Okta (SSO and User Provisioning)

11/27/2026 3:33 pm MST

Single Sign On (SSO) is available for DocBoss. If enabled, users with the company domain will be redirected to their identity provider to sign in to access DocBoss. The instructions below outline how to set up SSO with DocBoss when using **Okta** as the identity provider.

Requirements

Typically, DocBoss Support will provide the following:

- Single Sign-On URL (Recipient URL or Destination URL)
- Audience Restriction URL
- SCIM connector base URL: https://system.docboss.com/scim/v2/ [system2, 3 …]
- Instructions on how to get a token
- The list of fields for creating/updating user requests (only needed if using SCIM protocol)
    - **username** [required] – This must be an email address within the SSO domain
    - **user. givenName** [required]
    - **user. familyName** [required]
    - **user.title** – This value is saved as the **Title** field for the user in DocBoss
    - **user.timezone** - This value is saved as user's time zone in DocBoss. It must exactly match one of the DocBoss time zone values, for example America/Toronto (Ontario, Quebec) or America/Edmonton (Alberta). If it is not sent or does not match, the user gets the company or instance time zone.
    - **user.userType** – This value is saved as the user's role in DocBoss. Allowed values are Admin, Full, Reviewer, and View. If not included, user's role will be set to View.

DocBoss Support will need the following information from your IT:

- **Metadata URL**

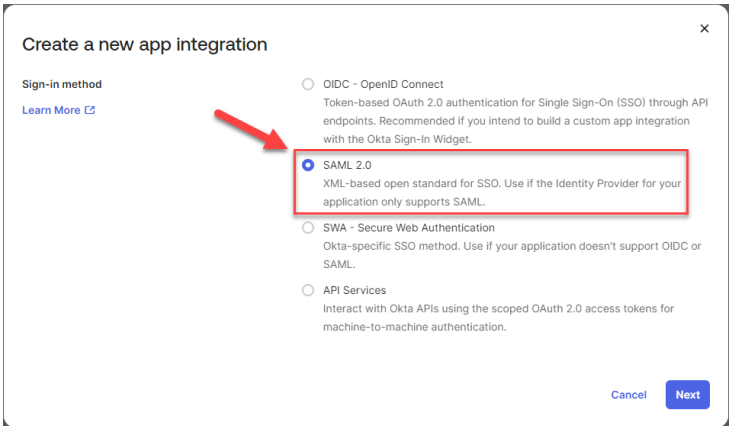
Below is an example of how we configured application and setup fields for mapping, but your IT will know how to configure this best for your company's needs.

Setup

Add application in Okta

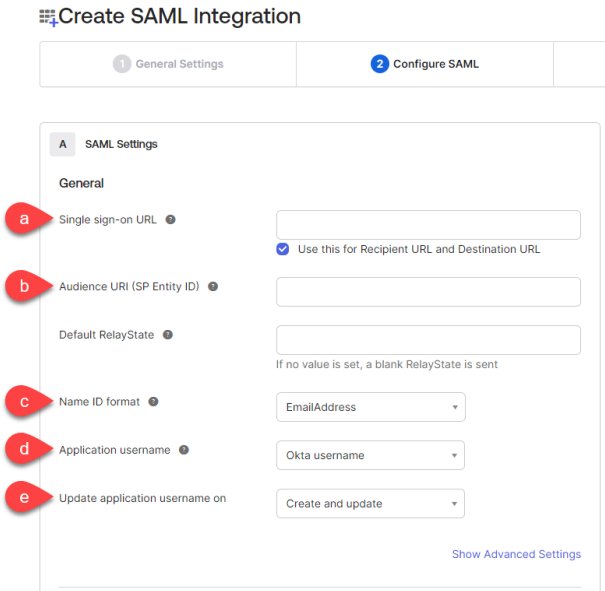
In Okta, follow the steps below:

