# RSA SECURID® ACCESS
# Implementation Guide

## Mojo Helpdesk

Gina Salvalzo, RSA Partner Engineering
Last Modified: September 27, 2017

RSA READY

## Solution Summary

Mojo Helpdesk is a hosted ticket tracking/on-demand help desk service that allows companies and businesses to centralize, assign and monitor user tech and customer requests, as well as internal tasks within the organization. Mojo Helpdesk delivers a single sign on experience to the user through SAML. This integration supports both IdP and SP initiated authentication flows.

| RSA SecurID Access Features | Mojo Helpdesk |
|---|---|
| **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 Mojo Helpdesk 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** – Mojo Helpdesk 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**
**Mojo Helpdesk 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 Mojo Helpdesk 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.

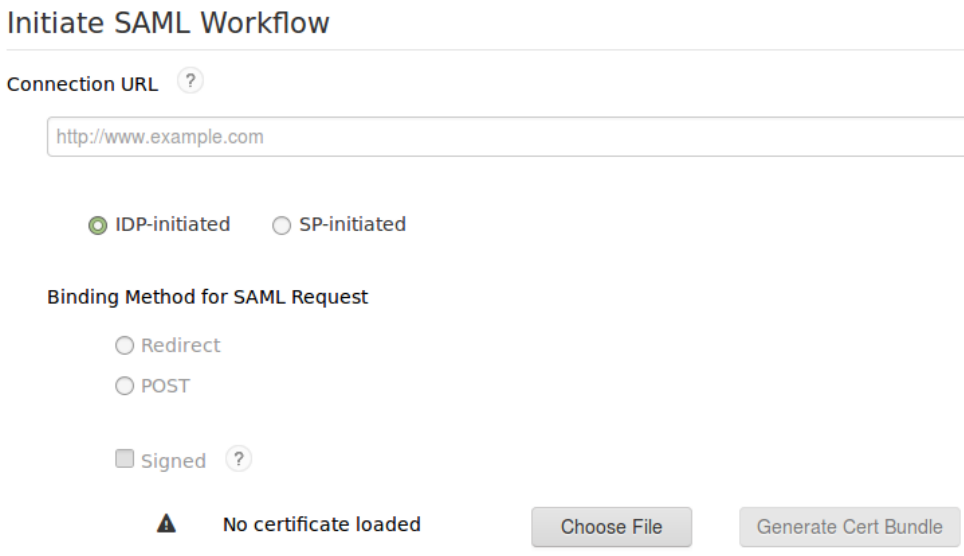
#### Configure RSA Identity Router SAML IdP

