RSA SecurID Access SAML Configuration for Salesforce Desk

Last Modified: March 4, 2016

Salesforce Desk offers online customer service, support ticket, and help desk software to improve customer satisfaction. Sales and support teams can share a complete view of the customer with Desk.com.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Salesforce Desk Business Plus edition.
- Verify the RSA SecurID Access user account. Refer to the User, Rule, and Policy section of the RSA SecurID Access Manual.

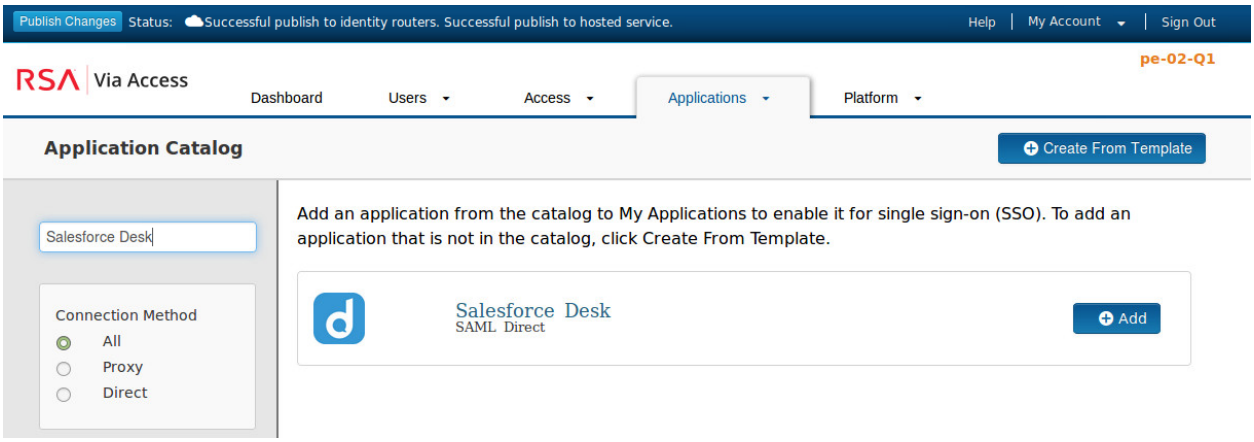
Procedure

1. Add the Application in RSA SecurID Access
2. Configure Salesforce Desk to Use RSA SecurID Access as an Identity Provider

Add the Application in RSA SecurID Access

Procedure

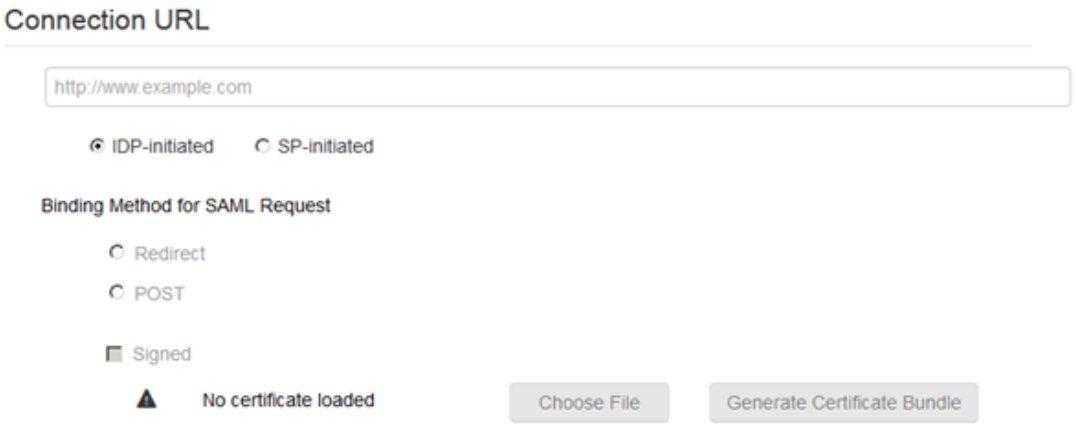
1. In the RSA SecurID Access Administration Console, click **Applications > Application Catalog**.
2. From the list of applications, click **+Add** for the SAML application that you wish to add.



