TextExpander Okta SCIM Configuration

This integration with Okta is currently available to customers. Contact TextExpander support to learn more. *http://smle.us/support*

Supported Features

TextExpander supports the following provisioning features:

- **Create Users**: New or existing users in Okta will be pushed to TextExpander as new users. See Known Issues for tips about possible issues with pre-existing TextExpander users.
- **Update User Attributes:** Updates to user profiles in Okta will be pushed to TextExpander.
- **Deactivate Users:** Users deactivated in Okta will be automatically deactivated in TextExpander. Deactivated users can also be re-assigned from Okta to reactivate them in TextExpander.
- **Push Groups:** Okta Groups can be mapped to create Teams in TextExpander.

The following attributes are synchronized between Okta and TextExpander:

- Email
- First Name
- Last Name

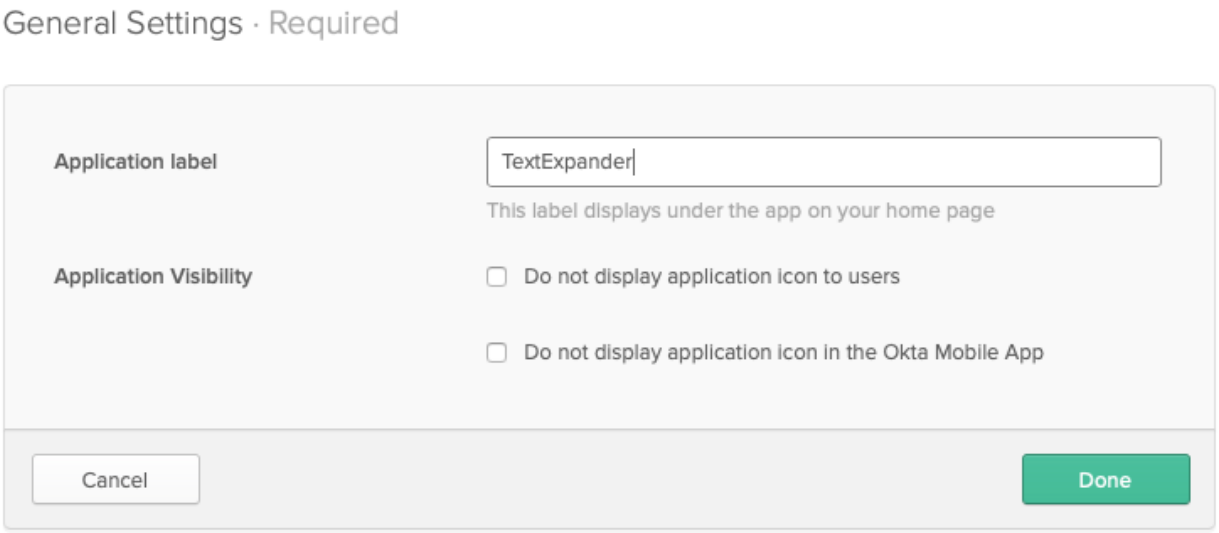
Requirements

In order to get started with SCIM provisioning, you must contact TextExpander support. Our support staff will verify that your account is ready for provisioning and will then provide the following two pieces of information:

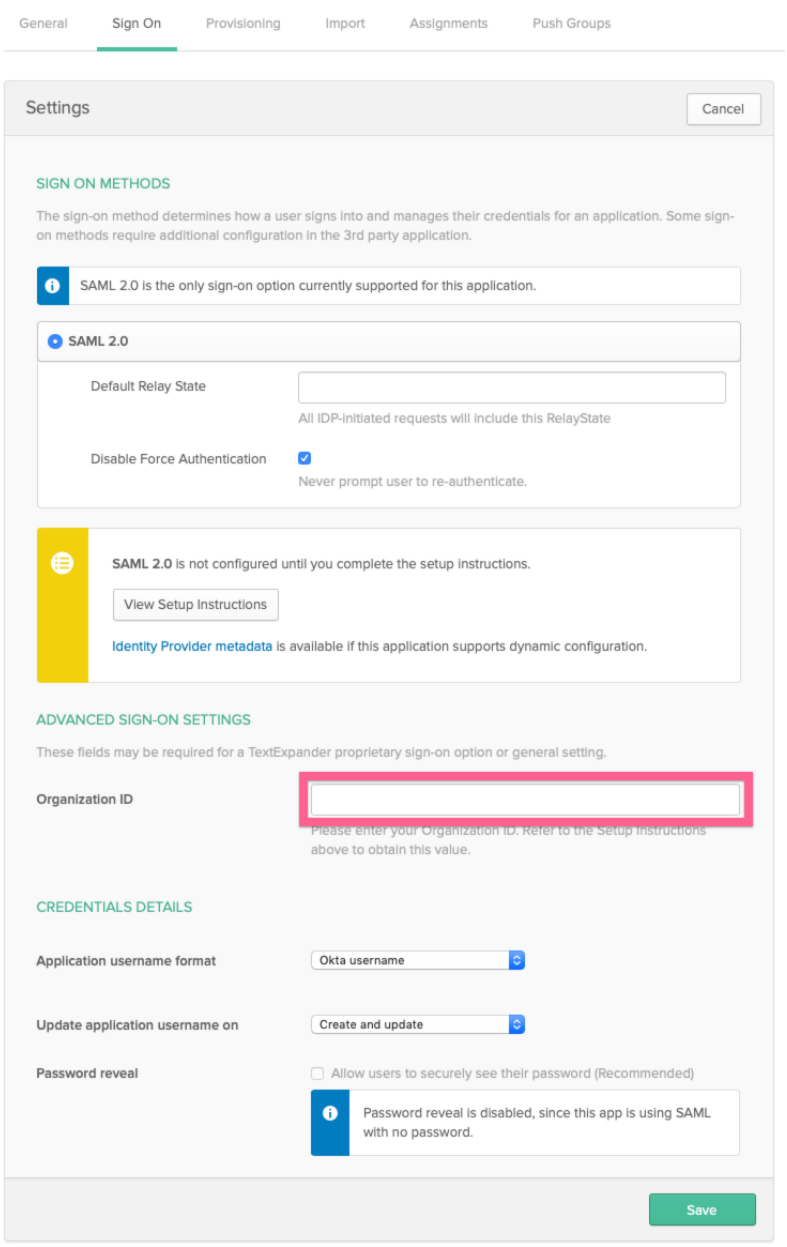
1. TextExpander Organization ID
2. SCIM Authentication Token