1) Create a new app integration > select **SAML 2.0**

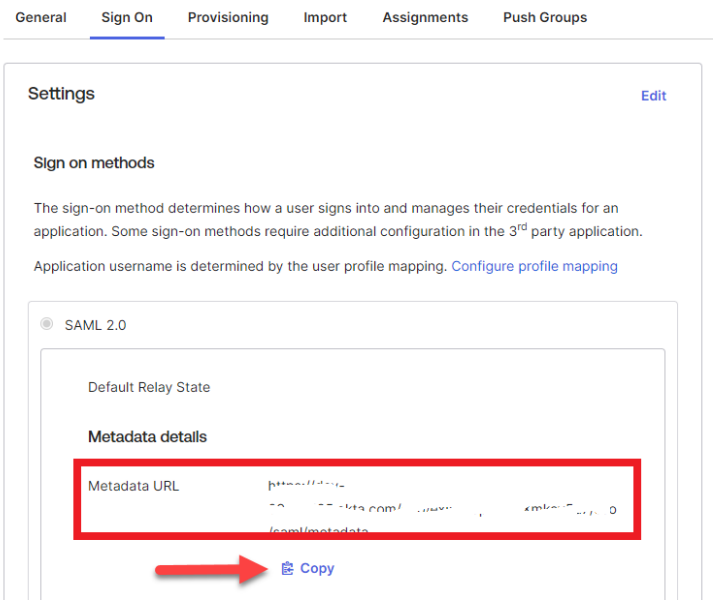


2) Set the following values on the next slide:

a)	Single sign-on URL	*[provided by DocBoss]*
b)	Audience URI (SP Entity ID)	*[provided by DocBoss]*
c)	Name ID format	EmailAddress
d)	Application username	Okta username
e)	Update application username on	Create and update



3) Copy the Metadata URL to send to DocBoss Support:

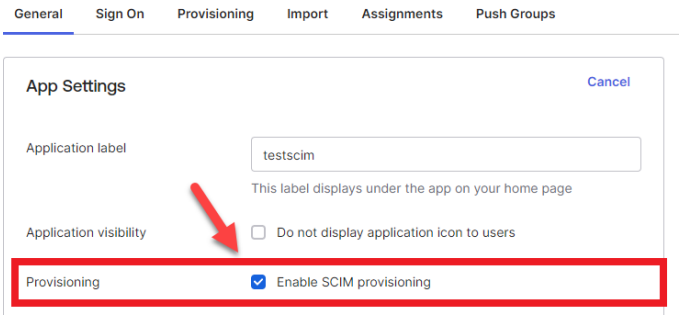


Set up SCIM provisioning

Next, set up SCIM provisioning to allow adding and updating DocBoss users through Okta.

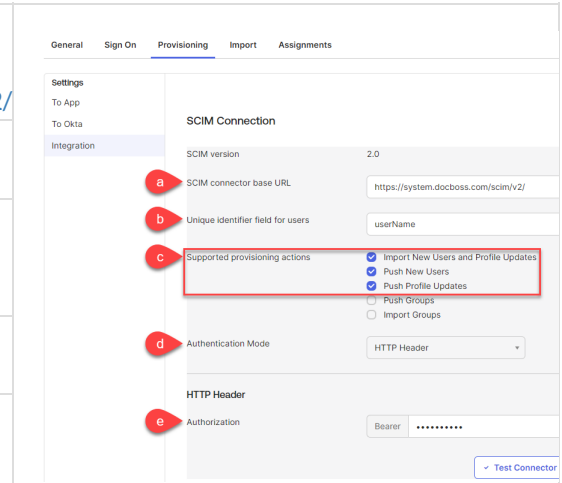
If your DocBoss instance already has users, read Enabling User Provisioning (SCIM) with Existing Users before turning provisioning on.

4) Enable SCIM provisioning and Save.