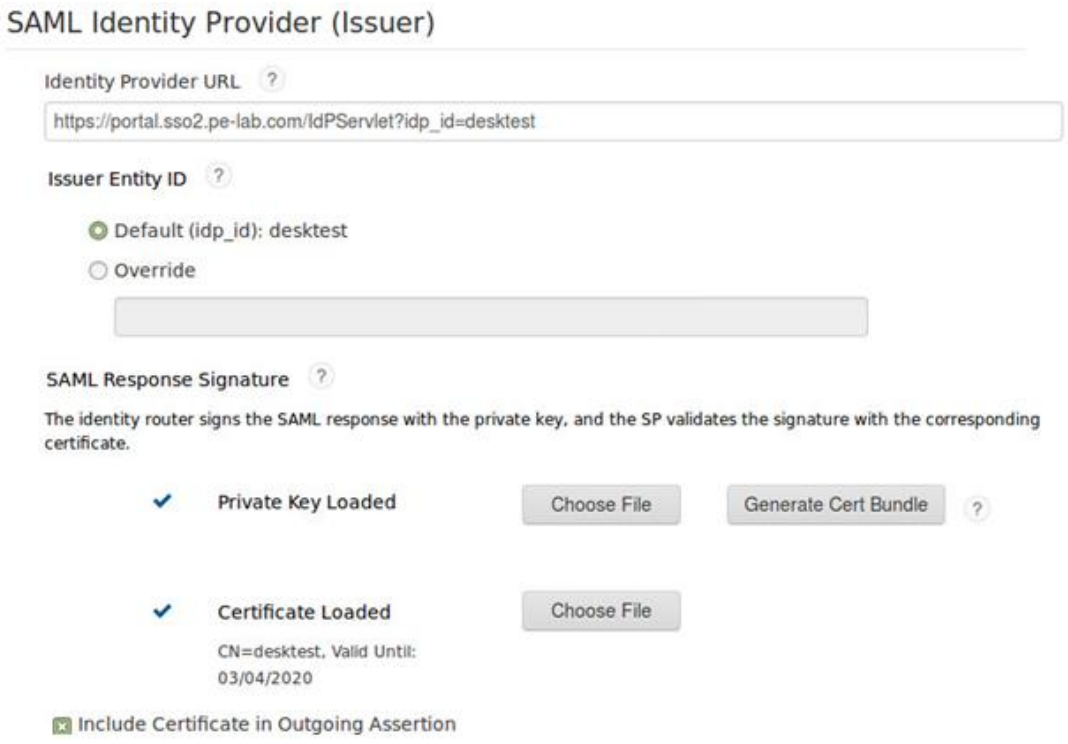
3. On the Basic Information page, specify the application name and click **Next Step**.

> **Note: The following IDP-initiated configuration works for both IDP-initiated and SP- initiated connections.**

