RSA SECURID® ACCESS
Implementation Guide

HelpScout

Gina Salvalzo, 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	
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 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.

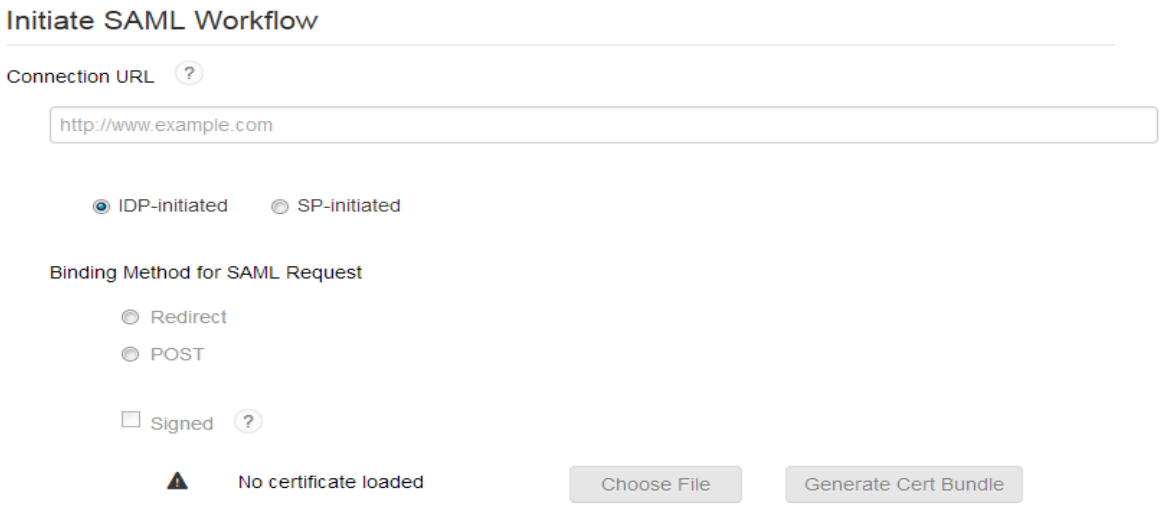
Configure RSA Identity Router SAML IdP

Procedure

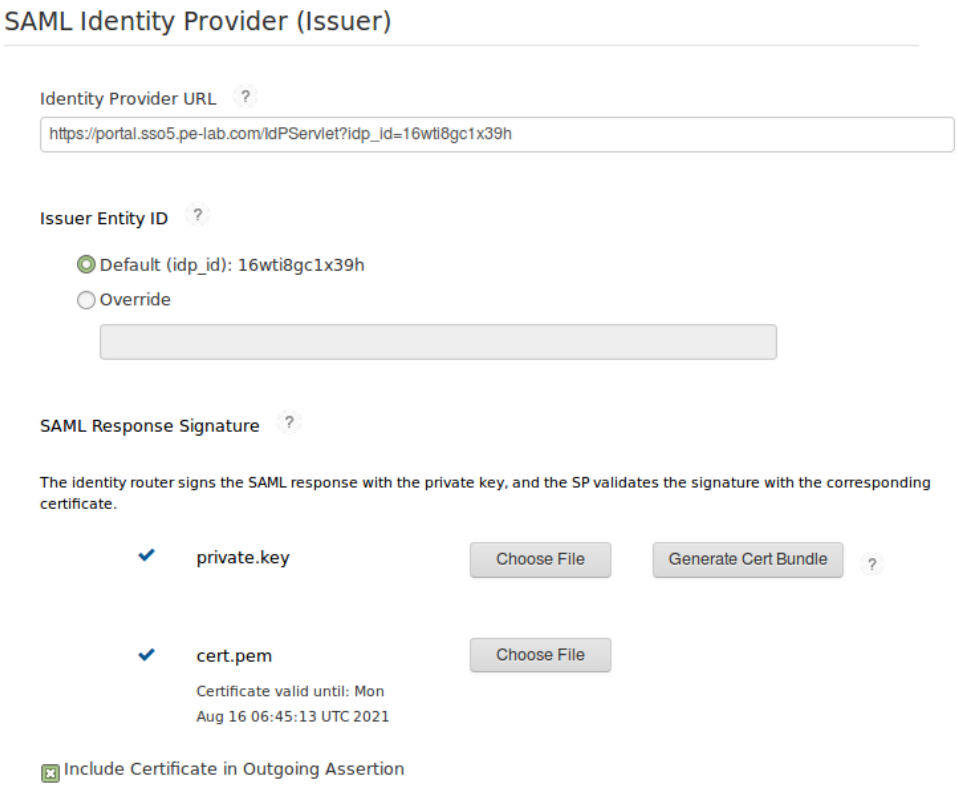
1. Logon to the RSA SecurID Access console and browse to Applications > Application Catalog, search for HelpScout and click **+Add** to add the connector.

