RSA SecurID Access Implementation Guide

Keeper Security, Inc.

Password Manager & Digit Vault 14.4

Certified: April 30, 2019

Table of Contents

Solution Summary

This section describes the ways in which Keeper Password Manager can integrate with RSA SecurID Access. Use this information to determine which use case and integration type your deployment will employ.

Use Case

When integrated, Keeper Password Manager users must authenticate with RSA SecurID Access to sign in. Keeper Password Manager can integrate using Authentication Agent, SSO Agent or relying party integration types.

Integration Types

SSO Agent integrations use SAML 2.0 or HFED technologies to direct users' web browsers to RSA SecurID Access for authentication. SSO Agents also provide Single Sign-On using the RSA Application Portal.

Relying Party integrations use SAML 2.0 to direct users' web browsers to RSA SecurID Access for authentication. Primary authentication is configurable, so relying party can be a good choice for adding additional authentication (only) to existing deployments.

Authentication Agent integrations use an embedded RSA agent to provide RSA SecurID and Authenticate Tokencode authentication methods within the partner's application. Authentication agents are simple to configure and support the highest rate of authentications.

Supported Features

This section shows all of the supported features by integration type and by RSA SecurID Access component. Use this information to determine which integration type and which RSA SecurID Access component your deployment will use.

Keeper Password Manager integration with RSA Cloud Authentication Service

Authentication Methods	Authentication API	RADIUS	Relying Party	SSO Agent
RSA SecurID	-	-	✔	✔
LDAP Password	-	-	✔	✔
Authenticate Approve	-	-	✔	✔
Authenticate Tokencode	-	-	✔	✔
Device Biometrics	-	-	✔	✔
SMS Tokencode	-	-	✔	✔
Voice Tokencode	-	-	✔	✔
FIDO Token	n/a	n/a	✔	✔

Keeper Password Manager integration with RSA Authentication Manager

Authentication Methods	Authentication API	RADIUS	Authentication Agent
RSA SecurID	-	-	✔
On-Demand Authentication	-	-	✔
Risk-Based Authentication	n/a	-	-

✔ Supported

- Not supported

n/a Not applicable

n/t Not yet tested or documented, but may be possible.

Configuration Summary

This section links to instructions for integrating Keeper Password Manager with RSA SecurID Access using all of the integration types.

This document is not intended to suggest optimum installations or configurations. assumes 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 RSA SecurID Access and Keeper Password Manager components must be installed and working prior to the integration.

Integration Configuration

Authentication Agent

Relying Party

SSO Agent - SAML

Certification Details

Date of testing: April 19th, 2019

RSA Cloud Authentication Service

RSA Authentication Manager 8.3, Virtual Appliance

Keeper Security Password Manager & Digital Vault 14.4.4

Keeper Security SSO Connect 14.02

Known Issues

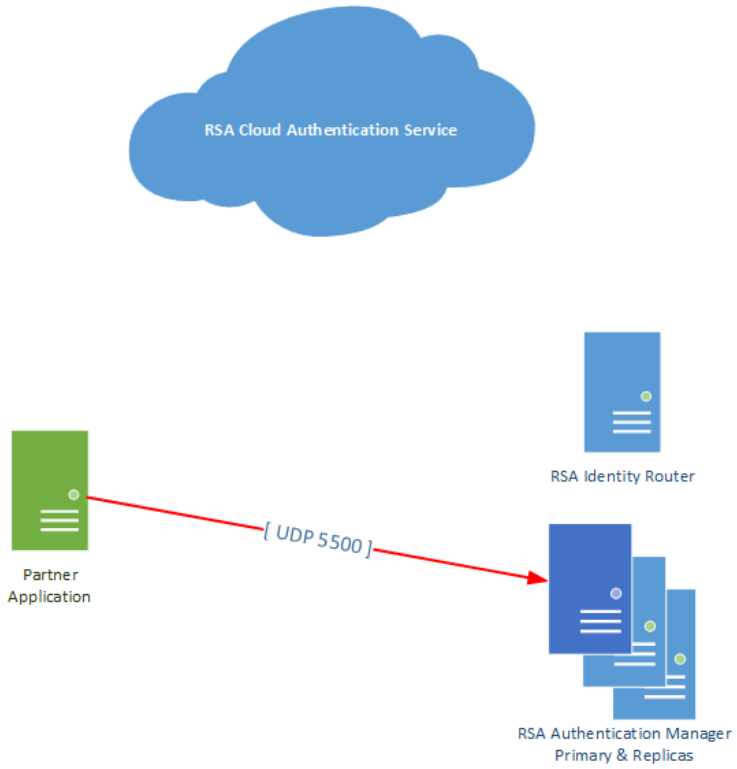
No known issues.

Integration Configuration

Authentication Agent

This section describes how to integrate RSA SecurID Access with Keeper Password Manager as an authentication agent.

Architecture Diagram



RSA Authentication Manager

To configure your RSA Authentication Manager for use with an authentication agent, you must create an agent host record in the Security Console of your Authentication Manager and download its configuration file (sdconf.rec).

Agent host record configuration differs slightly depending on whether you are using a UDP-based agent (using 8.1.x or earlier RSA Agent API) or TCP-based agent (using 8.5 or newer RSA Agent API).

If UDP-based agent:

- Hostname: Configure the agent host record name to match the hostname of the agent.
- IP Address: Configure the agent host record to match the IP address of the agent.

Note: Authentication Manager must be able to resolve the IP address from the hostname

If TCP-based agent:

- Hostname: Configure the agent host record name to match the agent name as specified in the agent's configuration. It does not have to match the hostname of the authentication agent.
- IP Address: Leave blank. Any input to this field will be disregarded.

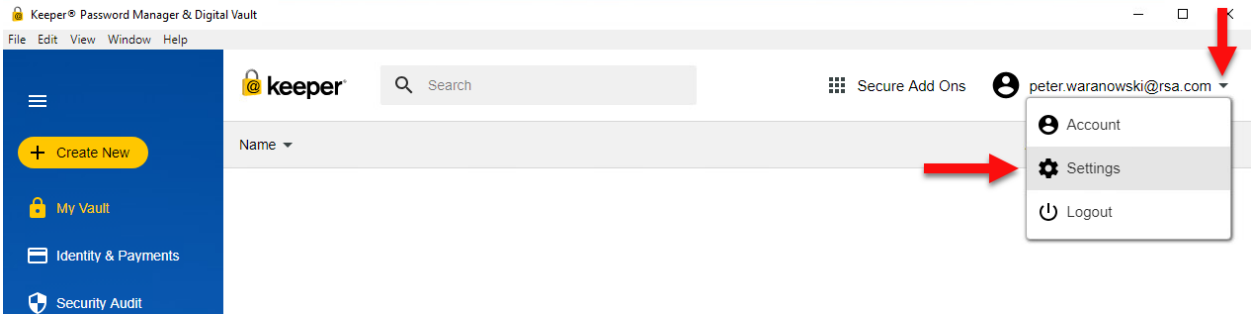
Keeper Password Manager

Perform these steps to configure Keeper Password Manageras an authentication agent to RSA Authentication Manager.

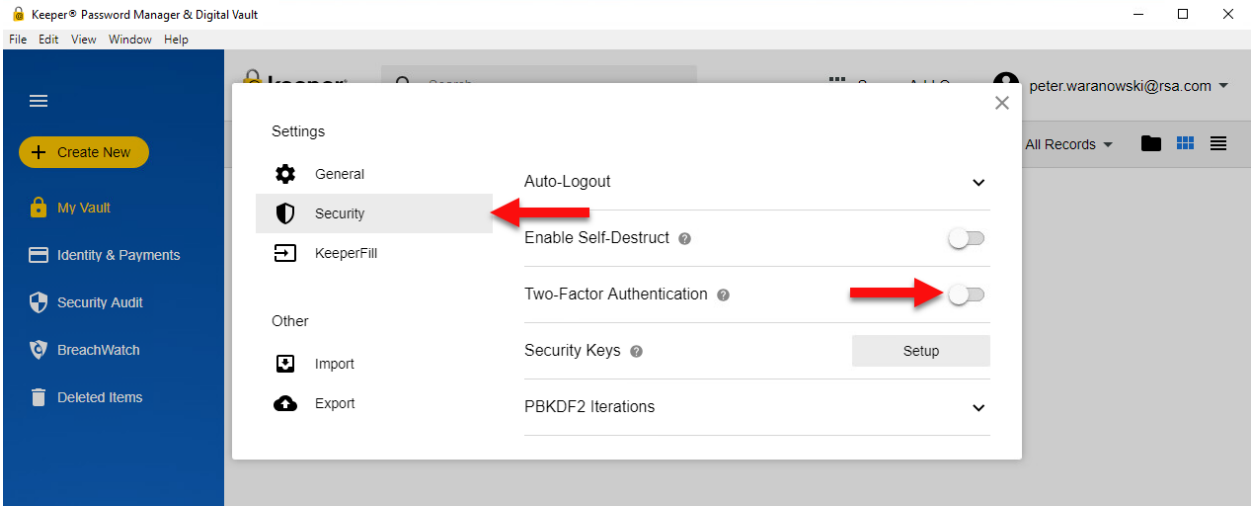
Procedure

Important! Work with Keeper Security support team to enable back-end setup before performing these steps.