#### Procedure

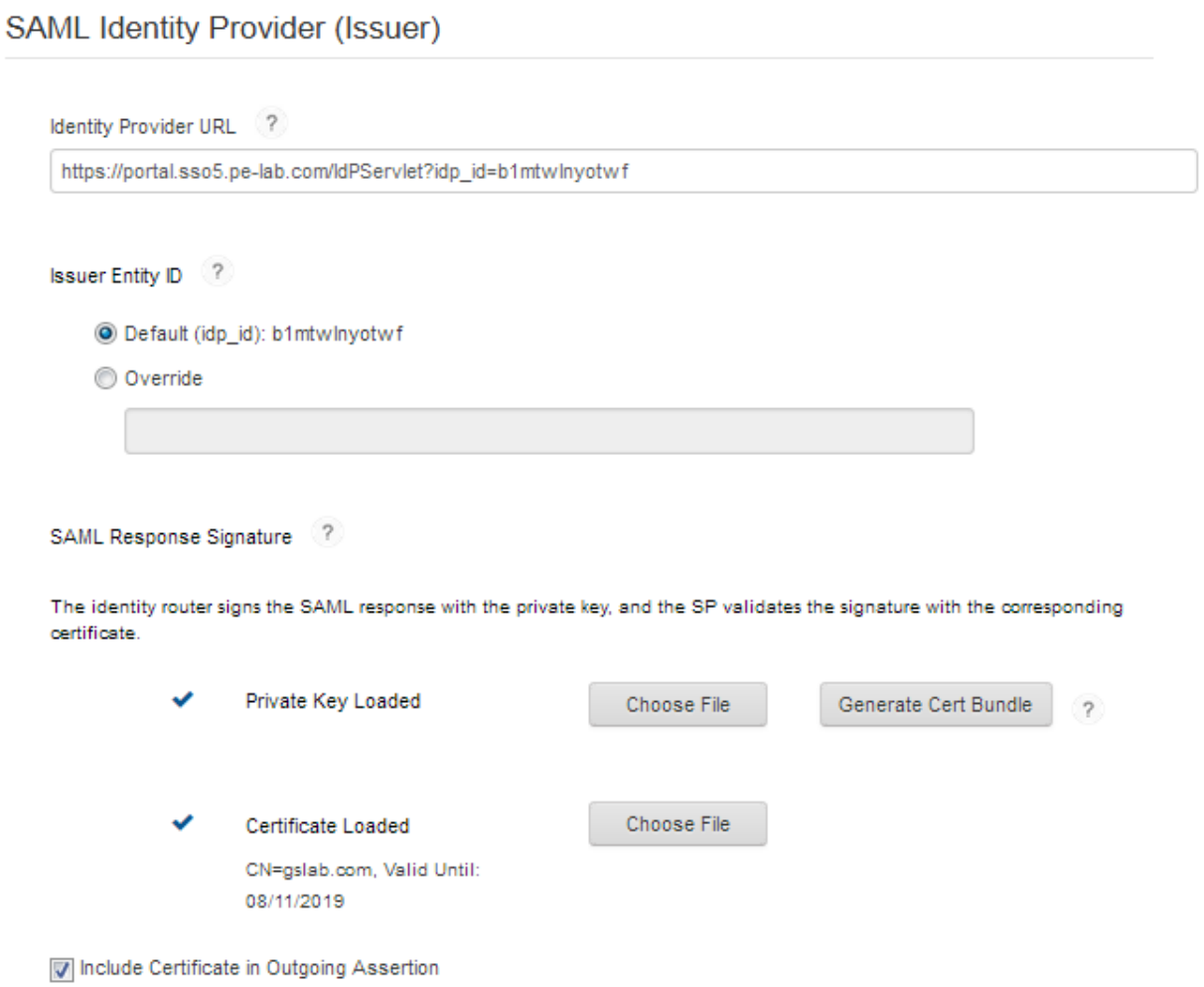
1. Logon to the RSA SecurID Access console and browse to **Applications** > **Application Catalog**, search for Mojo Helpdesk and click **+Add** to add the connector.


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 Mojo Helpdesk connections as well.