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.

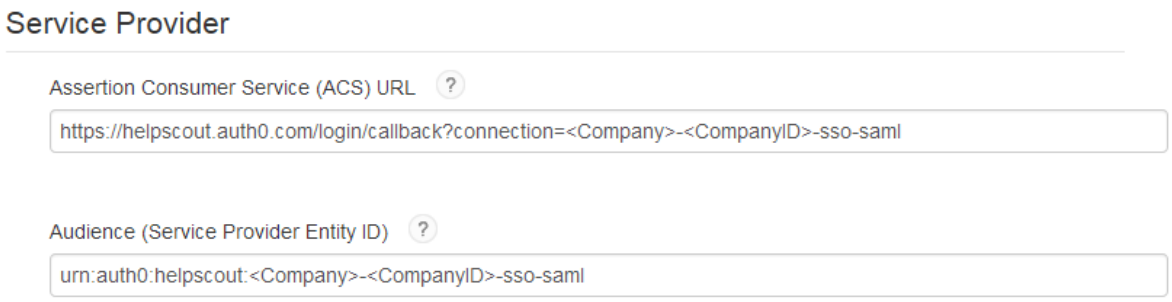


4. Scroll down to SAML Identity Provider (Issuer) section.

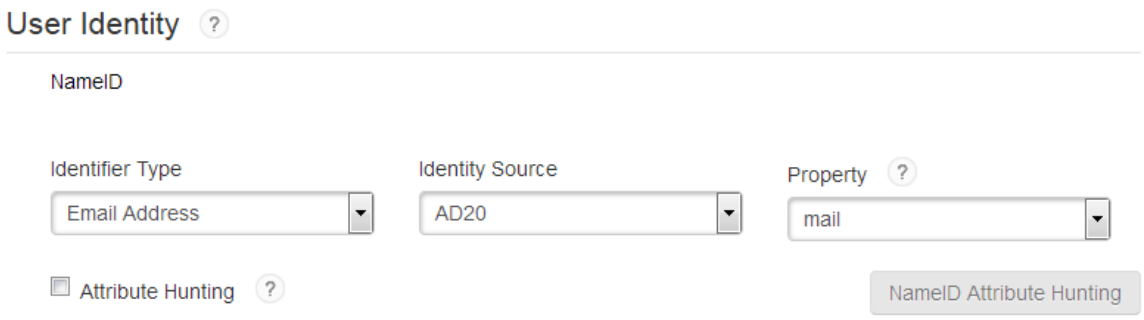


a. Take note of the Identity Provider URL.
b. Take note of the Issuer Entity ID.
c. Select **Choose File** and upload the private key.
d. Select **Choose File** to import the public signing certificate.
e. Select the checkbox for **Include Certificate in Outgoing Assertion**.

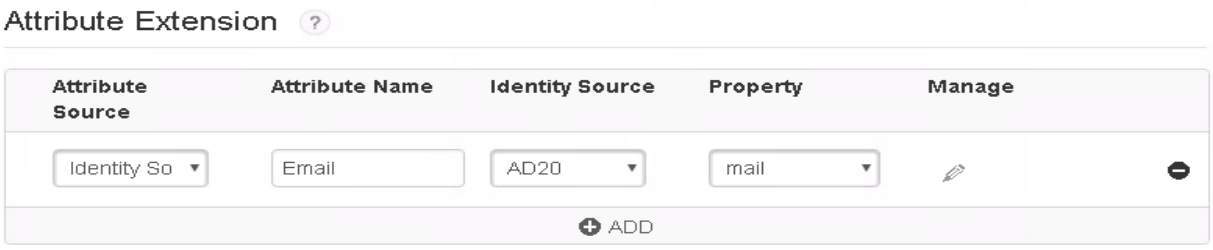
5. Scroll down to the **Service Provider** section.



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.