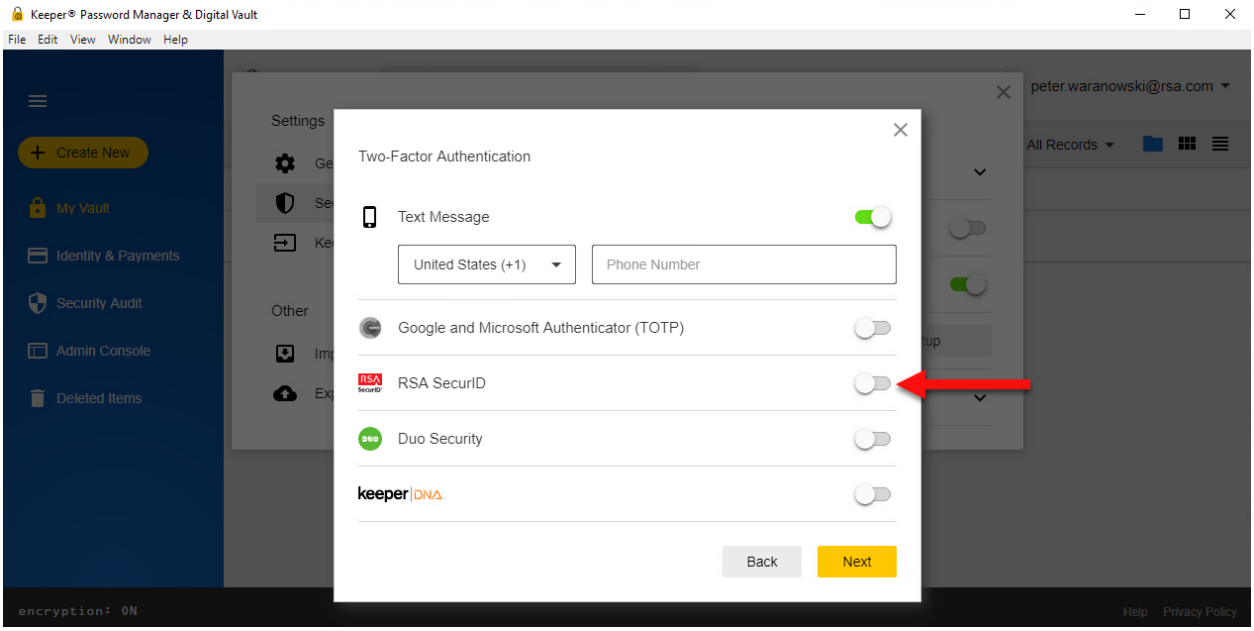
1. Sign in to Keeper Password Manager using an administrator account and click to open **Settings**.



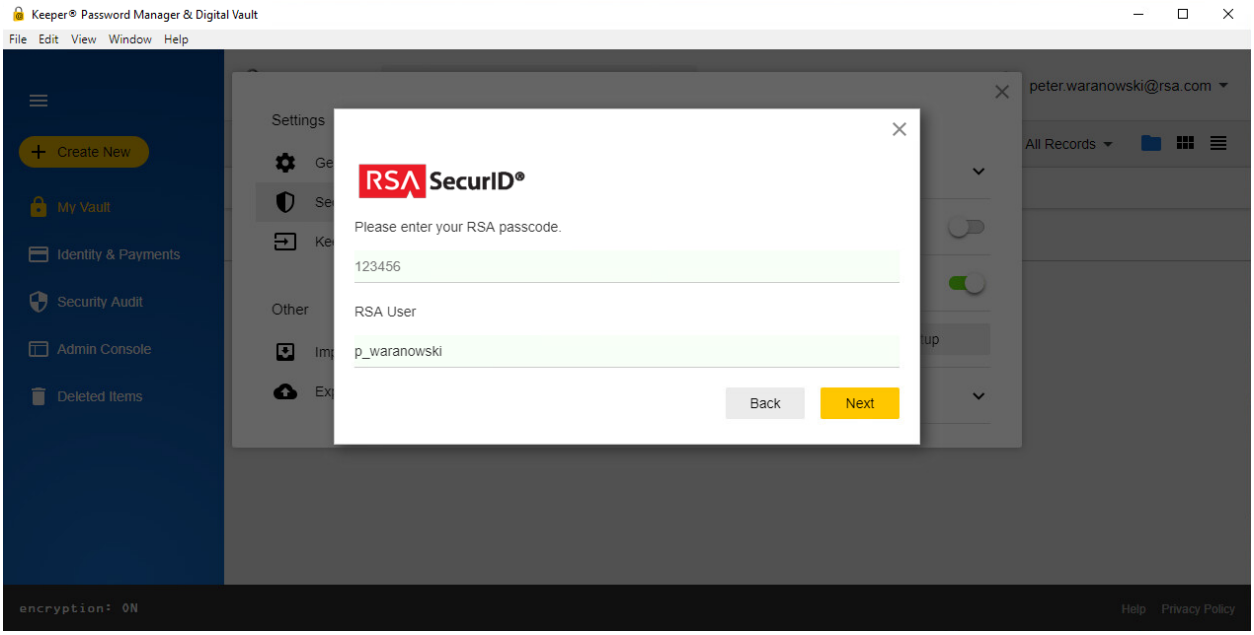
2. Open the **Security** tab and click to enable **Two-Factor Authentication**.



3. Click to enable **RSA SecurID**.



4. Enter your RSA SecurID username and passcode and click **Next**.



Configuration is complete.

SecurID Agent Integration Details

RSA Authentication Agent API	8.1.3.0 build 567
RSA SecurID Authentication API (REST)	N/A
RSA SecurID User Specification	Designated Users
Display RSA Server Info	No
Perform Test Authentication	No
Agent Tracing	No

RSA Authentication Agent Files (C and Java Agents)

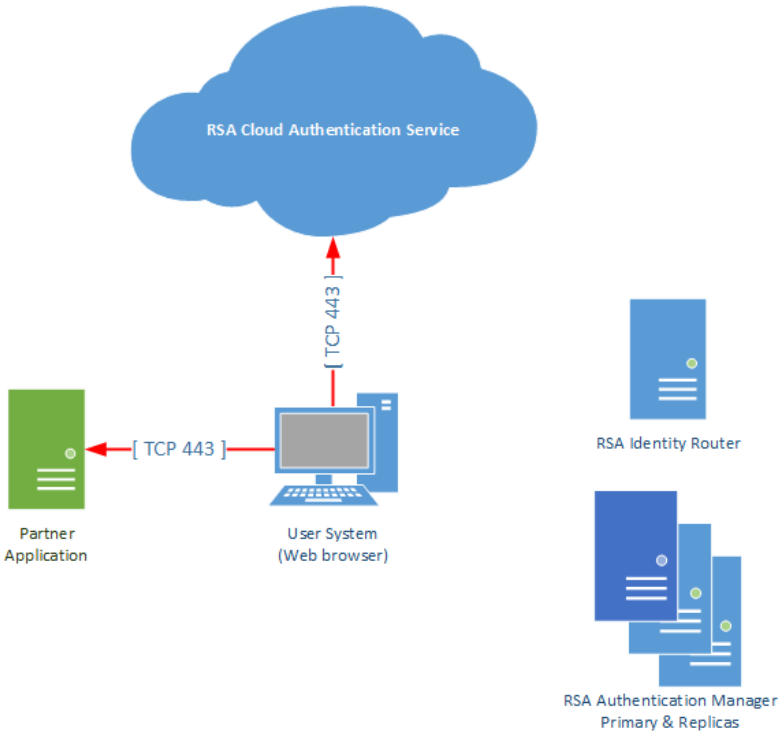
Agent Files	Location
sdconf.rec	In Keeper Security Cloud
sdopts.rec	In Keeper Security Cloud
Node secret	In Keeper Security Cloud
sdstatus.12 / jastatus.12	In Keeper Security Cloud
rsa_api.properties	N/A

Return to the main page for more integration related information.

Relying Party

This section describes how to integrate RSA SecurID Access with Keeper Password Manager using relying prty. Relying party uses SAML 2.0 to integrate RSA SecurID Access as a SAML Identity Provider (IdP) to Keeper Password Manager SAML Service Provider (SP).