4. On the Connection Profile page, choose **IDP –initiated** and leave the URL blank.

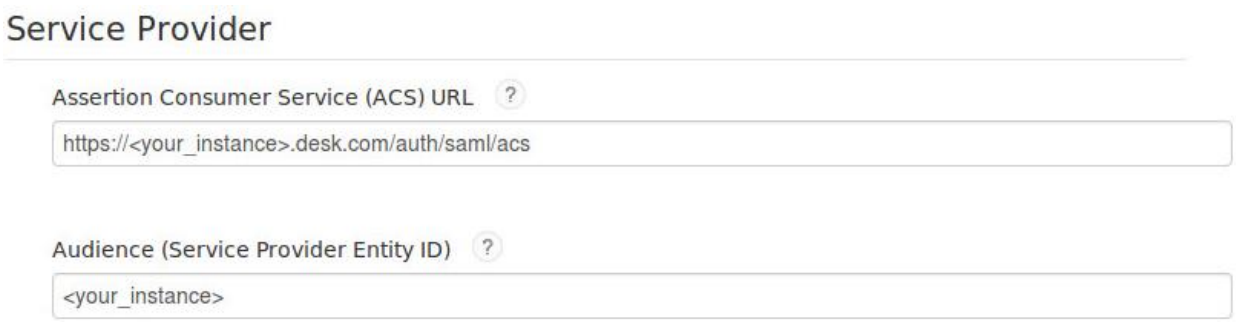


5. Scroll down to the **SAML Identity Provider (Issuer)** section.



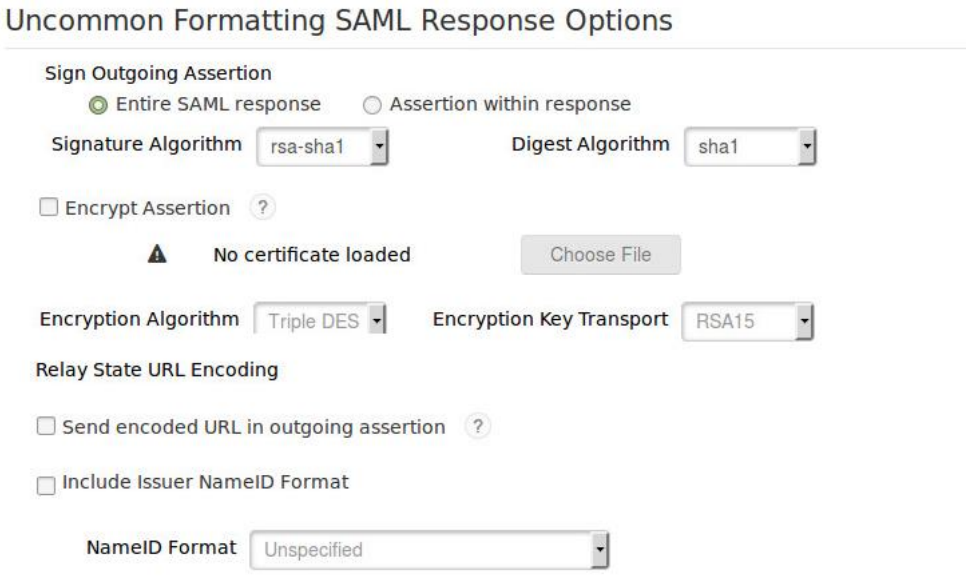
   a. In the **Identity Provider URL** field, copy the URL which will be needed later to configure the Salesforce Desk.
   b. Select **Choose File** and upload the RSA SecurID Access private key.
   c. Select **Choose File** and upload the RSA SecurID Access public certificate.
   d. Select the check box **Include Certificate in Outgoing Assertion**.

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



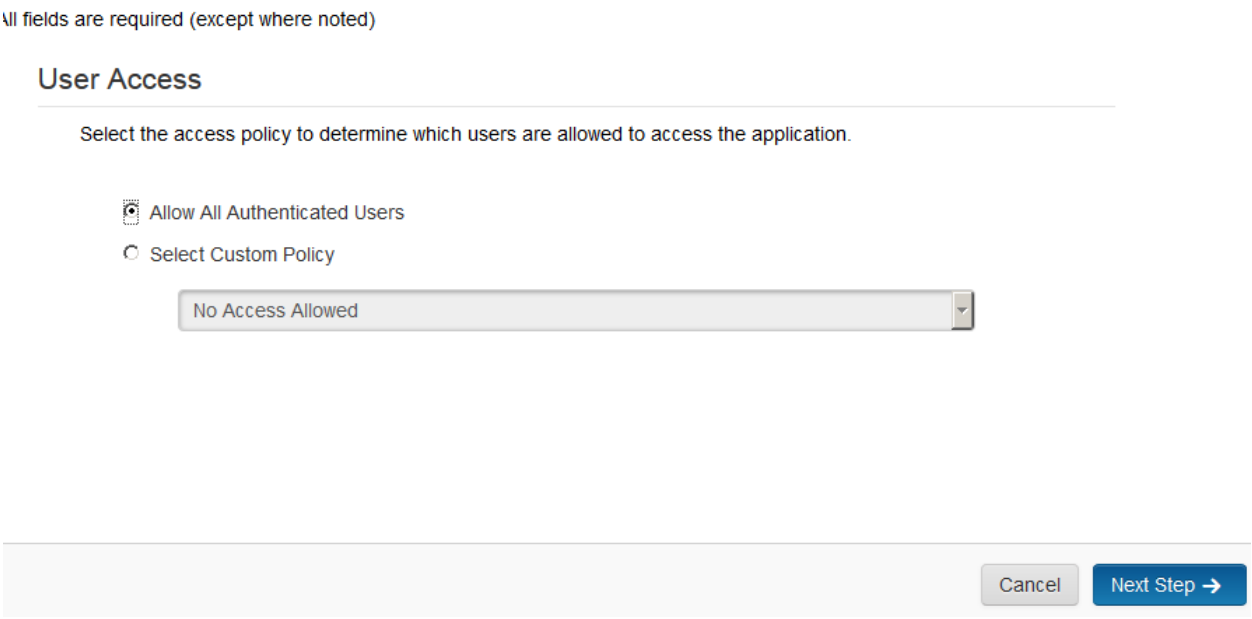
   a. In the **Assertion Consumer Service (ACS) URL** field, replace **<your_instance>** with your site's subdomain. Example: https://pe-lab.desk.com/auth/saml/acs
   b. In the **Audience (Service Provider Entity ID)** field, replace **<your_instance>** with your site's subdomain. Example: **pe-lab**.
7. Scroll down to the **User Identity** section. Set the **Identifier Type** to **Email Address** and **Property** to **mail**.