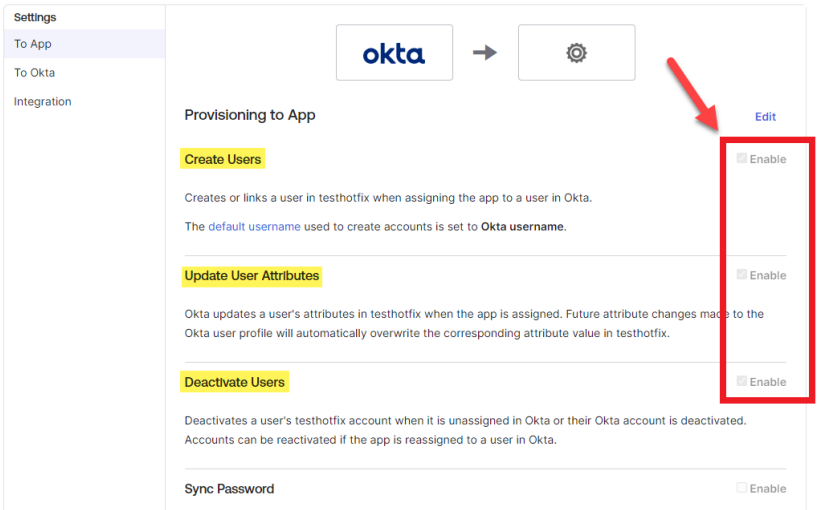
5) Add the following SCIM Connection settings:

a)	SCIM connector base URL	DocBoss Support will provide. For example, https://system.docboss.com/scim/v2/
b)	Unique identifier field for users	userName
c)	Supported provisioning actions	Import New Users and Profile Updates, Push New Users, Push Profile Updates
d)	Authentication Mode	HTTP Header
e)	Authorization Bearer	Long-term token from DocBoss **Security Settings > API Authorization > Tools > Token**



DocBoss provisions users only. Do not select **Push Groups** or set up Group Push for this application; Okta groups can still be used to choose which users are assigned to DocBoss.

6) On the **Provisioning > To App** tab, enable **Create Users**, **Update User Attributes**, and **Deactivate Users**:



Set up user info fields

Next, set up fields for users. The following fields exist in the Okta by default:

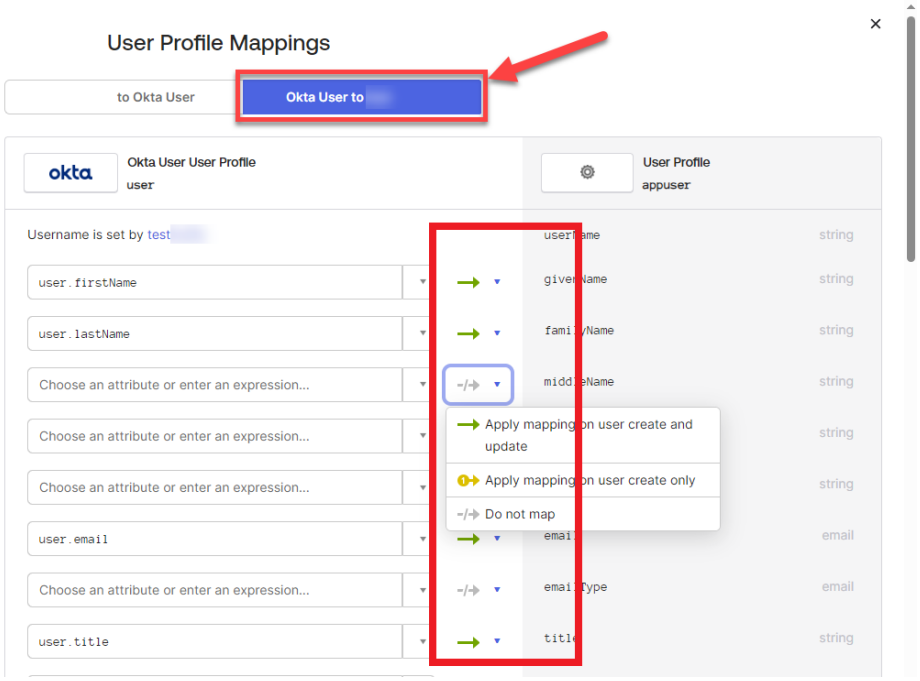
- user. givenName [required]
- user. familyName [required]
- user.title – We used it for title field for the user in the docboss
- user.timezone
- user.userType – we used it for the Role

Note that there is no default field in Okta that matches our "affiliate" field. A custom field can be added for this (see below instructions on adding custom fields). If not included, the user will be given access to the affiliate with the smallest company ID (the original affiliate).

