

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.

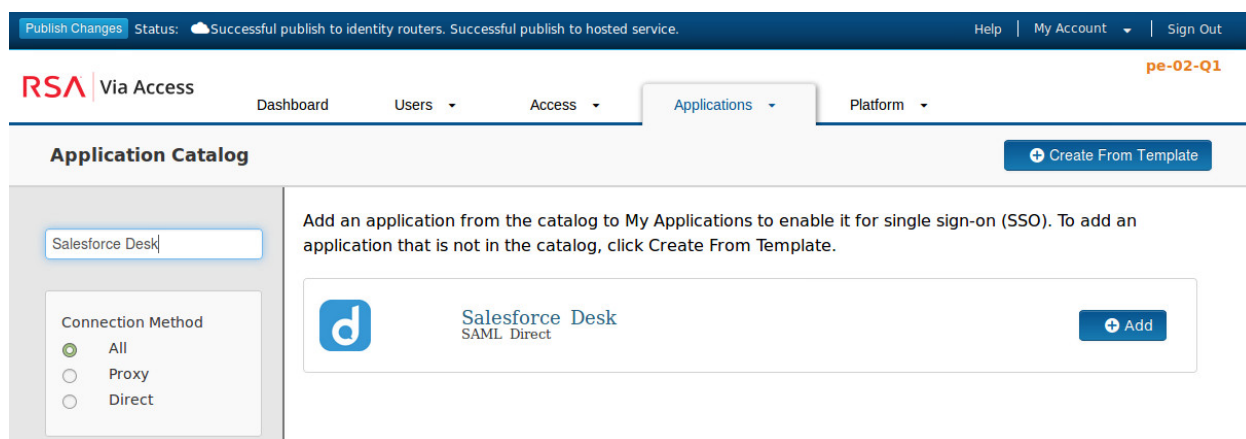
Procedure

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.

Connection URL


IDP-initiated SP-initiated

Binding Method for SAML Request

Redirect


POST


Signed

 No certificate loaded

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


SAML Identity Provider (Issuer)

Identity Provider URL 


Issuer Entity ID 

Default (idp_id): desktest

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 Loaded 

Certificate Loaded

CN=desktest, Valid Until:
03/04/2020

Include Certificate in Outgoing Assertion

- 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.

Service Provider

Assertion Consumer Service (ACS) URL ?

https://<your_instance>.desk.com/auth/saml/acs

Audience (Service Provider Entity ID) ?

<your_instance>

- 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**.

User Identity ?

NameID

Identifier Type

Email Address

Identity Source

AD

Property ?

mail

Attribute Hunting ?

NameID Attribute Hunting

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

Uncommon Formatting SAML Response Options

Sign Outgoing Assertion

Entire SAML response Assertion within response

Signature Algorithm

Digest Algorithm

Encrypt Assertion ?

▲ No certificate loaded

Choose File

Encryption Algorithm

Encryption Key Transport

Relay State URL Encoding

Send encoded URL in outgoing assertion ?

Include Issuer NameID Format

NameID Format

10. Click **Next Step**.

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

All fields are required (except where noted)

User Access

Select the access policy to determine which users are allowed to access the application.

Allow All Authenticated Users

Select Custom Policy

No Access Allowed

Cancel

Next Step →


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.

Publish Changes


Status:  Changes Pending

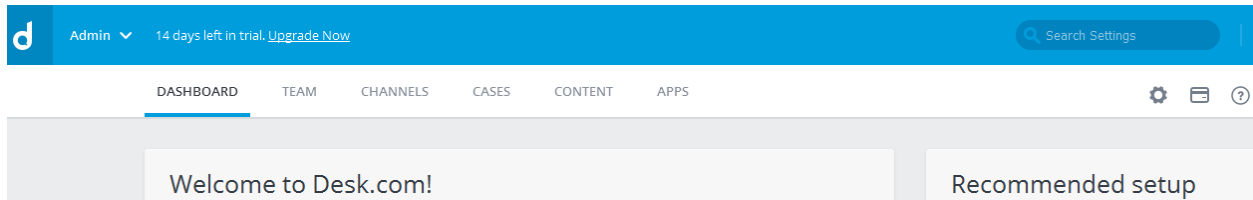
Next Steps

[Configure Salesforce Desk to Use RSA SecurID Access as an Identity Provider](#)

