

RSA SecurID Access Delegated Authentication Configuration for Salesforce



Last Modified: October 26, 2015

Salesforce is a customer relationship management (CRM) solution for sales.

About Delegated Authentication

- When a user tries to log in, Salesforce validates the username and checks the user's permissions and access settings. If the user is enabled for SSO, a Web services call is made to RSA SecurID Access to validate the username and password. If they are valid, the user proceeds to the application. If they are not valid, the user is informed that his or her username and password combination is invalid.
- Delegated Authentication supports SP-initiated style single sign-on only.
- Delegated Authentication does not allow for step-up authentication.

Before You Begin

- Acquire an administrator account to both RSA SecurID Access and Salesforce.
- Enable the Delegated Authentication feature on your Salesforce instance. You may need to open a help ticket with Salesforce support to enable Delegated Authentication.
- Ensure the RSA SecurID Access Portal is configured with a trusted SSL certificate.
- Verify the RSA SecurID Access user accounts.
- Verify Salesforce users are enabled for SSO.

Procedure

1. [Add the Application in RSA SecurID Access](#)
2. [Configure Salesforce to Use RSA SecurID Access for Delegated Authentication](#)

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, locate the **Salesforce DelegatedAuth** connector and click **+Add**.

The screenshot shows the RSA Via Access Administration Console. The top navigation bar includes 'RSA Via Access', 'Dashboard', 'Users', 'Access', 'Applications', and 'Platform'. The 'Applications' tab is active. The main content area is titled 'Application Catalog' and features a search bar containing 'salesf'. Below the search bar is a 'Connection Method' filter with radio buttons for 'All', 'Proxy', and 'Direct'. The main list displays three application entries, each with a Salesforce logo, a name, a connection method, and an '+ Add' button. The 'Salesforce DelegatedAuth' entry is highlighted, and a mouse cursor is clicking its '+ Add' button.

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

The screenshot shows the 'Basic Information' page for the 'Salesforce.com (Delegated Authentication)' application. The top navigation bar is the same as the previous screenshot. The page title is 'Salesforce.com (Delegated Authentication)'. On the left, there is a sidebar with 'Edit Connection' and 'Type: Salesforce DelegatedAuth'. Below this is a list of steps: '1. Basic Information >', '2. Configuration', '3. User Access', and '4. Portal Display'. The main form area has a heading 'Basic Information' and a note 'All fields are required (except where noted)'. It contains a 'Name' field with the value 'Salesforce.com (Delegated Authentication)', a 'Description (optional)' text area, and a 'Disabled' checkbox. At the bottom right, there are 'Cancel' and 'Next Step' buttons, with a mouse cursor clicking the 'Next Step' button.

4. On the Configuration page, set the **User Store Setup** settings, take note of the **Identity Provider URL** and click **Next Step**.

RSA Via Access RSA Partner Engineering

Dashboard Users Access Applications Platform

Salesforce.com (Delegated Authentication) Cancel Next Step →

Edit Connection
Type: Salesforce DelegatedAuth

1. Basic Information

2. Configuration >

3. User Access

4. Portal Display

All fields are required (except where noted)

User Store Setup

User Store: PE_AD Property: mail

Setup

Identity Provider URL: https://portal.example.com/DelegatedAuthenticationServlet?idp_id=1920zt0z823a5

Verify Certificates

User Name Transformation Configuration

Remove matching string

Regular Expression

Cancel Next Step →

5. On the User Access page, choose **Allow All Authenticated Users** and click on **Next Step**.

RSA Via Access GsLab

Dashboard Users Access Applications Platform

Twitter Cancel Next Step →

Add Connection
Type: Twitter

1. Basic Information

2. Branded Settings

3. User Access >

4. Portal Display

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 →

6. On the Portal Display page, uncheck **Display in Portal** checkbox and click **Save and Finish**.

RSA Via Access RSA Partner Engineering

Dashboard Users Access Applications Platform

Salesforce.com (Delegated Authentication) Cancel Save and Finish

Edit Connection
Type: Salesforce DelegatedAuth

1. Basic Information
2. Configuration
3. User Access
4. Portal Display >

All fields are required (except where noted)


Portal Display

Specify how the application appears in the end-user portal.

Display in Portal ?

Application Icon

Image file must be JPG or PNG format, and no larger than 50 KB. The recommended size is 75x75 pixels.



Change Icon

Application Tooltip ?