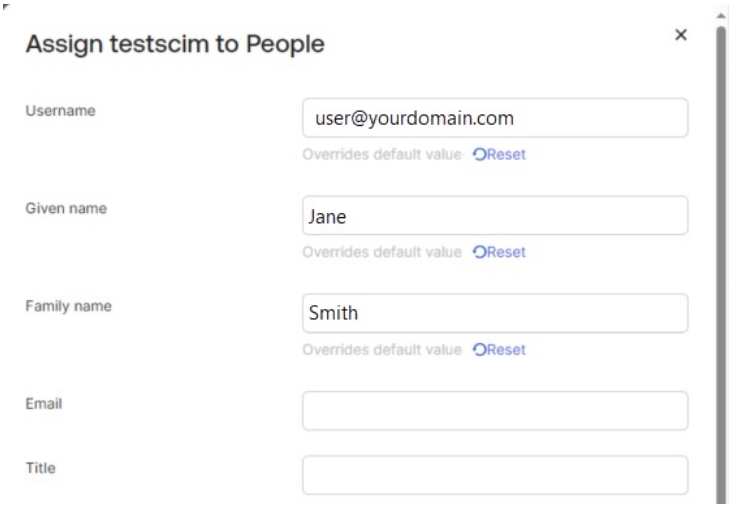
Mapping is set by default. User only should remove mapping for excess fields:

7) Under **Provisioning > To App > Attribute Mappings**, set to *not* apply mapping for all fields except the following:

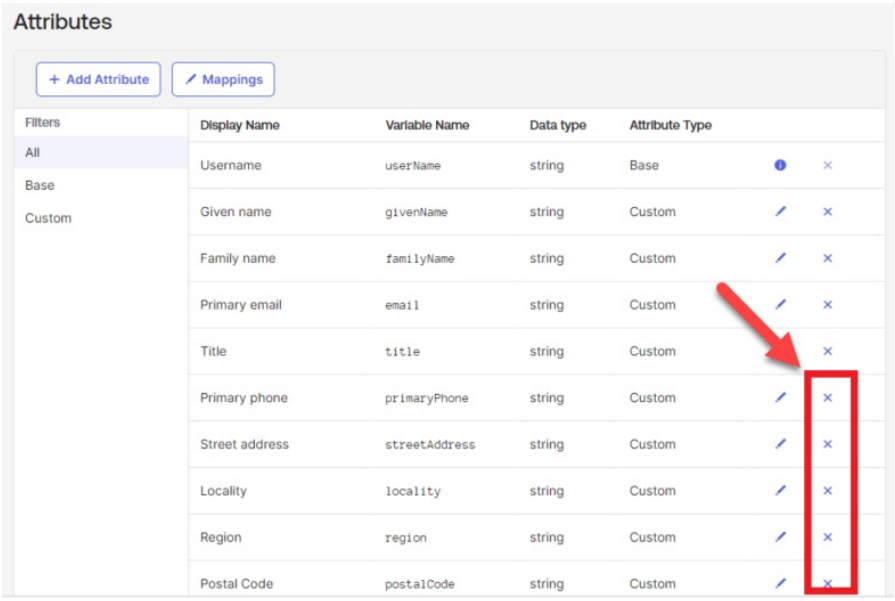
- user.firstName
- user.lastName
- user.title
- user.timezone
- user.userType



This is set so that when a user is assigned to DocBoss in Okta, only the selected fields will be copied and sent to DocBoss.