8. Click **Show Advanced Configuration** and scroll down to **Uncommon Formatting SAML Response Options**.
9. Uncheck **Send encoded URL in outgoing assertion**.

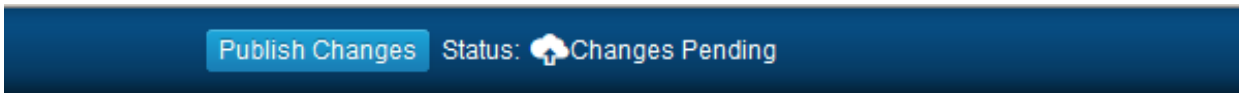


10. Click **Next Step**.

11. On the **User Access** page, select the desired user policy from the drop down list.



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



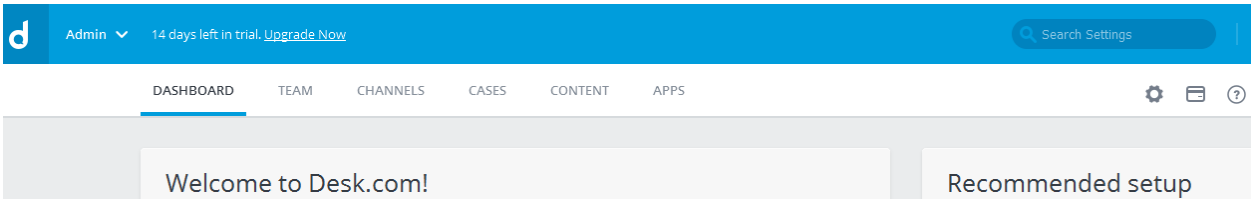
Next Steps

Configure Salesforce Desk to Use RSA SecurID Access as an Identity Provider

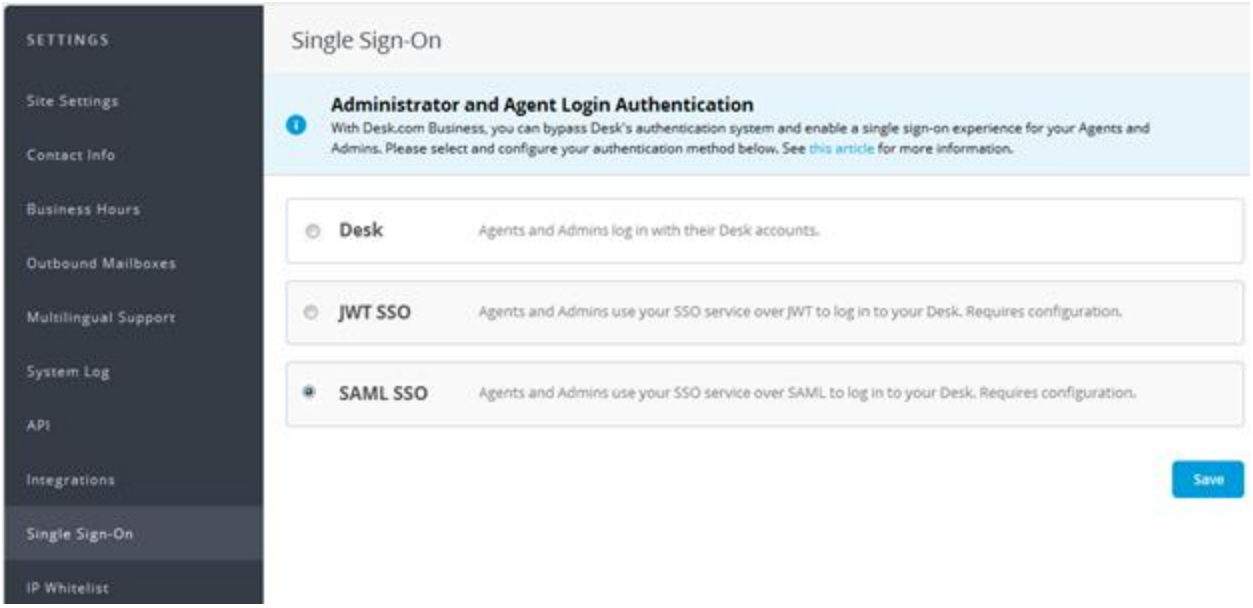
Configure Salesforce Desk to Use RSA SecurID Access as an Identity Provider

Procedure

1. Login to Salesforce Desk with an admin account. https://<your_instance>.desk.com/web/agent
2. Select the list icon in the upper left corner and choose **Admin**.
3. On the Admin Dashboard select the gear icon in the upper right corner.