Configuration Steps (Step-by-Step)

1. Add the TextExpander application in Okta.
   a. From the Admin section, choose Applications from the Applications menu and then click the Add Application button.
   b. Enter “TextExpander” in the search box and click the Add button in the search results.
   c. In the General Settings section, click Done.



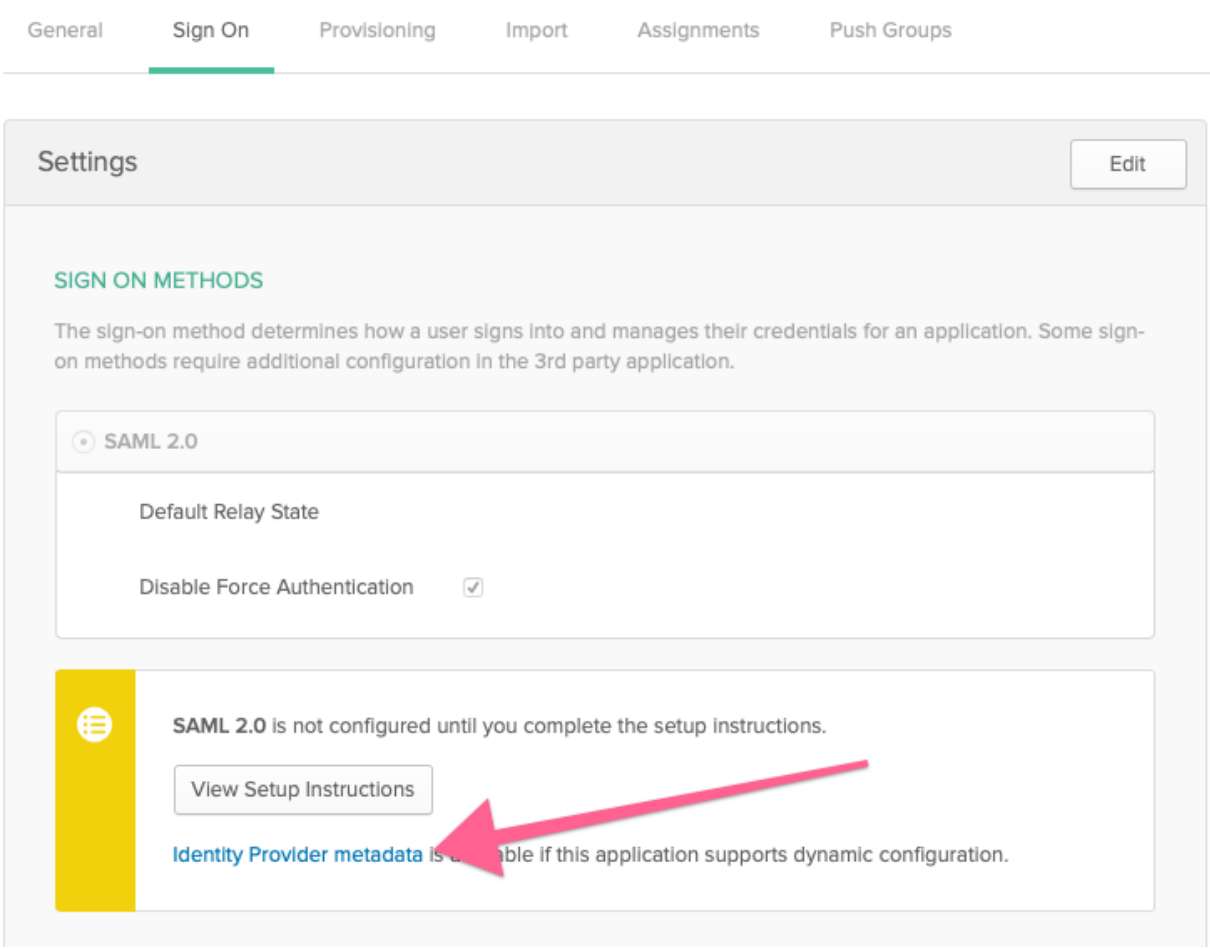
2. In the created app, click on the Sign On tab and then click on Edit to the right of the Settings header.