Architecture Diagram

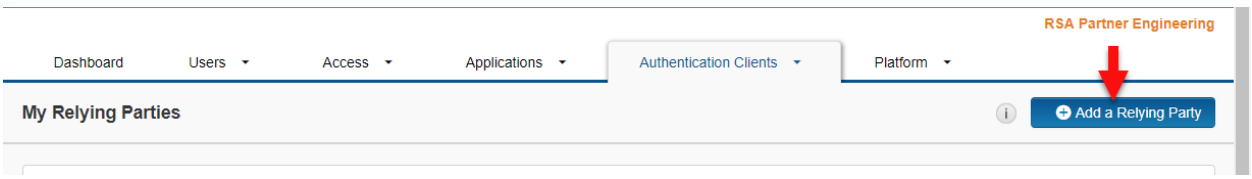


RSA Cloud Authentication Service

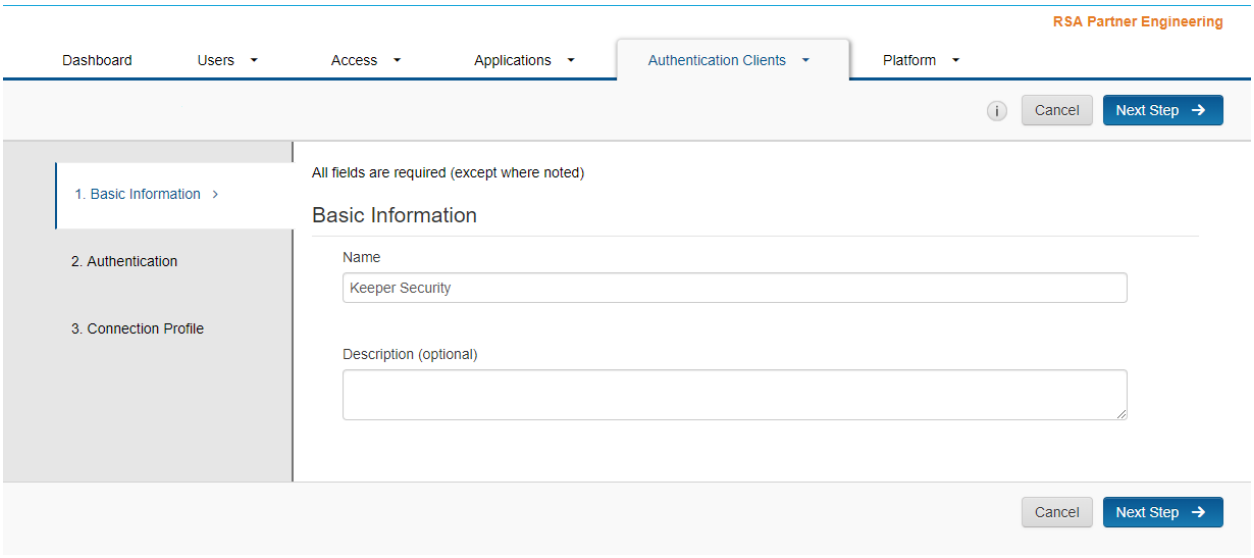
Perform these steps to configure RSA Cloud Authentication Service as a relying party SAML IdP to Keeper Password Manager.

Procedure

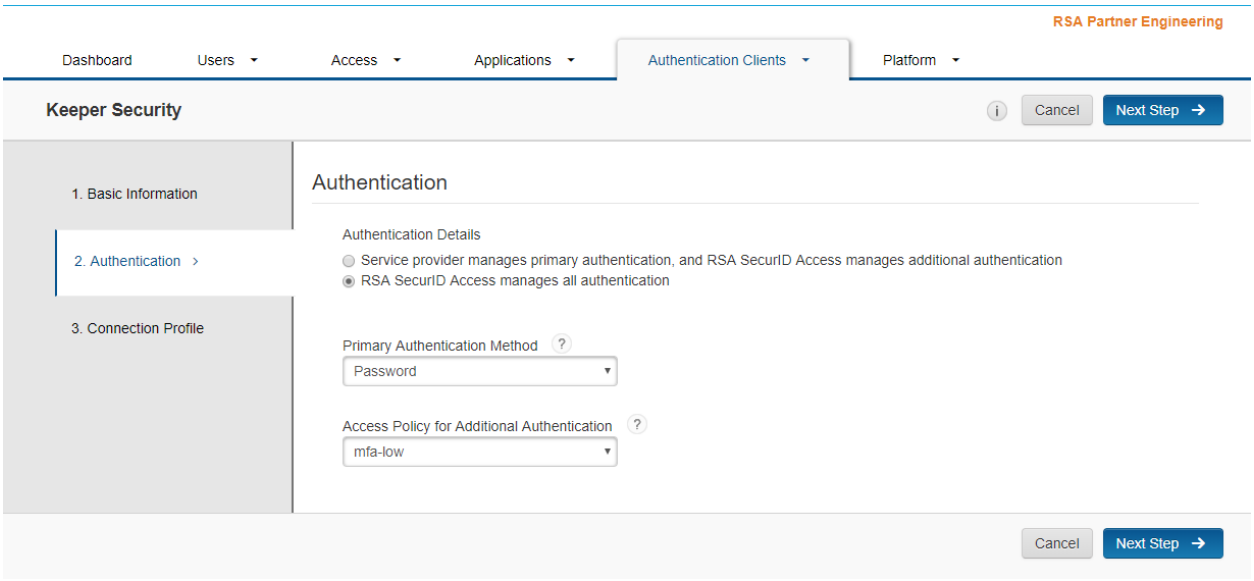
1. Logon to the **RSA Cloud Administrative Console** and browse to **Authentication Clients** > **Relying Parties** and click **Add a Relying Party**.



2. Enter a **Name** and click **Next Step**.

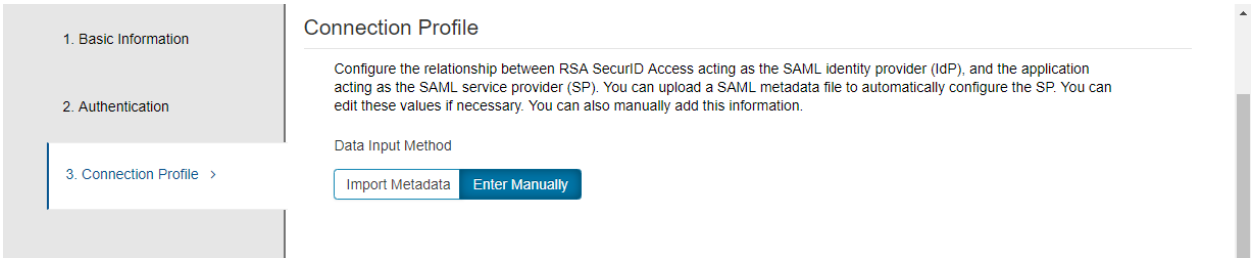


3. Configure the Authentication settings and click **Next Step**.

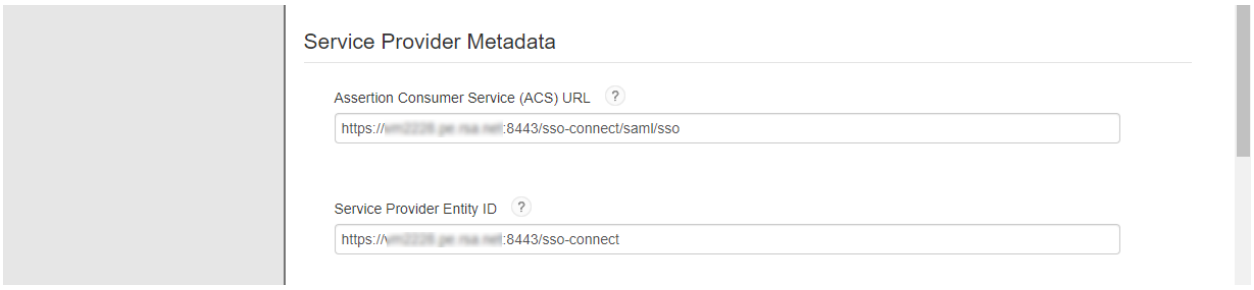


a. Select **RSA SecurID Access manages all authentication**.
b. Select your desired **Primary Authentication Method**.
c. Select your desired **Access Policy for Additional Authentication**.

4. Set **Data Input Method** to **Enter Manually** and scroll down to the **Service Provider Metadata** section.



5. Configure the Service Provider Metadata settings and scroll down to the **Audience for SAML Response** section.



a. Enter the **Assertion Consumer Service (ACS) URL** in the format below and changing <*fqdn*> and <*port*> to match your Keeper SSO Connect deployment.

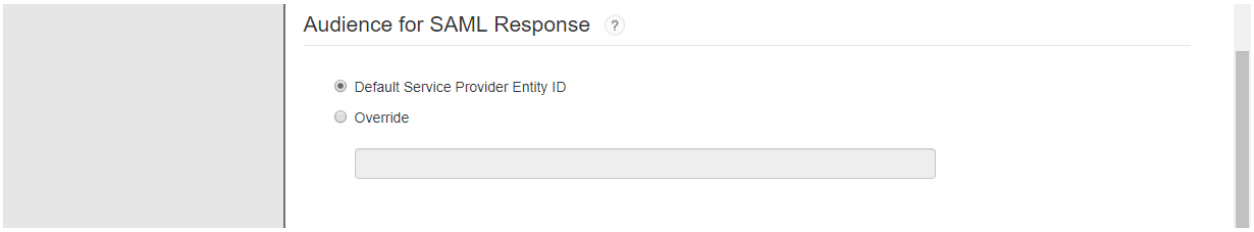
```
https://<fqdn>:<port>/sso-connect/saml/sso
```

b. Enter the **Service Provider Entity ID** in the format below and changing <*fqdn*> and <*port*> to match your Keeper SSO Connect deployment.