Salesforce.com (Delegated Authentication)

Portal URL ?

https://portal.example.com/DelegatedAuthenticationServlet?idp_id=192ozt0z823a5

Cancel **Save and Finish**

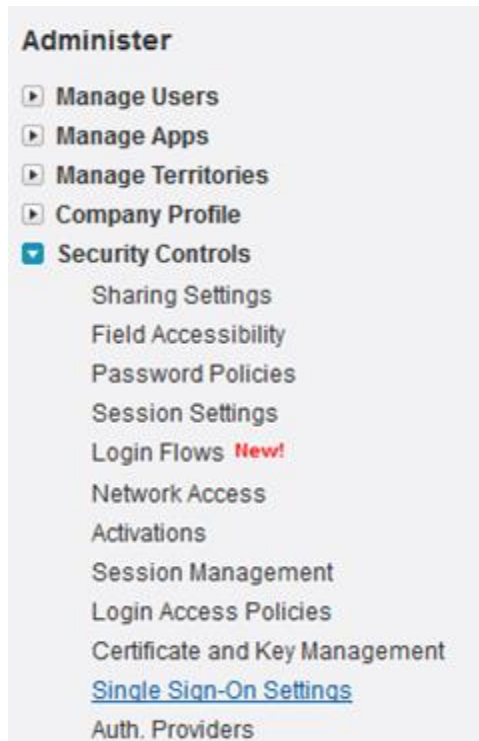
7. Click **Publish Changes**.

Publish Changes Status:  Changes Pending

Configure Salesforce to Use RSA SecurID Access for Delegated Authentication

Procedure

1. Login to the Salesforce administration console, in the **Administer** tool bar, select **Security Controls > Single Sign-On Settings**.

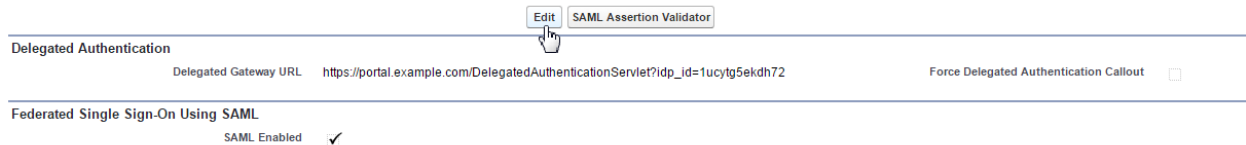


2. Click **Edit** to edit the Delegated Authentication settings.

Single Sign-On Settings

Configure single sign-on in order to authenticate users in salesforce.com from external environments. Your organization has the following options available for single sign-on:

- Delegated authentication is a single sign-on method that uses a Web service call sent from salesforce.com to an endpoint.
- Federated authentication, a single sign-on method that uses SAML assertions sent to a Salesforce endpoint.



3. Enter the Identity Provider URL from the RSA SecurID Access console (on page 3 of this guide) into the **Delegated Gateway URL** field and click **Save**.

Single Sign-On Settings

Delegated Authentication

Delegated Gateway URL:
Force Delegated Authentication Callout

Federated Single Sign-On Using SAML

SAML Enabled

Configure Salesforce User

1. In the **Administer** tool bar, select **Manage Users > Users**.

All Users

[Help for this Page](#)

[Expand All](#) | [Collapse All](#)

Salesforce1 Setup New!

[Force.com Home](#)

Administer

Manage Users

[Users](#)

[Mass Email Users](#)

View: All Users [Edit](#) | [Create New View](#)

[A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#) [Other](#) [All](#)

<input type="checkbox"/>	Action	Full Name ↑	Alias	Username	Last Login	Role	Active	Profile	Manager
<input type="checkbox"/>	Edit	Salvalzo, Alicia	AS	alicia@pe-lab.com	11/25/2014 1:01 PM		<input checked="" type="checkbox"/>	Standard User	
<input type="checkbox"/>	Edit	Salvalzo, Gina	GSalv	gsalvalzo@pe-lab.com	11/25/2014 1:27 PM		<input checked="" type="checkbox"/>	System Administrator	

2. Click **New User**.
3. Complete all the required fields.

General Information

First Name

Last Name

Alias

Email

Username

Community Nickname

Title

Company

Department

Division

Role

User License

Profile

Active

Marketing User

Offline User

Sales Anywhere User

Mobile User

Mobile Configuration

Accessibility Mode

4. Select **Save**.