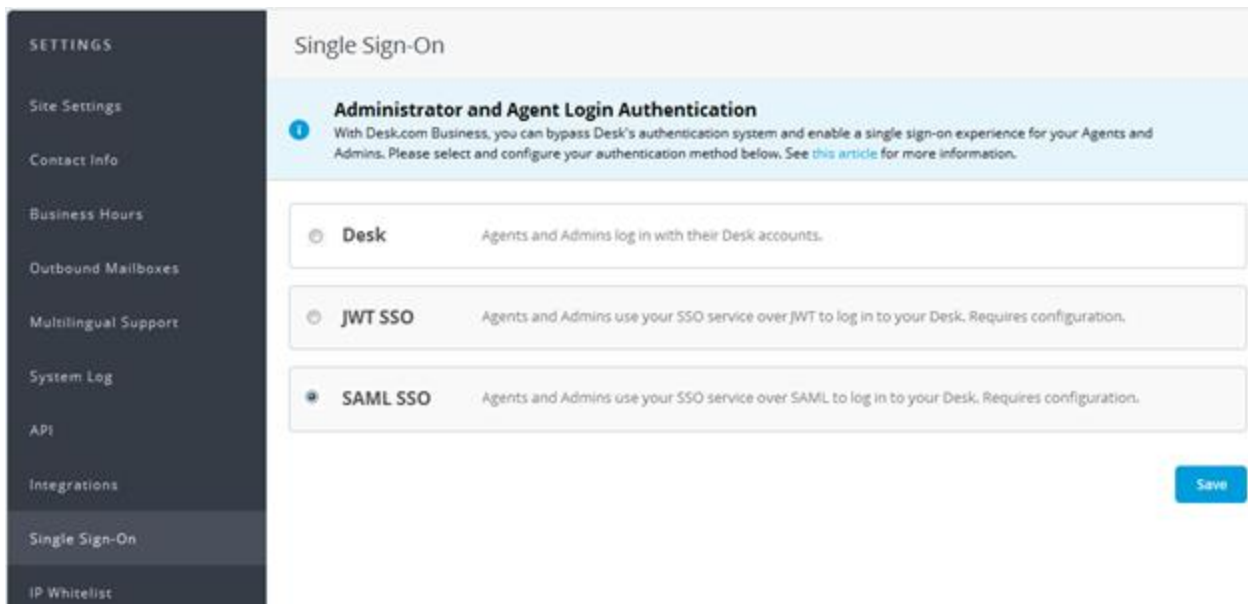
Configure Salesforce Desk to Use RSA SecurID Access as an Identity Provider

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**.

SAML SSO Agents and Admins use your SSO service over SAML to log in to your Desk. Requires configuration.
SAML 2.0 (Security Assertion Markup Language), is another industry standard SSO framework based on XML. It is older than JWT and might be a better choice for legacy systems

Authentication Service Name

This is the name of your login service that will be presented on the Desk.com login form.

Remote login URL

This is the URL that Desk will redirect your users to for remote authentication, e.g. https://www.example.com/services/login

Remote logout URL (Optional)

This is the URL that Desk will redirect your users to after they log out, e.g. https://www.example.com/services/logout

Certificate fingerprint

The SHA1 fingerprint of the SAML certificate. Obtain this from you SAML identity provider.


Also allow Desk Authentication

This is highly recommended when you're first setting up your SSO integration so that if you misconfigure, you won't lock yourself out of Desk. When you're comfortable with your integration, you may want to disable this option.

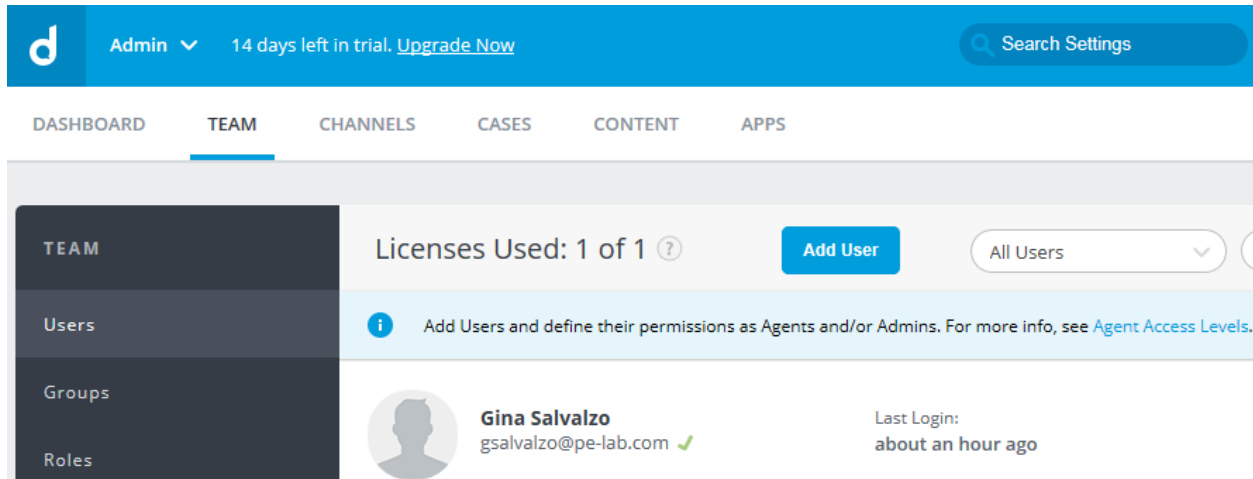
Save

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 activate the new user account.



The screenshot shows the Admin console interface. At the top, there is a blue header with the 'd' logo, 'Admin' with a dropdown arrow, '14 days left in trial. Upgrade Now', and a 'Search Settings' button. Below the header is a navigation bar with tabs for DASHBOARD, TEAM (selected), CHANNELS, CASES, CONTENT, and APPS. The main content area is divided into a left sidebar and a main panel. The sidebar has 'TEAM' selected, with sub-items 'Users', 'Groups', and 'Roles'. The main panel shows 'Licenses Used: 1 of 1' with a help icon, an 'Add User' button, and a dropdown menu set to 'All Users'. Below this is an information message: 'Add Users and define their permissions as Agents and/or Admins. For more info, see Agent Access Levels.' The user list shows one user: 'Gina Salvalzo' with email 'gsalvalzo@pe-lab.com' and a green checkmark. To the right, it says 'Last Login: about an hour ago'.