


Configure the Conga Composer Connected App

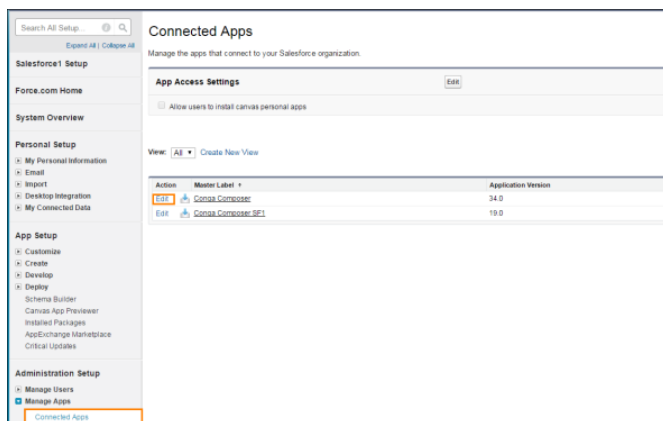
Administrators can pre-approve users to connect via OAuth when running solutions. This method masks the session ID and URL when using Visualforce[®] buttons, and prevents pop-up authorization requests on mobile devices when running Composer solutions on Salesforce1[®].

 In addition to configuring Conga Composer[®] as a Connected App, you will want to [Create Conga Composer OAuth buttons](#) (or update existing non-OAuth buttons) to launch your Composer solutions. This is not required in Salesforce Classic[®], but it is required in Salesforce Lightning[®].

To configure Conga Composer as a connected app to use OAuth:

Media, iframe, embed and object tags are not supported inside of a PDF.

1. Navigate to Setup > Manage Apps > Connected Apps > Conga Composer.



2. Click Edit.
3. Change the Permitted Users picklist to Admin approved users are pre-authorized.

Connected App
Conga Composer

Connected App Edit

Conga composer Version 34
Description Conga Composer makes it easy for Salesforce users to create sophisticated documents and reports

Basic Information

Start URL

OAuth policies

Permitted Users **Admin approved users are pre-authorized**

Session Level Policy

☐ High Assurance session required

Save Cancel



Admins must be pre-approved in the Connected App. If not, you may see an error message when trying to launch a Conga Composer OAuth button.

- Designate which users connect to Conga Composer via OAuth by adding Profiles (click Manage Profiles) or Permission Sets (click Manage Permission Sets).

App Info

Manage Profiles
Company Profile
Security Controls
Domain Management
Communication Templates
Translation Workbench
Data Management
Mobile Administration
Desktop Administration
Email Content Editor
Email Administration
Google Apps
Data from Administration

Build

Customize
Create
Develop
Schema Builder
Conga App Framework
Installed Packages
Application Management
Critical Updates

Deploy

Deployment Settings
Deployment Status

Monitor

System Overview
Imports
Outbound Messages
Trail-Based Monitor

App Info

This App Supports ☒ Force.com Connect

Basic Information

Info URL Start URL
Mobile Start URL

OAuth policies

Permitted users Admin approved users are pre-authorized
Image [View OAuth Logo](#)
This application has permission to Provide access to custom applications
This application has permission to Perform requests on your behalf at any time
This application has permission to Provide access to your data via the Web
This application has permission to Full access

IP Restriction Enforce IP restrictions ☐
Refresh Token Policy Refresh token is valid until revoked

Trusted IP Range for OAuth Web-server flow

Start IP address	End IP address
54.103.41.100	54.103.41.100
54.103.28.30	54.103.28.30

Profiles [Manage Profiles](#)
No profiles associated with the app

Permission Sets [Manage Permission Sets](#)
No permission sets associated with the app

Custom Attributes [View](#)
No Custom Attributes



After setting the Permitted Users to be pre-authorized, administrators can add Profiles or Permission Sets in order to specify which users are approved (also include the Sys Admin profile when setting profiles).

Pre-approved users will not see Allow or Deny prompts when accessing Composer via OAuth, and Conga Composer automatically creates a refresh token.

Users who are not part of the defined Profiles or Permission Sets will be denied access.