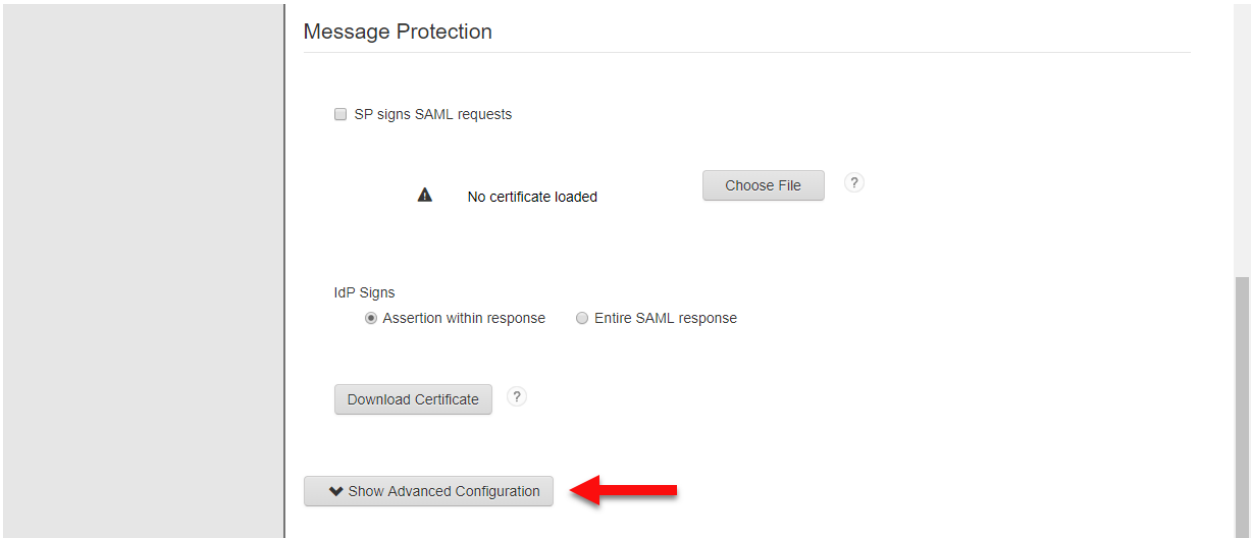
```
https://<fqdn>:<port>/sso-connect
```

Note: If the values for ACS URL and SP Entity ID are not known, enter placeholder values so that you can continue with the configuration. After you have configured the SP, return to this section and input the correct values.

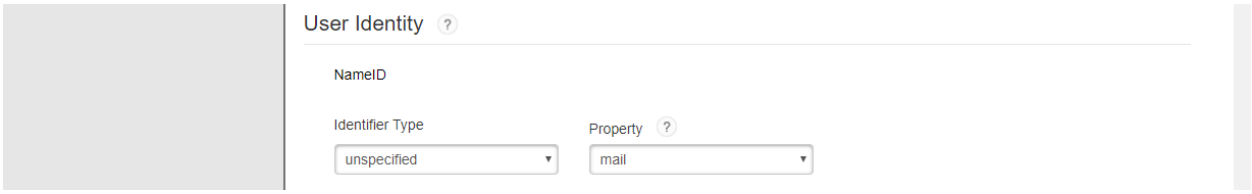
6. Leave the default settings and scroll down to the **Message Protection** section.



7. Leave the default settings and click to **Show Advanced Configuration**.

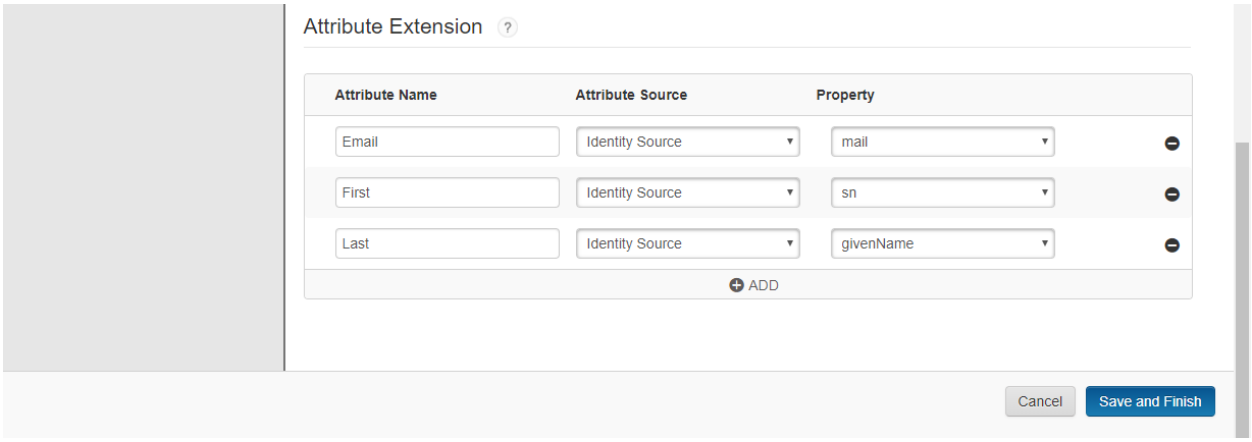


8. Configure the User Identity settings and scroll down to the **Attribute Extension** section.



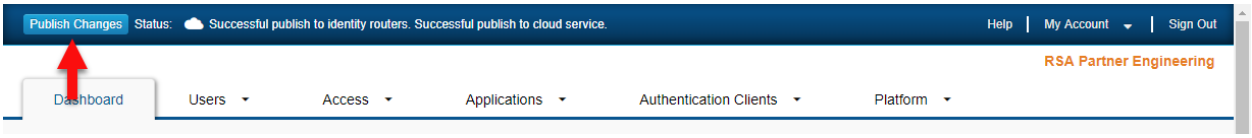
   a. Set NameID **Identifier Type** to **unspecified**.
   b. Set NameID **Property** to the identity source attribute which holds the Keeper Security account name.

9. Configure the Attribute Extension settings and click **Save and Finish**.



a. Add extension with Attribute Name **Email** with Attribute Source **Identity Source** and Property **mail**.
b. Add extension with Attribute Name **First** with Attribute Source **Identity Source** and Property **sn**.
c. Add extension with Attribute Name **Last** with Attribute Source **Identity Source** and Property **givenName**.

10. Click **Publish Changes**.



11. In the My Relying Party page, locate the application and click **Edit** > **View or Download IdP Metadata**. A file named *IdPMetadata.xml* should be downloaded.

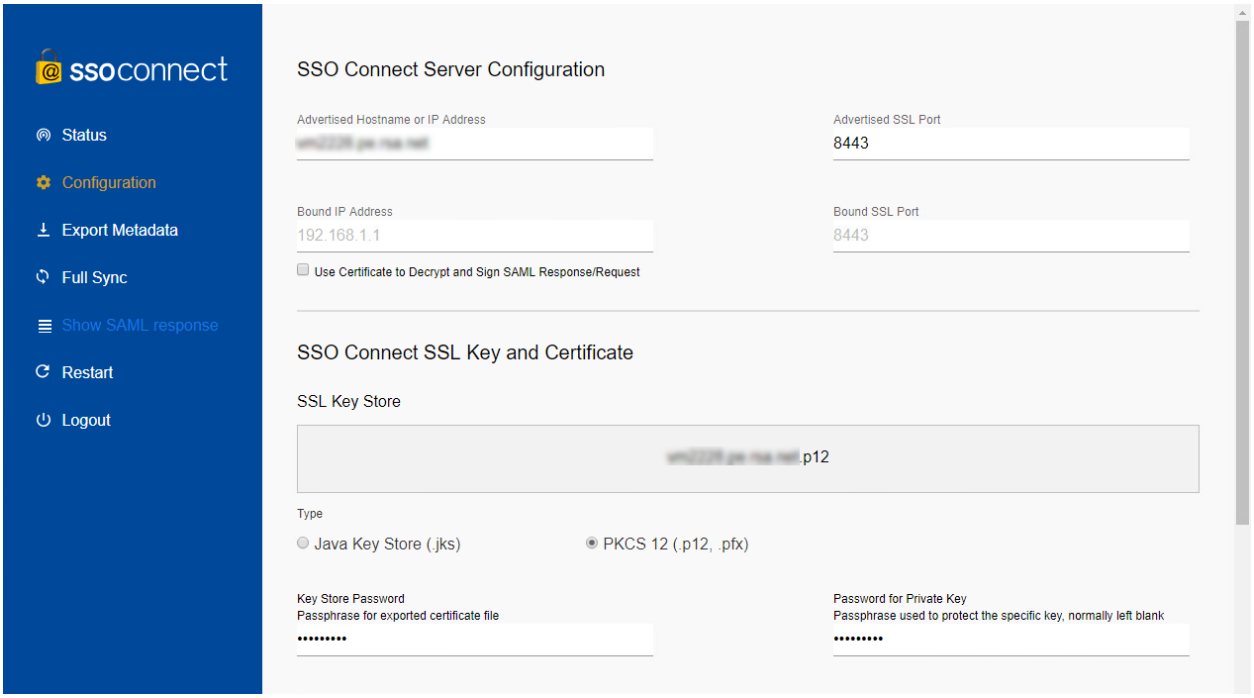
Keeper Password Manager

Follow the steps in this section to configure Keeper Password Manager as a Relying Party SAML SP to RSA Cloud Authentication Service.