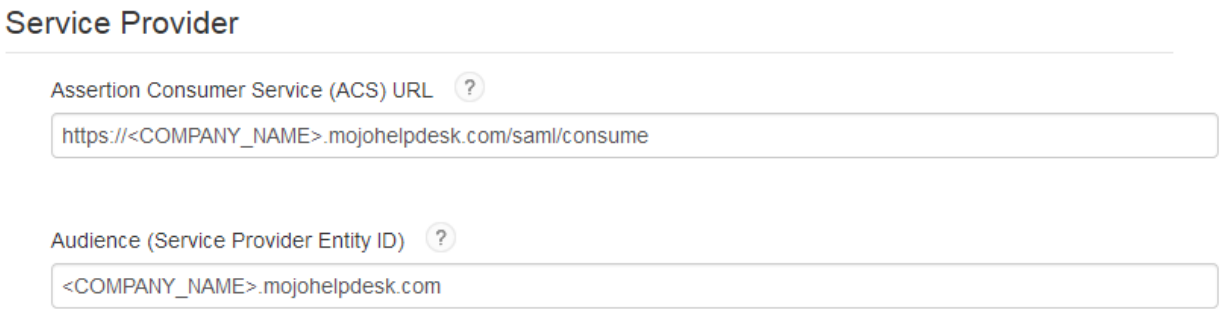


4. Scroll down to SAML Identity Provider (Issuer) section.

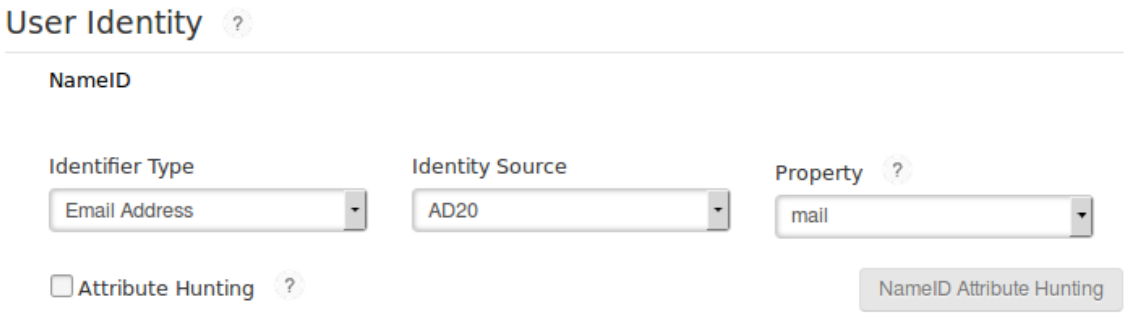



a. Make a note of **Identity Provider URL** field value, as it will be needed later to configure the Service Provider configuration.
b. Select **Default (idp_id)** for value for the **Issuer Entity ID**. Make sure that same **Issuer ID** is provided at SP-side SAML configuration.
c. Select **Choose File** 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**.
f. Note the value of Issuer Entity ID.

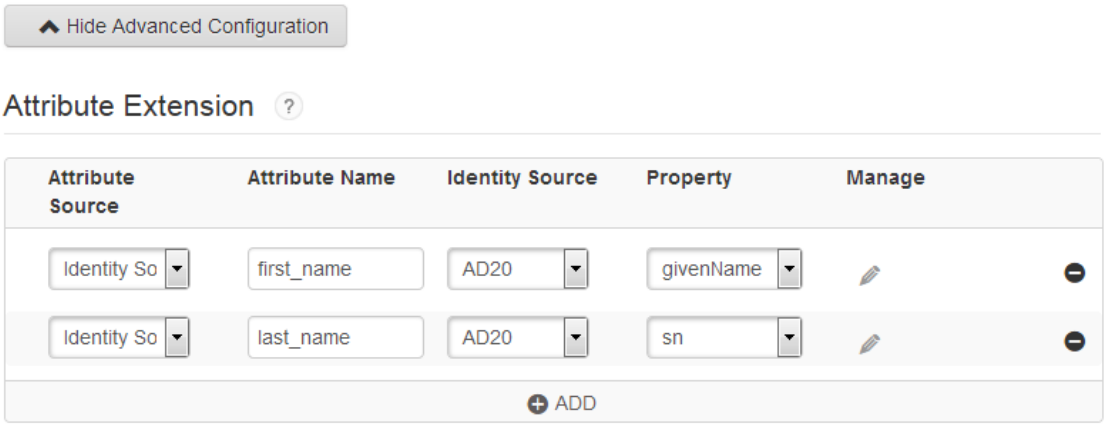
5. Scroll down to the **Service Provider** section.