8) Optionally, you can remove excess fields on the **Profile Editor > Application Profile > Attributes** to hide it on the assign user to application form:



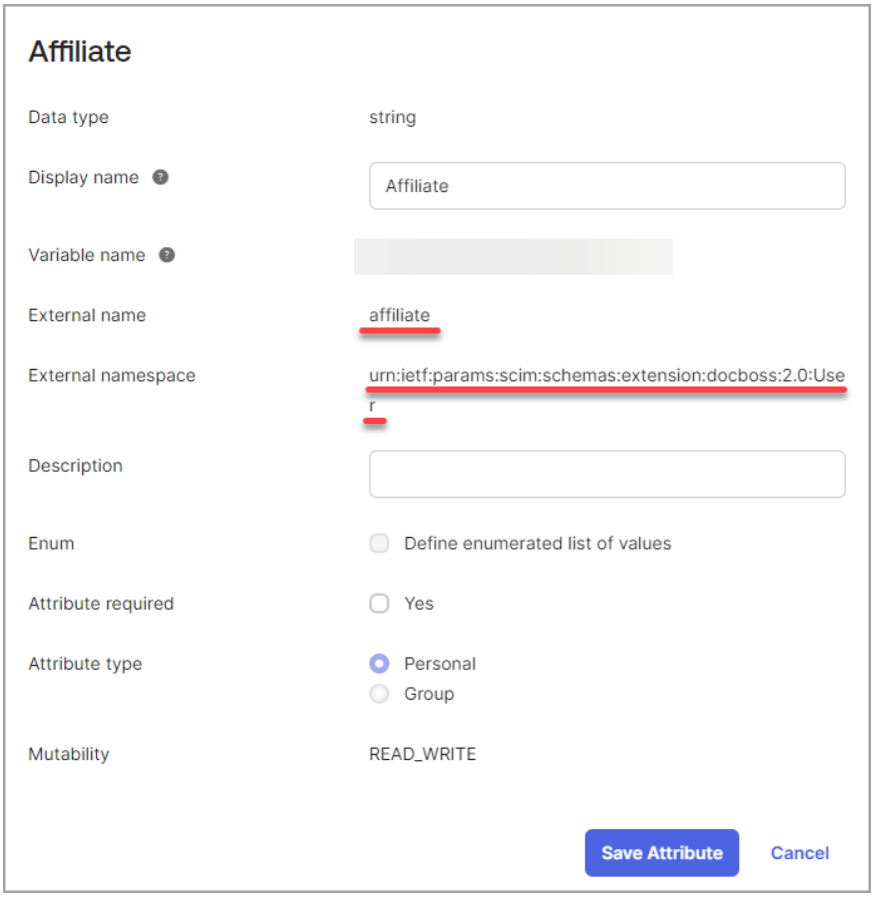
Or you can add some fields as custom to add more settings for the field.

Custom Fields

Affiliates

This is optional. If included, only one affiliate access can be granted at a time. Additional requests will ADD new affiliate access but not remove the existing affiliate access. The value for this should be the Company Short Name from the company profile in DocBoss.

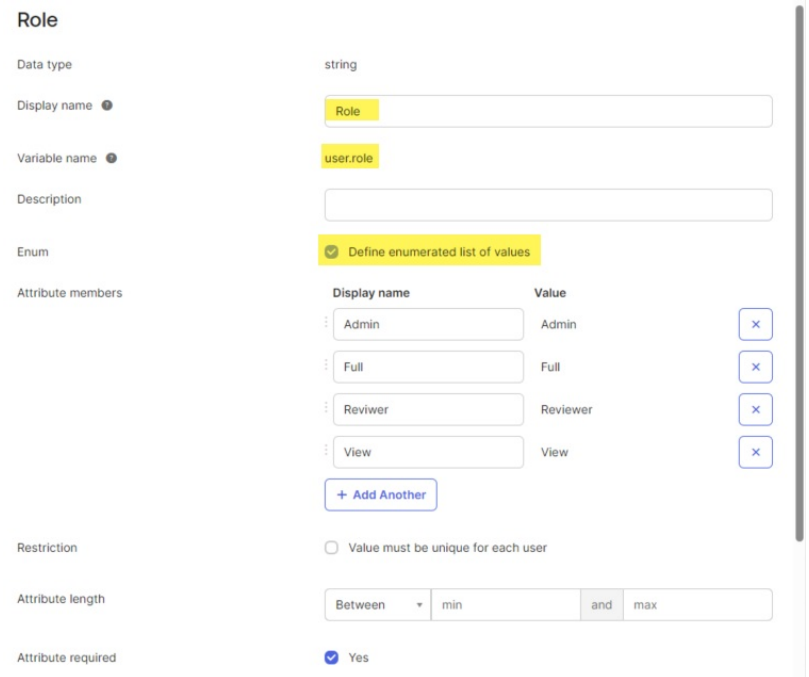
When configuring the field, External name should be set as "affiliate" and External namespace should be set as "urn:ietf:params:scim:schemas:extension:docboss:2.0:User".