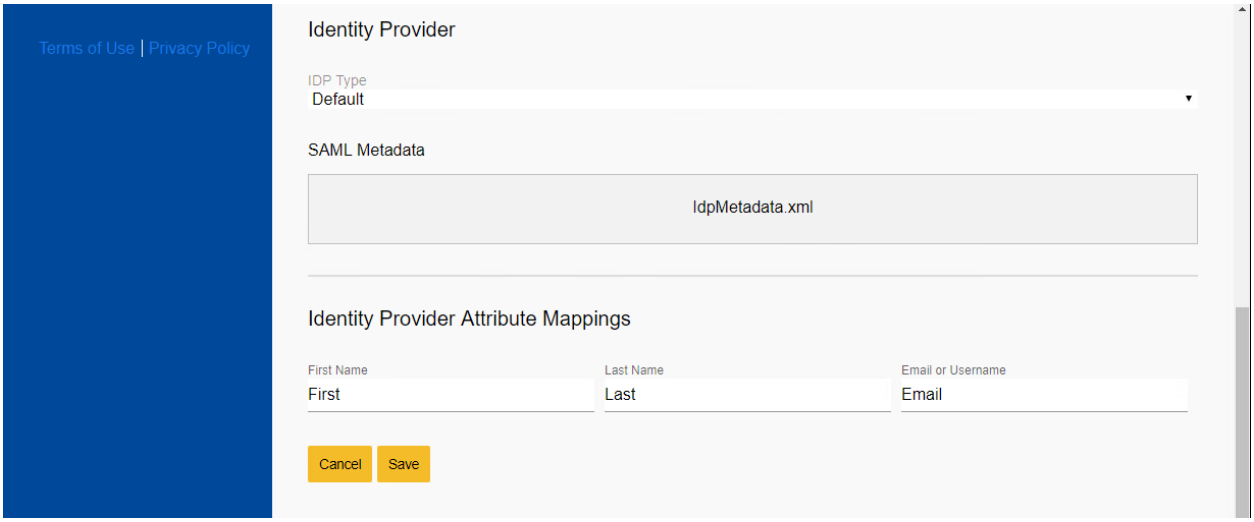
Procedure

1. Install Keeper Security SSO Connect and sign in using a Keeper Administrator account.

2. Open the **Configuration** tab, configure the **SSO Connect Server Configuration** settings and scroll down to the **Identity Provider** section.

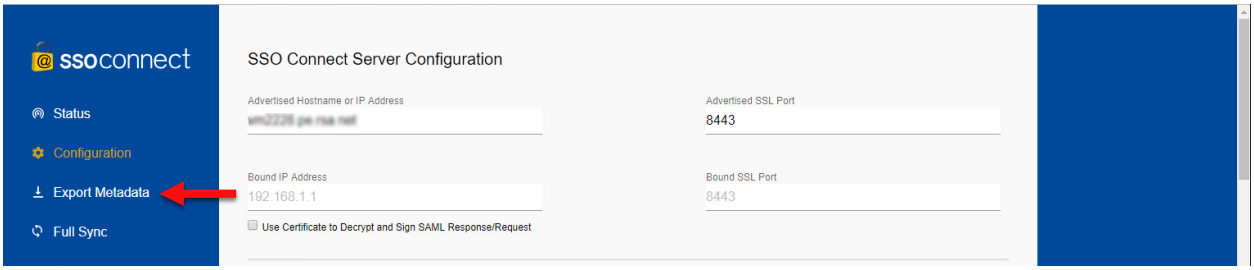


3. Set the IDP Type to **Default**, upload the **SAML Metadata** file you downloaded in the previous section and click to **Save**.

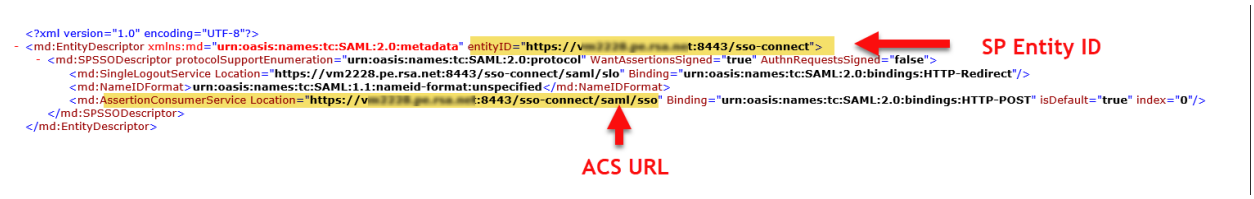


If you left placeholder values in the RSA Cloud Administration Console then follow the remaining steps. Otherwise, configuration is complete.

4. Click to Export Metadata from Keeper SSO Connect.



5. Open the metadata file with a text editor and locate the ACS URL and SP Entity ID values.



6. Return to the RSA Cloud Administration Console and replace the placeholder values with the correct ones and publish the changes.

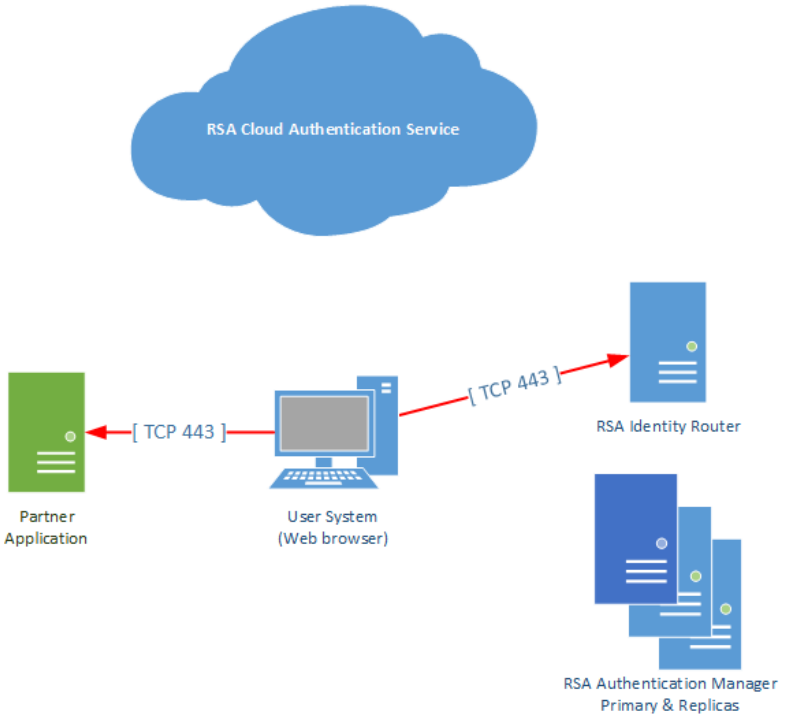
Configuration is complete.

Return to the main page for more integration related information.

SSO Agent - SAML

This section contains instructions on how to integrate RSA SecurID Access with Keeper Password Manager using a SAML SSO Agent.