a. In the Sign On Settings, locate the Organization ID field and enter the Organization ID that was provided to you in #1 from Requirements, above.

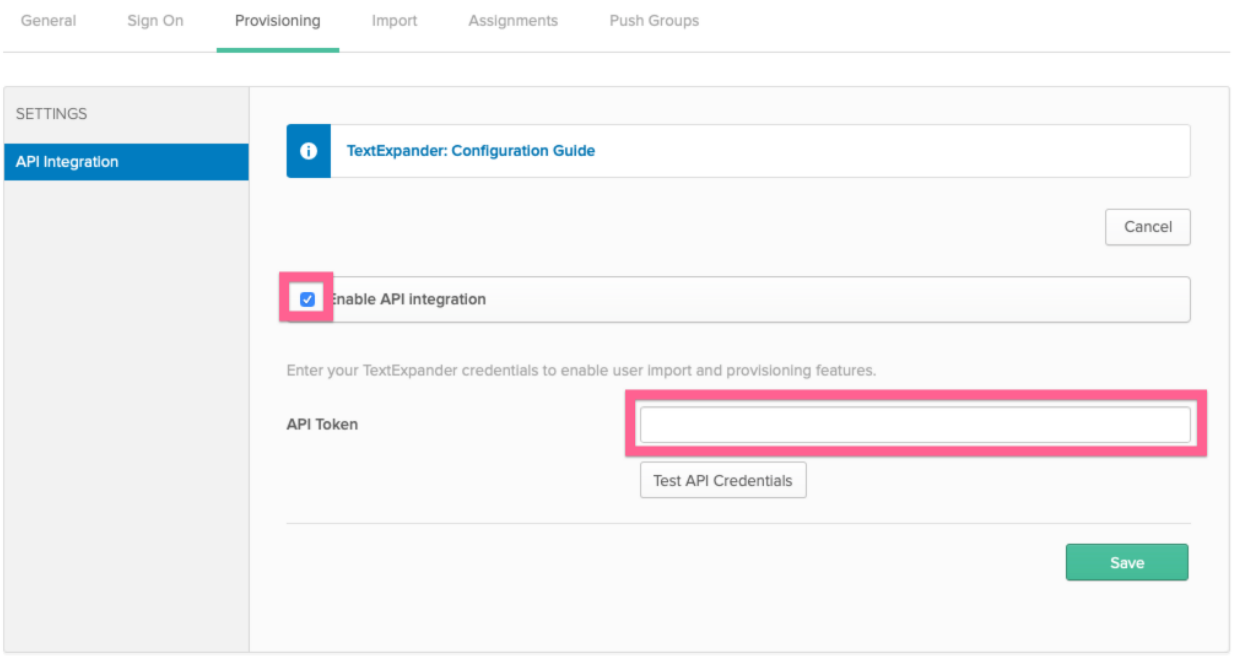
b. Click Save to save the Settings.

3. In the Sign On Settings view, click the “Identity Provider metadata” link.



a. This will open a new tab in your browser with the IdP metadata. Copy all of the text displayed in the browser and send the contents to your TextExpander contact. Once this information is received, it will be set up for you in your TextExpander organization’s account.

4. To enable SCIM, click on the Provisioning tab and then click the Configure API Integration button.



   a. In the API Integration Settings, check the Enable API Integration checkbox. This will then show the API Token field.
   b. Enter the SCIM Authentication Token (#2 from Requirements, above) in the API Token field.
   c. Click Test Credentials to check that the two systems can talk to each other. Note that this step will not work until the IdP metadata from step #7 has been sent to your TextExpander contact and configured by them in your TextExpander organization's account.
   d. Click Save to save your changes.

You're all done. You can now start provisioning users and teams.

Known Issues/Troubleshooting

- Attempting to provision a user that already exists in TextExpander but is not a member of your organization in TextExpander will result in an error, as this is a security violation. If you have an Organization Domain set up in TextExpander, the individual user should be able to add themselves into the organization via the 'Invites' section of the TextExpander web app, and then you can re-add them from Okta. Otherwise, contact TextExpander support for further assistance.
- TextExpander does not allow the removal of the last organization administrator or snippet group administrator for a specific snippet group. If you attempt to deactivate the user, the user will no longer appear as a member in Okta, but will remain active in TextExpander. Okta will show an error in the SCIM log.