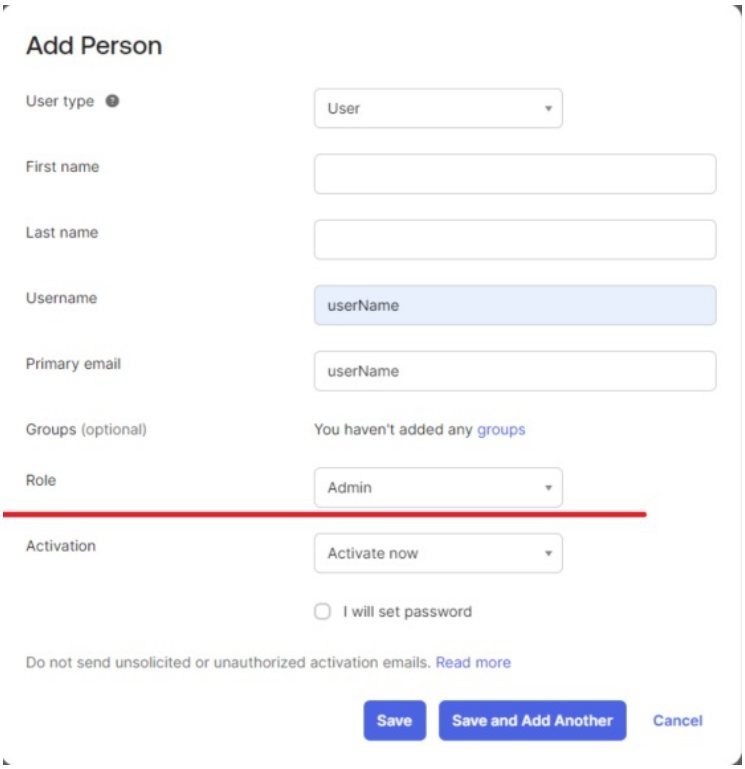
If Affiliate is not included in a request, the user will be given access to the affiliate with the smallest company ID (the original affiliate).