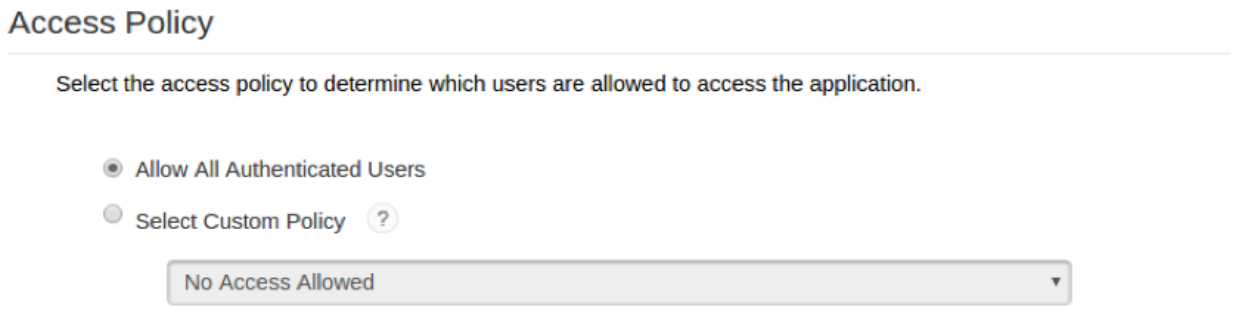


9. Click the **Show Advance** button.
10. Under the Attribute Extension section, enter the attribute **Email** and the mapped Active Directory attribute for this value.



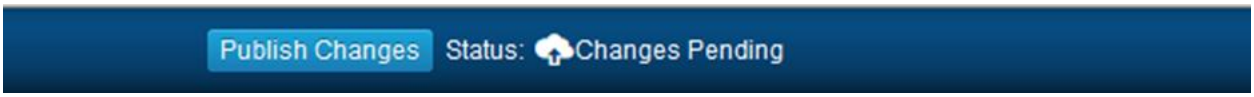
11. Click **Next Step**.

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.



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

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.

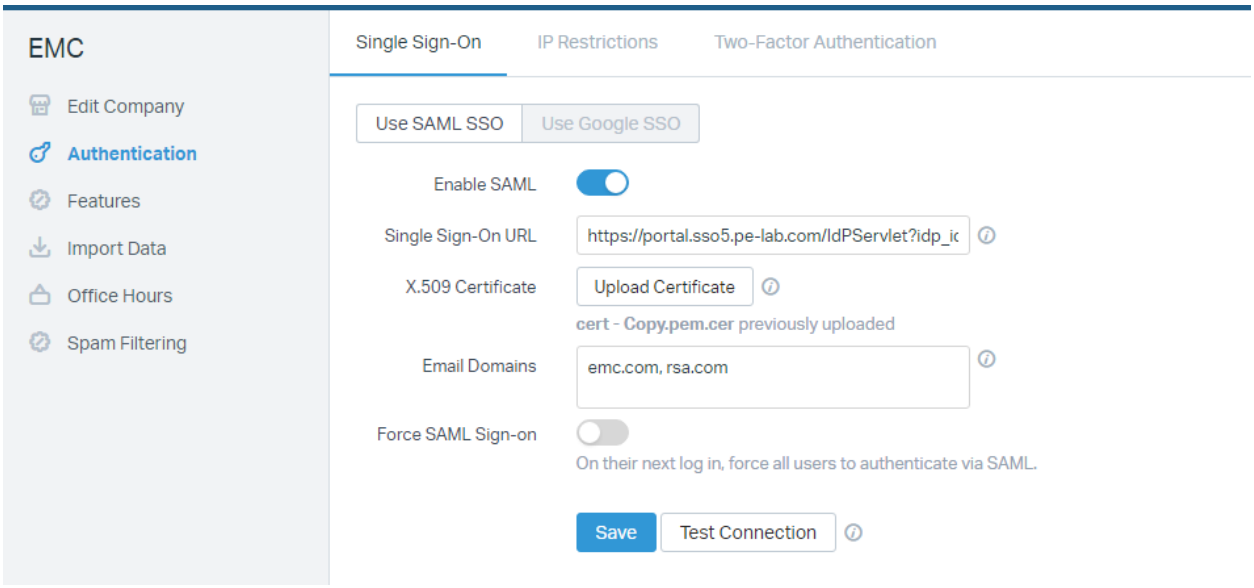
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

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**.



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