Architecture Diagram

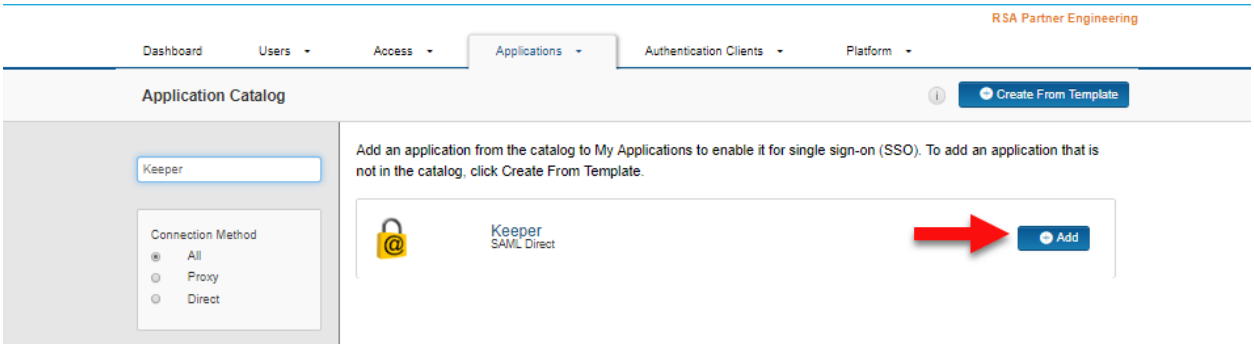


RSA Cloud Authentication Service

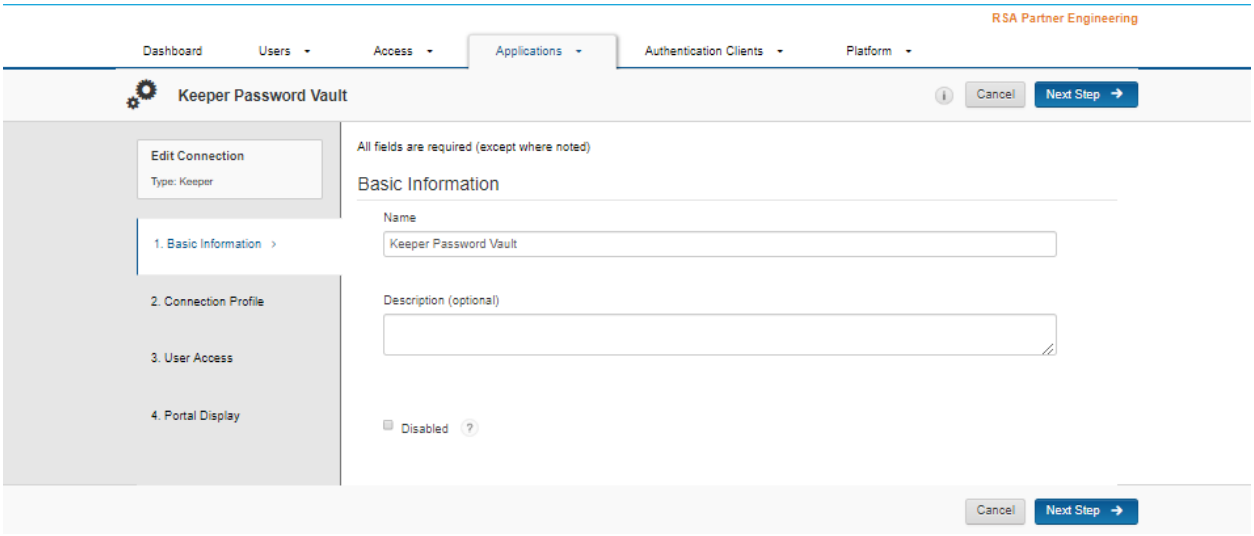
Perform these steps to configure RSA Cloud Authentication Service as an SSO Agent SAML IdP to Keeper Password Manager.

Procedure

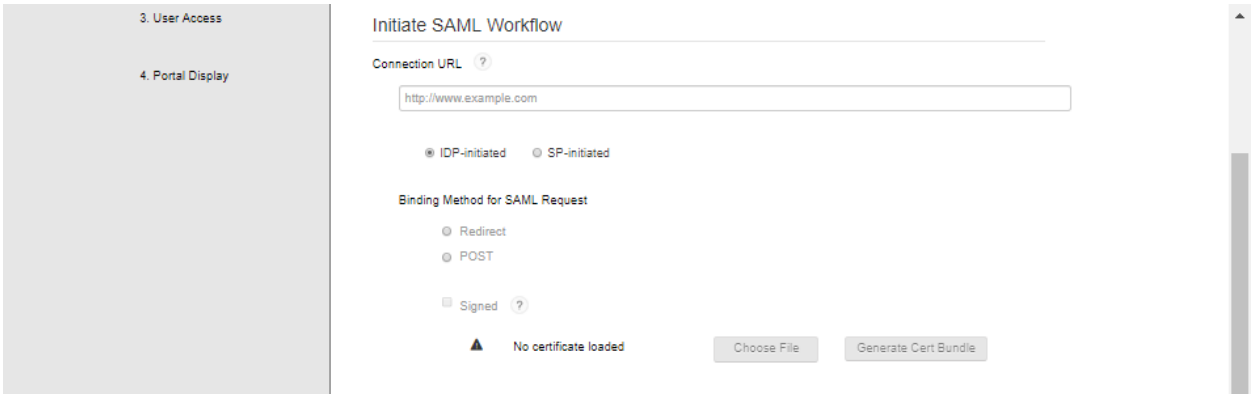
1. Log on to the RSA Cloud Administration Console and browse to **Applications** > **Application Catalog**, search for **Keeper** and click **+Add** to add the connector.



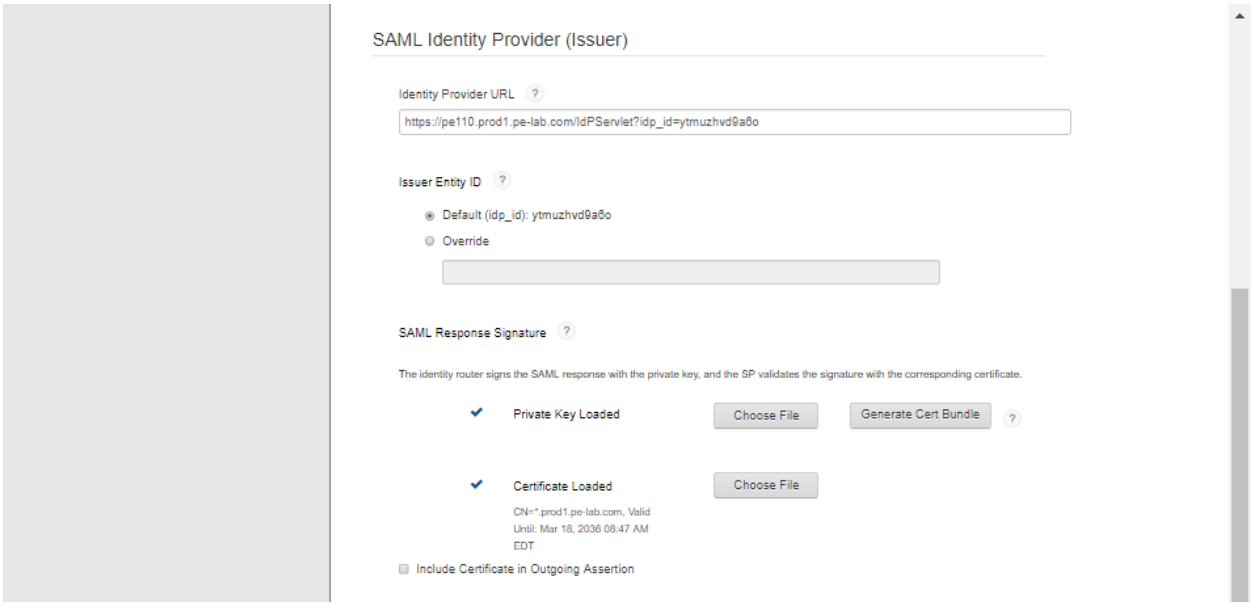
2. Enter a **Name** and click **Next Step**.



3. Leave the **default Initiate SAML Workflow** settings and scroll down to the **SAML Identity Provider (Issuer)** section.

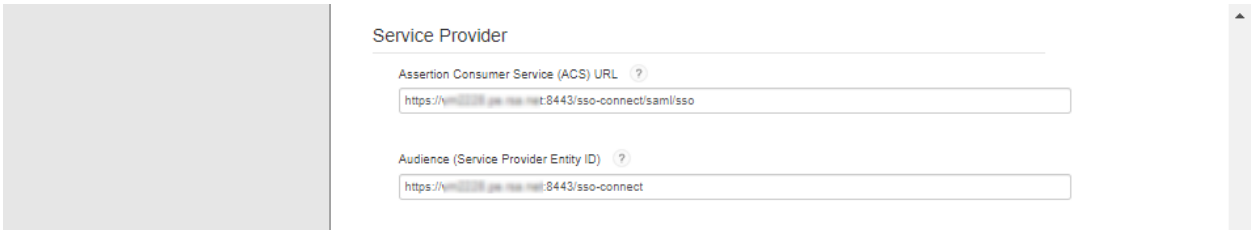


4. Configure the SAML Identity Provider settings and scroll down to the Service Provider section.



a. Leave the default **Identity Provider URL** and **Issuer Entity ID**.
b. Upload the SAML Response Signature **Private Key** and **Certificate**. Use from **Generate Cert Bundle** tool or your own.

5. Configure the Service Provider settings and scroll down to the **User Identity** section.



a. Enter the **Assertion Consumer Service (ACS) URL** in the format below and changing <*fqdn*> and <*port*> to match your Keeper SSO Connect deployment.

