch that is turned off. Below it, the text 'On their next log in, force all users to authenticate via SAML.' is displayed.

At the bottom of the configuration area are two buttons: a blue 'Save' button and a 'Test Connection' button with an information icon.



# HelpScout

10. You can view SP metadata on the same page.

## Post-back URL (Assertion Consumer Service URL)

```
https://helpscout.auth0.com/login/callback?connection=emc-75307-sso-saml
```

## Audience URI (Service Provider Entity ID)

```
urn:auth0:helpscout:emc-75307-sso-saml
```

## Help Scout logo

```
https://d12wqas9hcki3z.cloudfront.net/images/Help-Scout-Logo.png
```