# **Okta (SSO and User Provisioning)**

11/15/2024 12:32 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
  - **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

Create a new app integration	×	
Sign-in method Learn More 🖸	<ul> <li>OIDC - OpenID Connect</li> <li>Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended If you intend to build a custom app integration with the Okta Sign-In Widget.</li> </ul>	
	<ul> <li>SAML 2.0 XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.</li> </ul>	
	SWA - Secure Web Authentication Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.	
	<ul> <li>API Services Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.</li> </ul>	
	Cancel Next	

#### 2) Set the following values on the next slide:

a)	Single sign-on URL	[provided by DocBoss]	Integration Integration Integration
b)	Audience URI (SP Entity ID)	[provided by DocBoss]	G General Settings 2 Configure SAML
c)	Name ID format	EmailAddress	
d)	Application username	Okta username	A SAML Settings General
e)	Update application username on	Create and update	B       Single sign-on URL         B       Single sign-on URL         C       Name ID format         C       Value is set, a blank RelayState is sent         C       Name ID format         C       Value is set, a blank RelayState is sent         C       Name ID format         C       Create and update         V       Value is set, a blank RelayState is sent

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

	Sign On	Provisioning	import	Assignments	Push Groups
Setting	gs				Edi
Sign o	n methods				
The sig	n-on method d	letermines how a	user signs ir	to and manages th	eir credentials for an
applica	tion. Some sign	is determined by	quire addition	al configuration in	the 3 <sup>rd</sup> party application.
Applica	ition username	is determined by	the user pro	file mapping. Confi	gure profile mapping
SA	ML 2.0				
● SA	ML 2.0	State			
● SA	ML 2.0 Default Relay	State			
● SA	Default Relay Metadata de	State etails			
• SA	ML 2.0 Default Relay Metadata de Metadata URI	State etails	•ma.//		

# Set up SCIM provisioning

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

4) Enable SCIM provisioning and Save.

General	Sign On	Provisioning	Import	Assignments	Push Groups	
App Se	ttings					Cancel
Applicati	on label	te	estscim			
		This	s label displa	ays under the app o	on your home page	
Applicati	on visibility		Do not disp	lay application icor	n to users	
Provision	ing		Enable SCI	M provisioning		

#### 5) Add the following SCIM Connection settings:

a)	SCIM connector base URL	DocBoss Support will provide. For example, https://system.docboss.com/scim/v2/	General Si Settings To App	ign On Pro	visioning Import Assignments	
b)	Unique identifier field for users	userName	To Okta Integration	a	SCIM Connection	2.0 https://system.docboss.com/scim/v2/
c)	Supported provisioning actions	Import New Users and Profile Updates, Push New Users, Push Profile Updates, Push Groups		b	Unique identifier field for users Supported provisioning actions	UserName Import New Users and Profile Updates Push New Users Push Profile Updates Push Groups Pash Groups Import Owner Imp
d)	Authentication Mode	HTTP Header		d	Authentication Mode	HTTP Header •
e)	Authorization Bearer	Long-term token from DocBoss Security Settings > API Authorization > Tools > Token		e	Authorization	Bearer ••••••••••••••••••••••••••••••••••

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

Settings						
То Арр		okta	-	iõ;		
To Okta		UNCO	J	Ny T		
Integration	Provisioning to App					Edit
	Create Users					Enable
	Creates or links a user in tes The default username used Update User Attributes Okta updates a user's attrib	sthotfix when assigning to create accounts is s	g the app to a set to <b>Okta u</b>	a user in Okta. sername. assioned, Future attrib	oute changes mad	Enable
	Okta user profile will automa	atically overwrite the c	orresponding	g attribute value in te	sthotfix.	
	Deactivate Users					Enable
	Deactivates a user's testhot Accounts can be reactivated	fix account when it is d if the app is reassign	unassigned i ed to a user	n Okta or their Okta a in Okta.	ccount is deactiva	ited.
	Sync Password					Enable

## Set up user info fields

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

- user. givenName [required]
- user. givenName [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

User Profile Mappings				
to Okta User Okta User to				
okta User User Profile user			User Profile appuser	
Username is set by test	Г		useriame	string
user.firstName	•	$\rightarrow$ .	give Name	string
user.lastName	•	<b>→</b> •	famil/Name	string
Choose an attribute or enter an expression	-	-/-> •	midd.eName	string
Choose an attribute or enter an expression	•	- Apply update	mapping on user create and	string
Choose an attribute or enter an expression	•	O→ Apply	mapping on user create only	string
user.email	-	-/-> Do not	map emai:	email
Choose an attribute or enter an expression	-	-/-> •	emai:Type	email
user.title		→ •	title	string

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.

Assign testscim	to People
Username	user@yourdomain.com
	Overrides default value OReset
Given name	Jane
	Overrides default value OReset
Family name	Smith
	Overrides default value OReset
Email	
Title	

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

ttributes						
+ Add Attribu	Ite Mappings					
ilters	Display Name	Variable Name	Data type	Attribute Type		
di	Username	userName	string	Base	0	×
ase ustom	Given name	givenName	string	Custom	1	×
	Family name	familyName	string	Custom	1	×
	Primary email	email	string	Custom	1	×
	Title	title	string	Custom		×
	Primary phone	primaryPhone	string	Custom	1	×
	Street address	streetAddress	string	Custom	1	×
	Locality	locality	string	Custom	1	×
	Region	region	string	Custom	1	×
	Postal Code	postalCode	string	Custom	1	×

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".

Affiliate	
Data type	string
Display name	Affiliate
Variable name 💿	
External name	affiliate
External namespace	urn:ietf:params:scim:schemas:extension:docboss:2.0:Use
Description	
Enum	Define enumerated list of values
Attribute required	O Yes
Attribute type	<ul><li>Personal</li><li>Group</li></ul>
Mutability	READ_WRITE
	Save Attribute Cancel

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:

Role		
Data type	string	
Display name	Role	
Variable name	user.role	
Description		
Enum	Define enumerated list of value	es
Attribute members	Display name	Value
	Admin	Admin ×
	i Full	Full
	Reviwer	Reviewer
	View	View
	+ Add Another	
Restriction	Value must be unique for each	user
Attribute length	Between * min	and max
Attribute required	Ves Yes	

Result:

Add 1 croon			
User type 🔘	User	*	
First name			
Last name			
Username	userName		
Primary email	userName		
Groups (optional)	You haven't added any	groups	
Role	Admin	*	_
Activation	Activate now	¥	
	I will set password		
Do not send unsolicited or unau	thorized activation emails. Read I	more	
	Save Sav	e and Add Another	Cancel

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):

Role1		
Data type	string	
Display name	Role1	
Variable name		
External name	userType	
External namespace	urn:ietf:params:scim:schemas:core	:2.0:User
Description		
Enum	Define enumerated list of value	es
Attribute members	Display name	Value
	Admin	Admin
	Eull	Full
	Reviewer	Reviewer
	View	View
	+ Add Another	
Attribute required	🕑 Yes	
Attribute type	<ul><li>Personal</li><li>Group</li></ul>	
Mutability	READ_WRITE	

### 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:

testscim - Ro	le1		
Attribute value	Same value for al A	Admin 🔺	
	Select a type	Admin	
Apply on	Same value for all users	Full	
Apply on	Map from Okta Profile	View	
Preview	Expression	×	Save Cancel

# 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.