Limit values for Role type

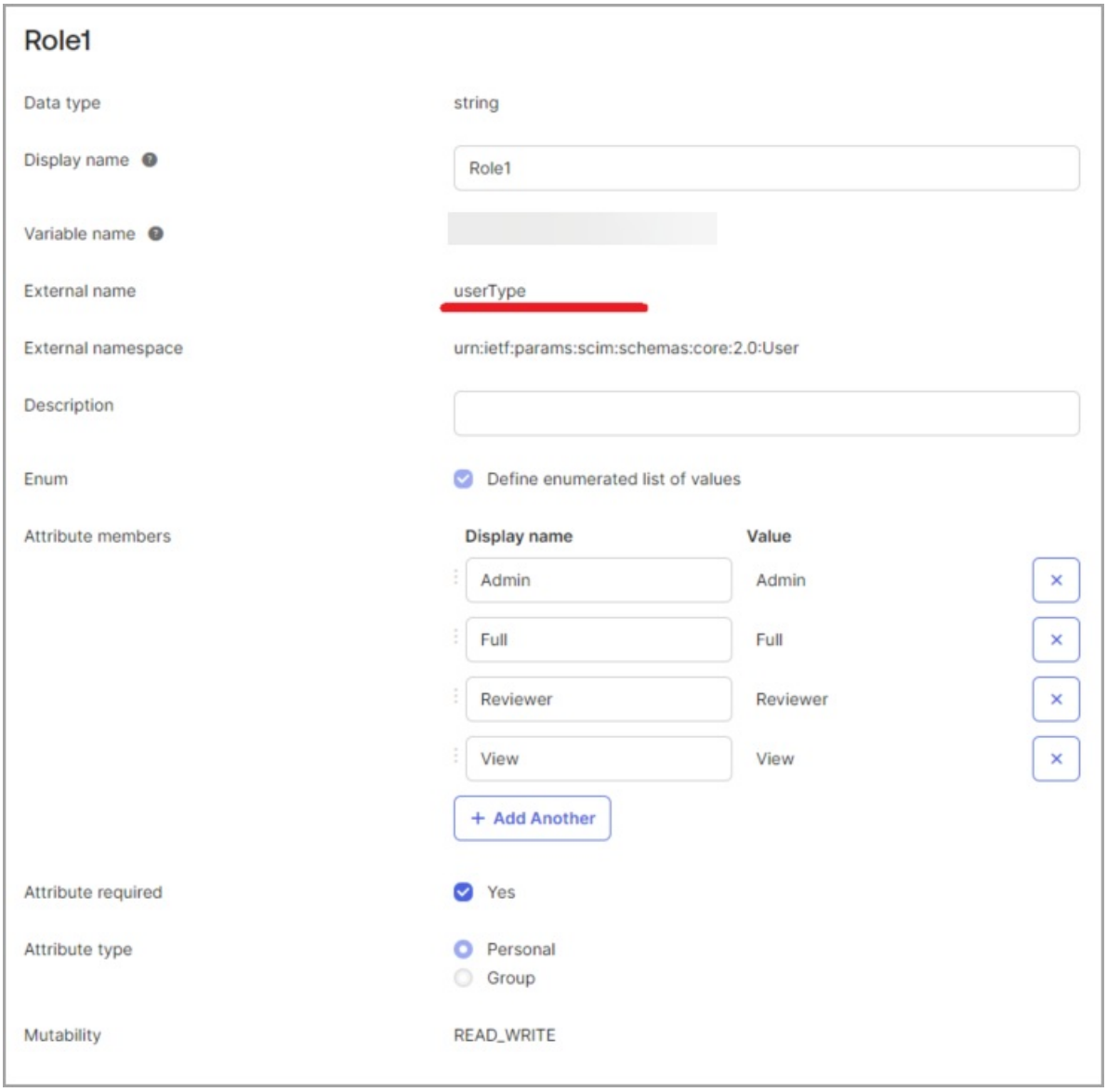
Configuration example:



Result:

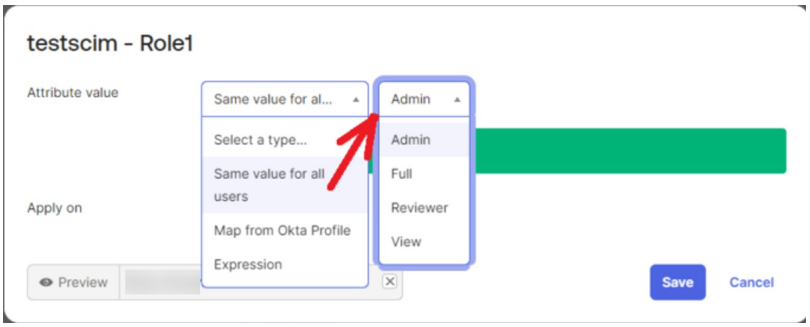


Add this to the Application profile in Okta (**Profile Editor > Application User Profile**). It is important to set correct External name (that DocBoss uses in our API):



Additional settings

There are additional settings in Okta which your IT may wish to configure. For example, there is an option to set a default value for fields:



Implementing

Once the steps above are complete and you have provided the information to DocBoss as noted in them, reach out to DocBoss Support and we will schedule a meeting to enable SSO (and user provisioning, if using). Our Support

will also provide a redirect URI for your application. This will redirect users back to DocBoss after authentication in your identity provider. This must be added in your identity provider application for SSO to function.

If you want to try the function, then schedule a roll out for your users we can schedule the meeting to enable, test (have a user login), then disable within a few minutes. Already logged in users would not be affected. You can then communicate to your user base with a timeline for the switch. Alternatively, we can just leave it enabled after the test is successful.