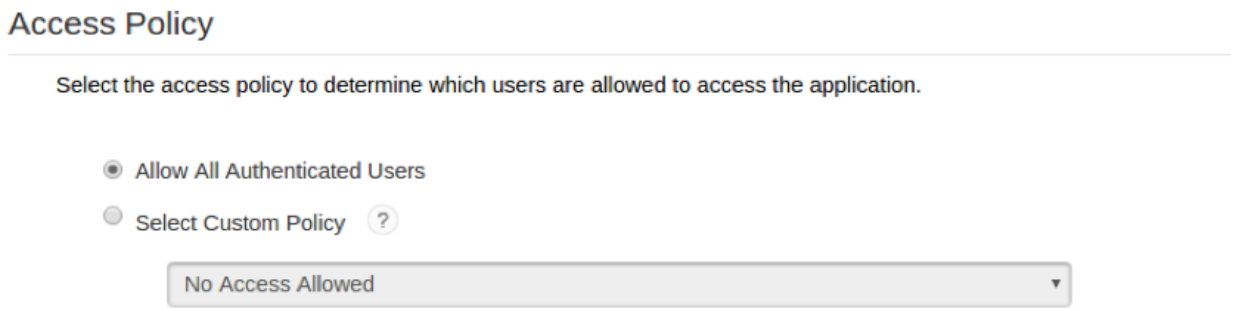

6. In the **Assertion Consumer Service (ACS) URL** field, provide the value as per received from the service provider. Replace <COMPANY_NAME> with your domain name.
7. In the **Audience (Service Provider Issuer ID)** field, provide the value as per received from the service provider. Replace <COMPANY_NAME> with your domain name.
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.



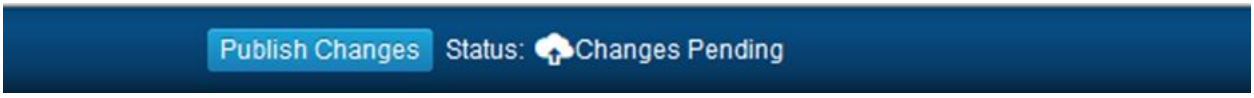

9. Scroll down below to *Advanced Configuration* section. Verify the settings are correct for your environment. In this example, *first_name* will be validated against *givenName* and last_name will be validated against sn from the user store selected.



10. 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.



# Partner Product Configuration

## *Before You Begin*

This section provides instructions for configuring the Mojo Helpdesk with RSA SecurID Access. This document is not intended to suggest optimum installations or configurations.

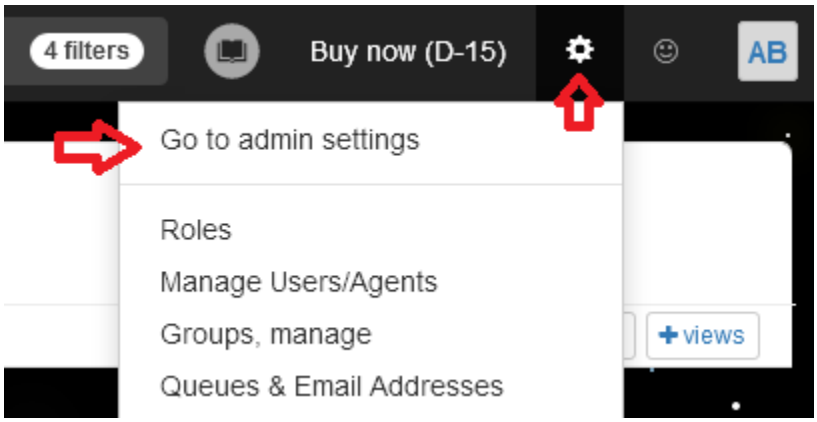
It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All Mojo Helpdesk components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