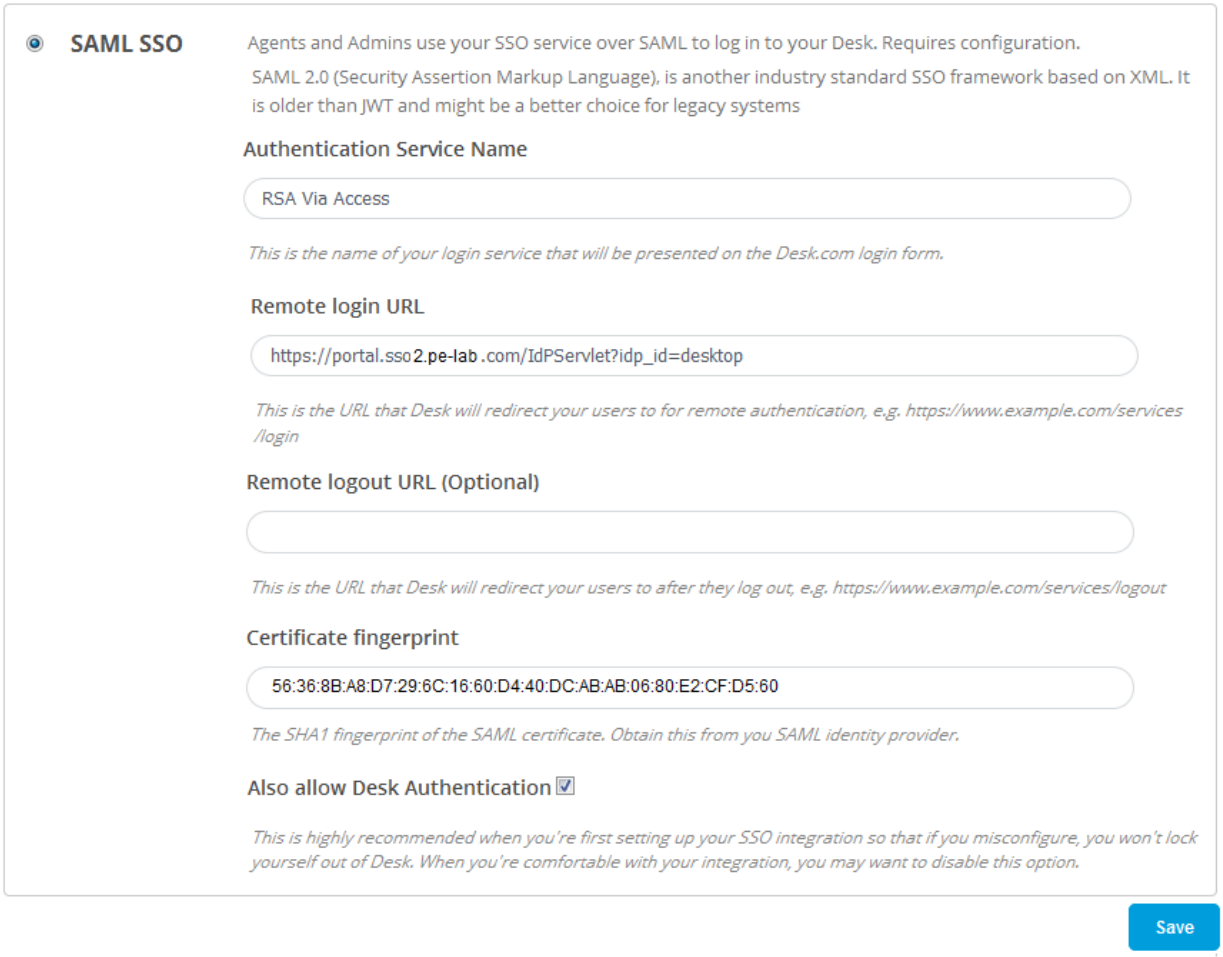


4. Under SETTINGS, select **Single Sign-On**.



5. Select **SAML SSO**.

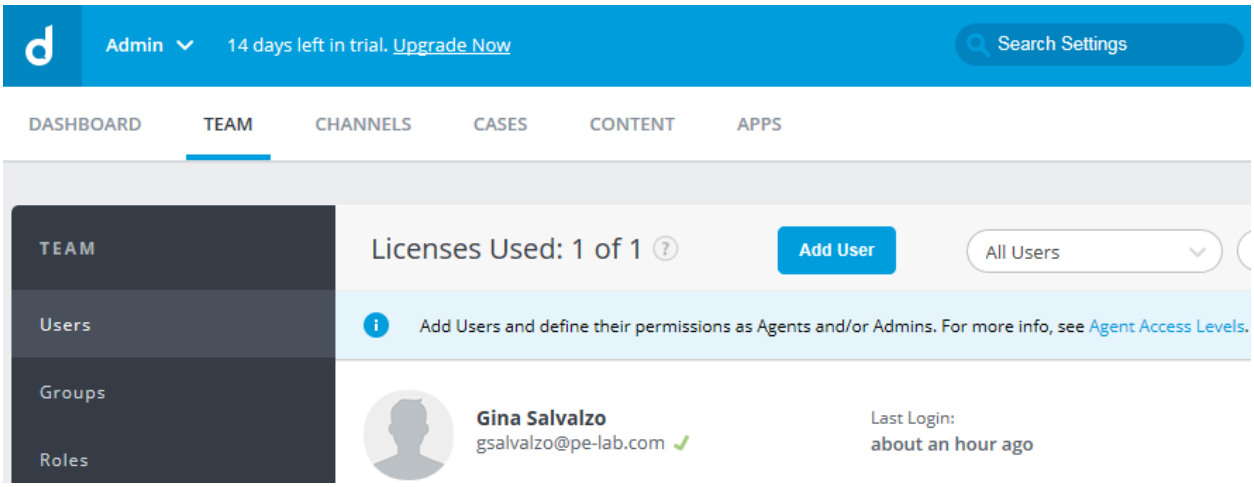
6. The SAML SSO page will open.
7. Enter **RSA SecurID Access** in the *Authentication Service Name* field.
8. Enter the Identity Provider URL from page 2 step 5 in the *Remote login URL* field.
9. Convert the RSA public certificate file **cert.pem** to a fingerprint.
   Use the following openssl command to do the conversion:
   openssl x509 –sha1 –in cert.pem –noout –fingerprint
10. Enter the fingerprint string into the *Certificate fingerprint* field.
11. Click **Save**.



12. From the top menu select **TEAM** to add a user.
13. Select **Add User**.

> **Note: The user's email address must match the RSA SecurID Access single sign-on user's email address.**

14. The user will be sent an email. The user must click the validation link in the email to active the new user account.



GLS