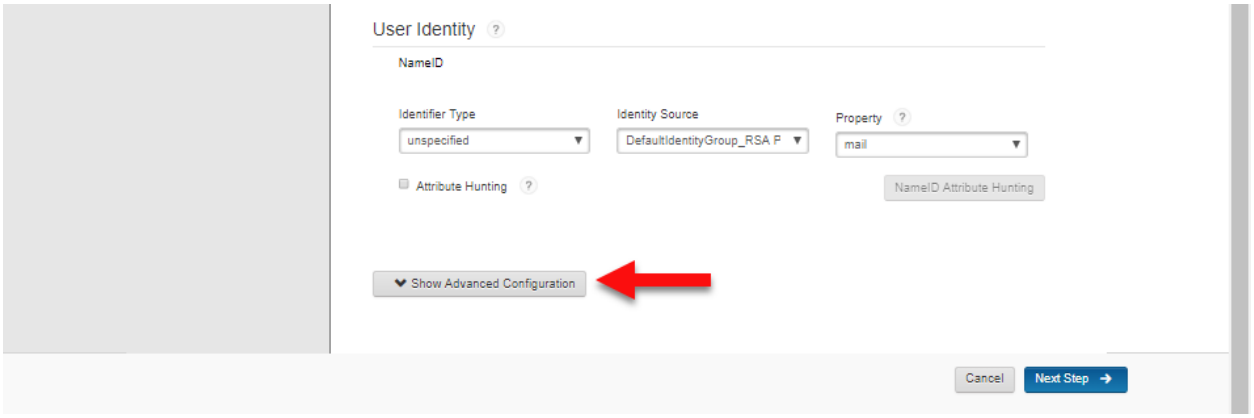
```
https://<fqdn>:<port>/sso-connect/saml/sso
```

b. Enter the **Service Provider Entity ID** in the format below and changing <*fqdn*> and <*port*> to match your Keeper SSO Connect deployment.

```
https://<fqdn>:<port>/sso-connect
```

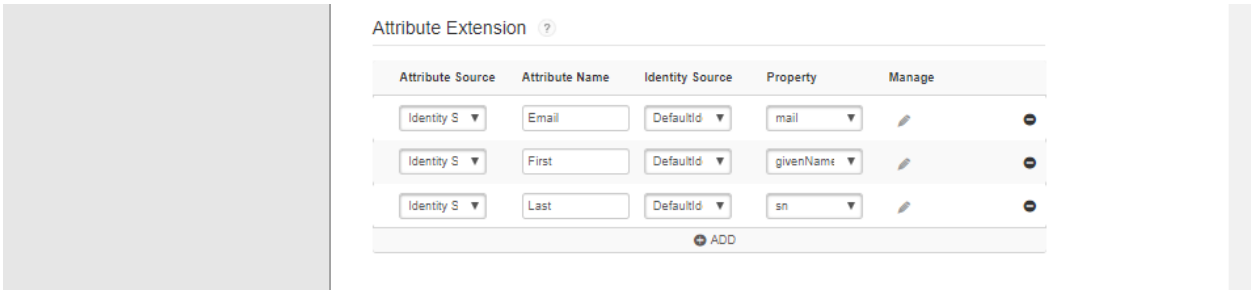
Note: If the values for ACS URL and SP Entity ID are not known, enter placeholder values so that you can continue with the configuration. After you have configured the SP, return to this section and input the correct values.

6. Configure the User Identity settings and click to **Show Advanced Configuration**.



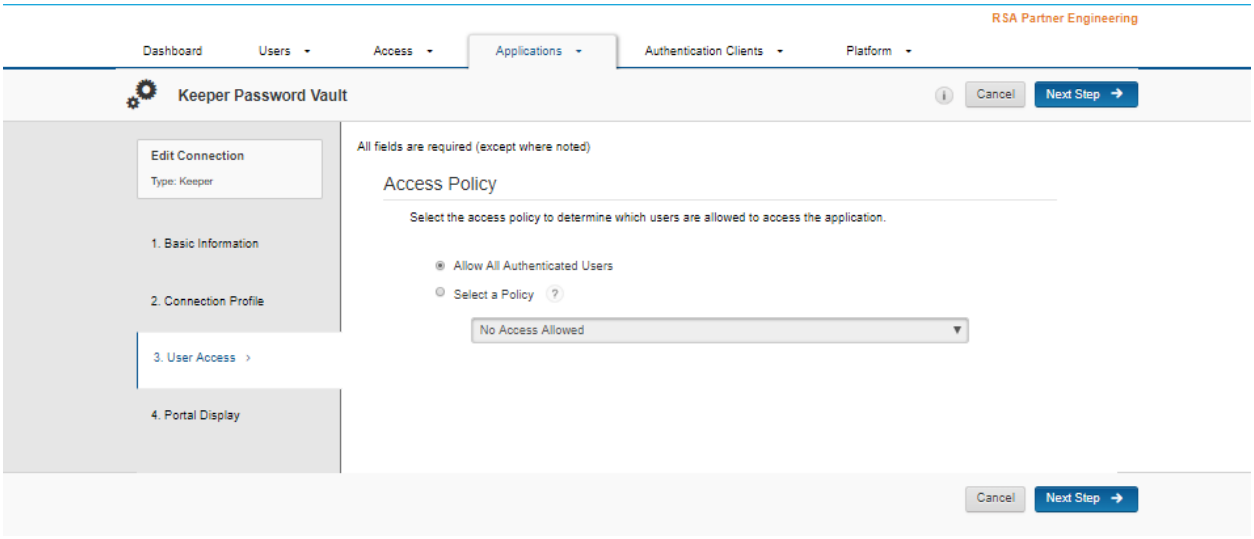
a. **Identifier Type**: Set to unspecified.
b. **Identity Source**: Choose your identity source.
c. **Property**: Set to the identity source attribute which contains the Keeper Security userid.

7. Configure Attribute Extensions and click **Next Step**.

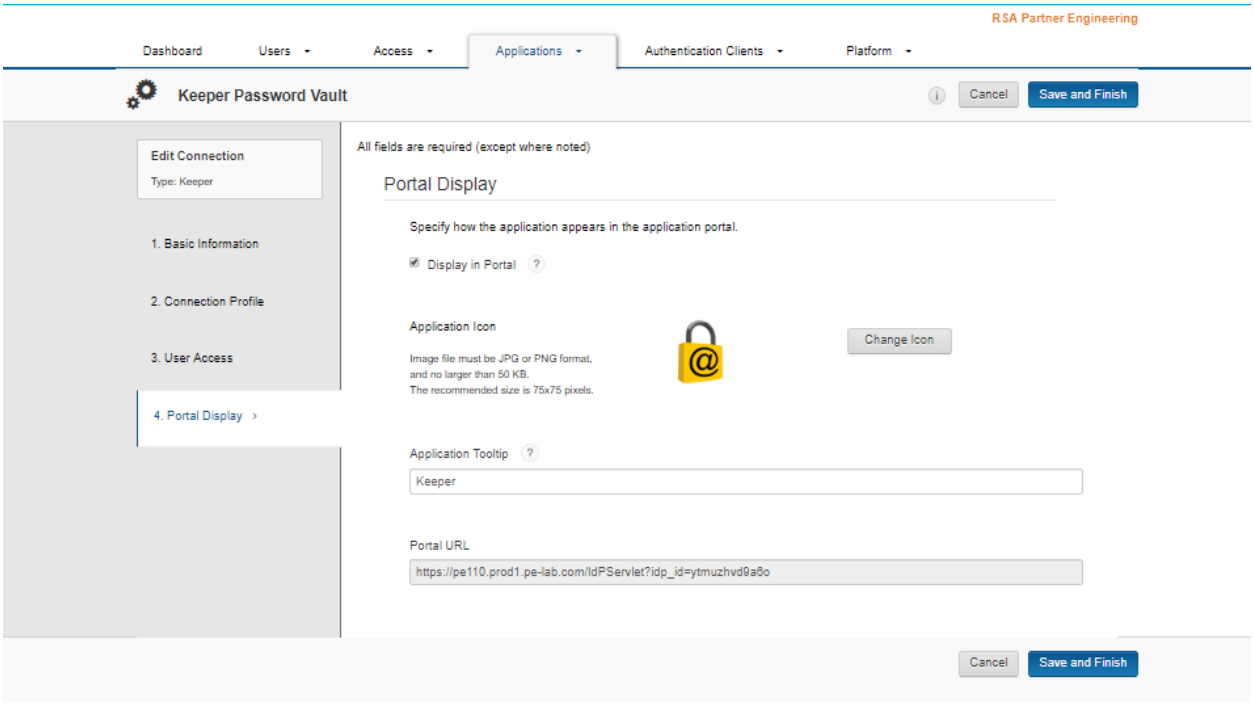


a. Add extension with Attribute Name **Email** with your **Identity Source** and Property **mail**.
b. Add extension with Attribute Name **First** with your **Identity Source** and Property **givenName**.
c. Add extension with Attribute Name **Last** with your **Identity Source** and Property **sn**.

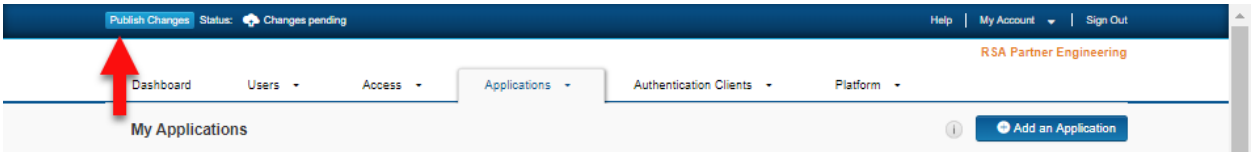
8. Configure Access Policy settings and click **Next Step**.