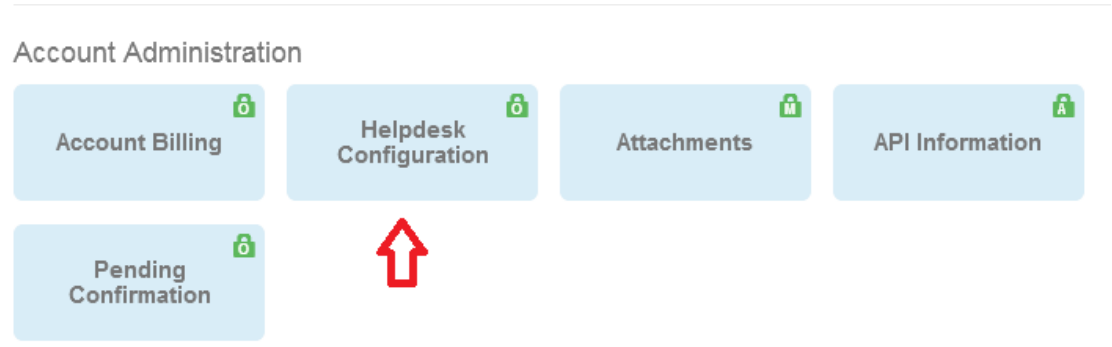
## Mojo Helpdesk SAML Configuration

**Procedure**

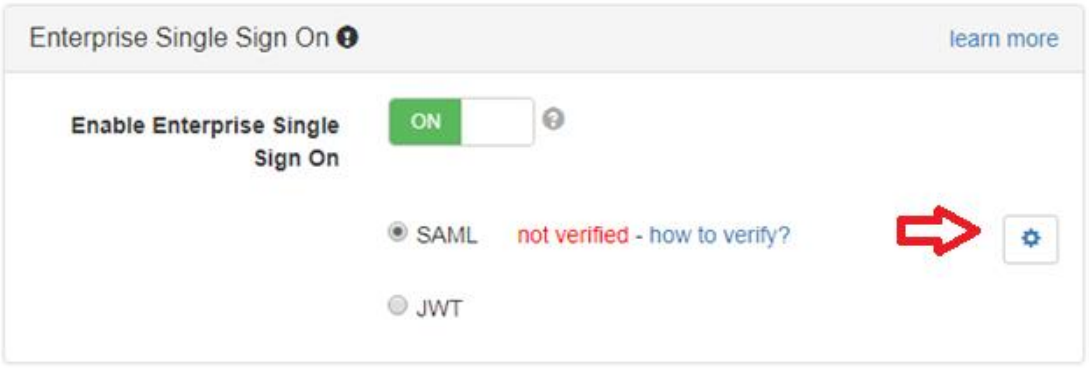
1. Login to your Mojo Helpdesk application web account.
   **https://<COMPANY_NAME>.mojohelpdesk.com**
2. On the displayed page, Click on *gear* icon on the upper right corner. Then click on *Go to admin settings.*




3. On the displayed settings, scroll down to *Account Administration*. Click on *Helpdesk Configuration*.

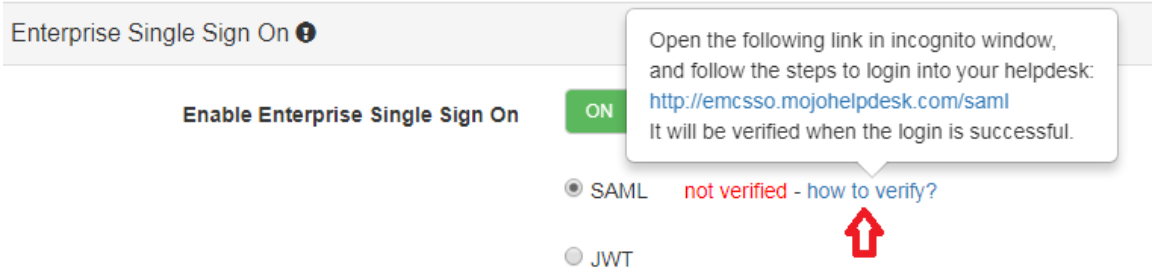


4. On the displayed page, click **ON** for *Enable Enterprise Single Sign On*. Select *SAML* radio button. Click on *gear* icon on the right side.




5. A pop up will get displayed. Enter **IDP URL** in **Remote Login URL** section. Enter fingerprint of **IDP certificate** in the **Certificate fingerprint** section. Click on **Save** button.


6. Mojo Helpdesk gives you SP initiated login URL. To get your SP initiated SSO URL click on *how to verify?* link as shown below.




7. Your Mojo Helpdesk account is now enabled for SAML Single Sign on.