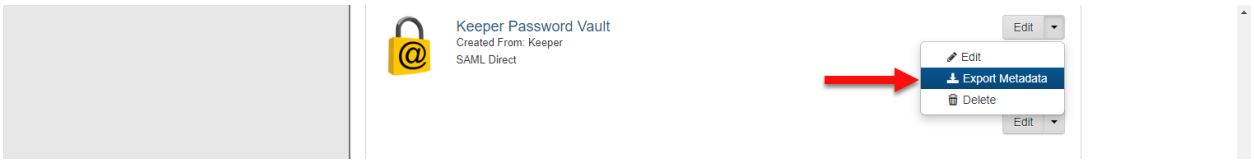
9. Configure Portal Display settings and click **Save and Finish**.



10. Click **Publish Settings**.



11. Click **Applications > My Applications**, locate the Keeper application, and click to **Export Metadata**.



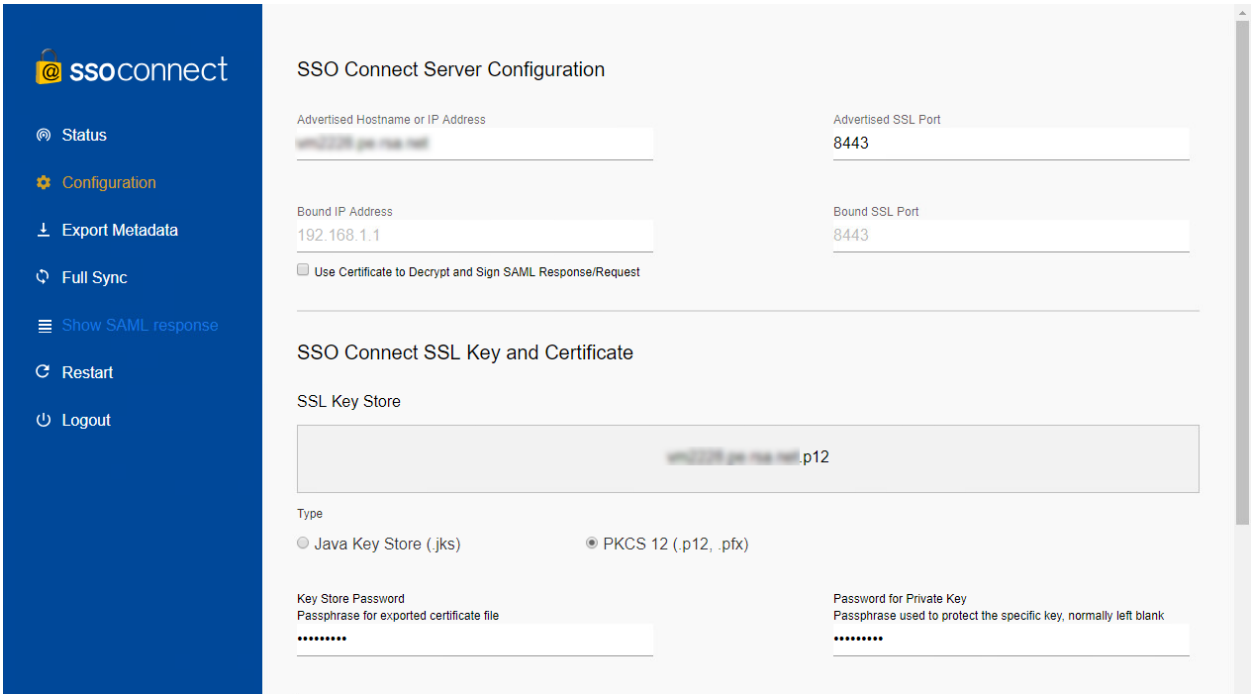
Keeper Password Manager

Perform these steps to configure Keeper Password Manager as an SSO Agent SAML SP to RSA Cloud Authentication Service.

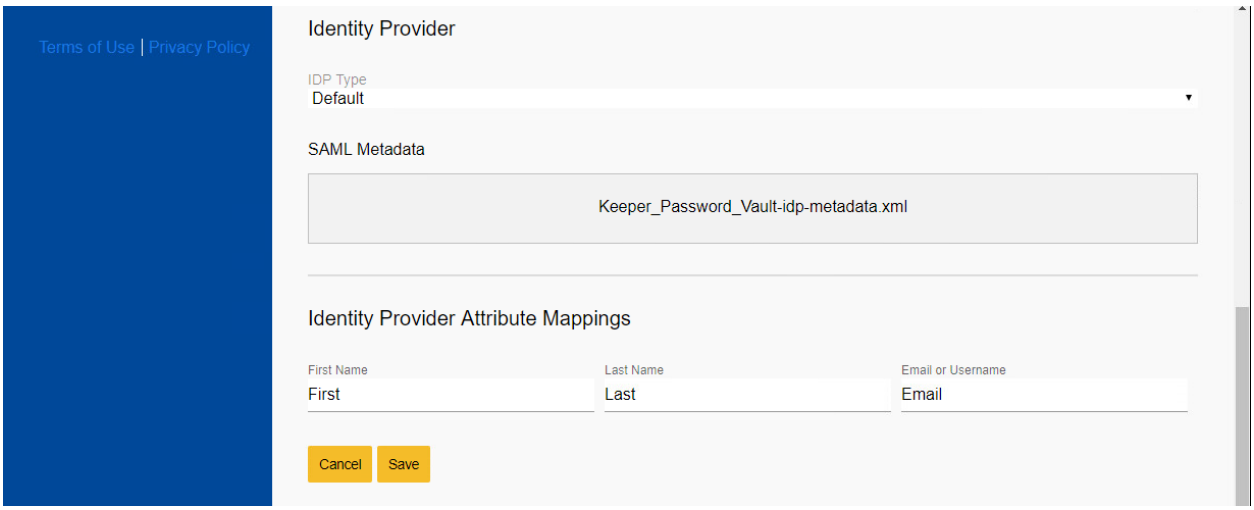
Procedure

1. Install Keeper Security SSO Connect and sign in using a Keeper Administrator account.

2. Open the **Configuration** tab, configure the **SSO Connect Server Configuration** settings and scroll down to the **Identity Provider** section.

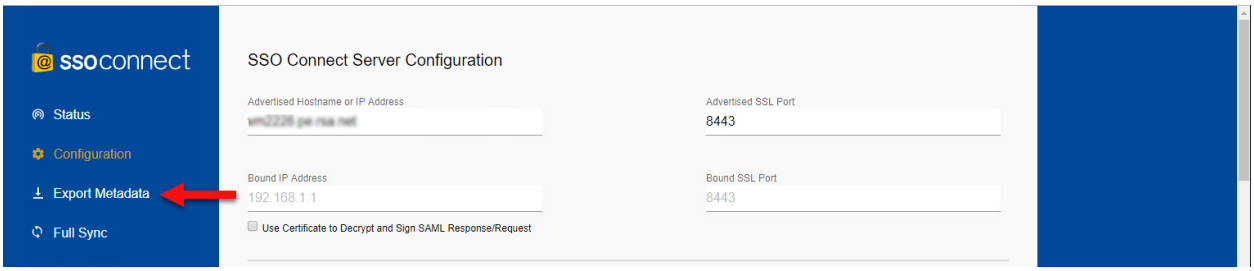


3. Set the IDP Type to **Default**, upload the **SAML Metadata** file you downloaded in the previous section and click to **Save**.

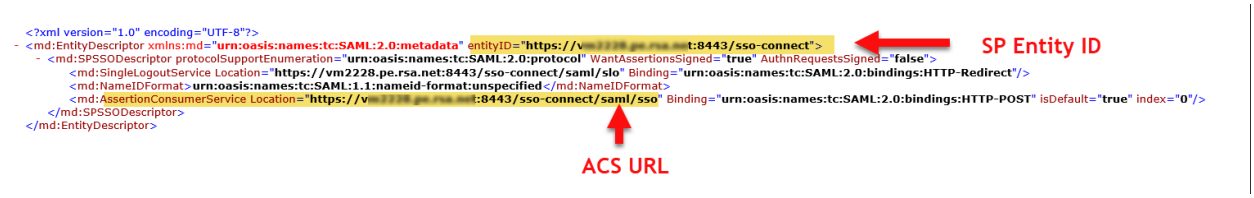


If you left placeholder values in the RSA Cloud Administration Console then follow the remaining steps. Otherwise, configuration is complete.

4. Click to Export Metadata from Keeper SSO Connect.



5. Open the metadata file with a text editor and locate the ACS URL and SP Entity ID values.



6. Return to the RSA Cloud Administration Console and replace the placeholder values with the correct ones and publish the changes.

Configuration is complete.

Return to the main page for more integration related information.