Inventsys

Instructions and Settings for

SSO OKTA Identity Platform

Introduction

This document brings an agile tutorial on how to set up Single-sign-on authentication method for Okta Identity provider platform.

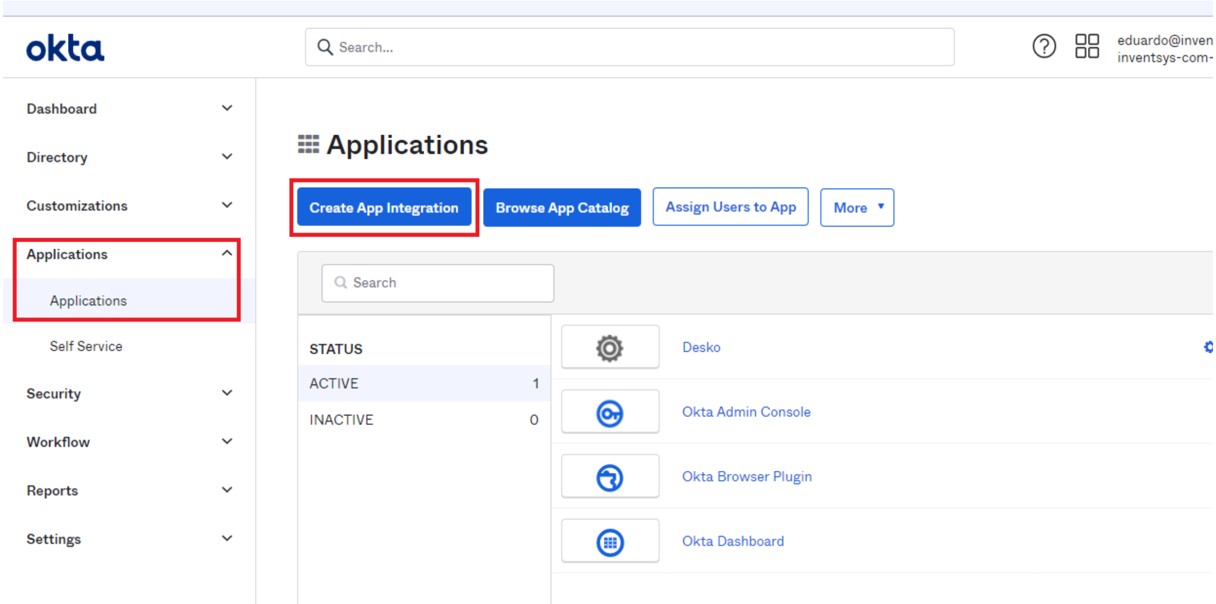
Contents

Creating Desko Application on Okta Admin portal and setting up SSO (SAML 2.0) **2**

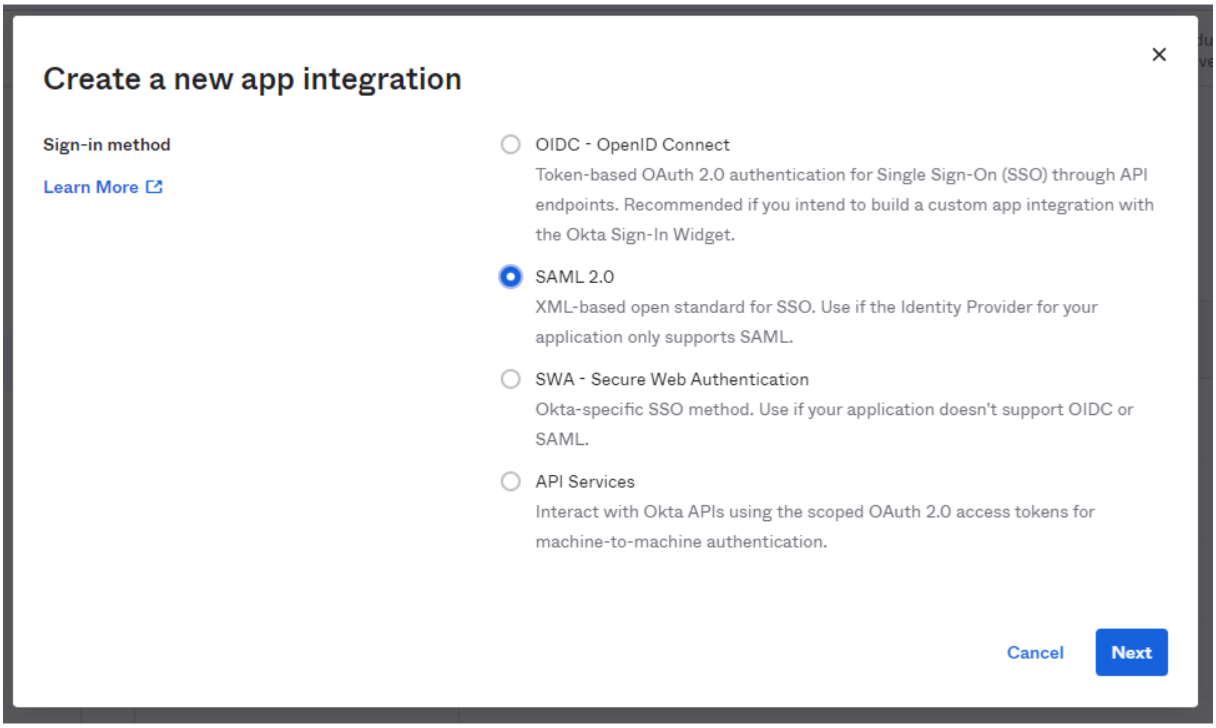
Versioning **12**

Creating *Desko* Application on Okta Admin Portal and setting up SSO (SAML 2.0)

1. Access your Okta Admin Console at https://<YourCompanyName>-admin.okta.com/admin go to **Applications** and click on **Create App Integration**



2. Choose **SAML 2.0** option and click on **Next**



Create a new app integration

Sign-in method

Learn More

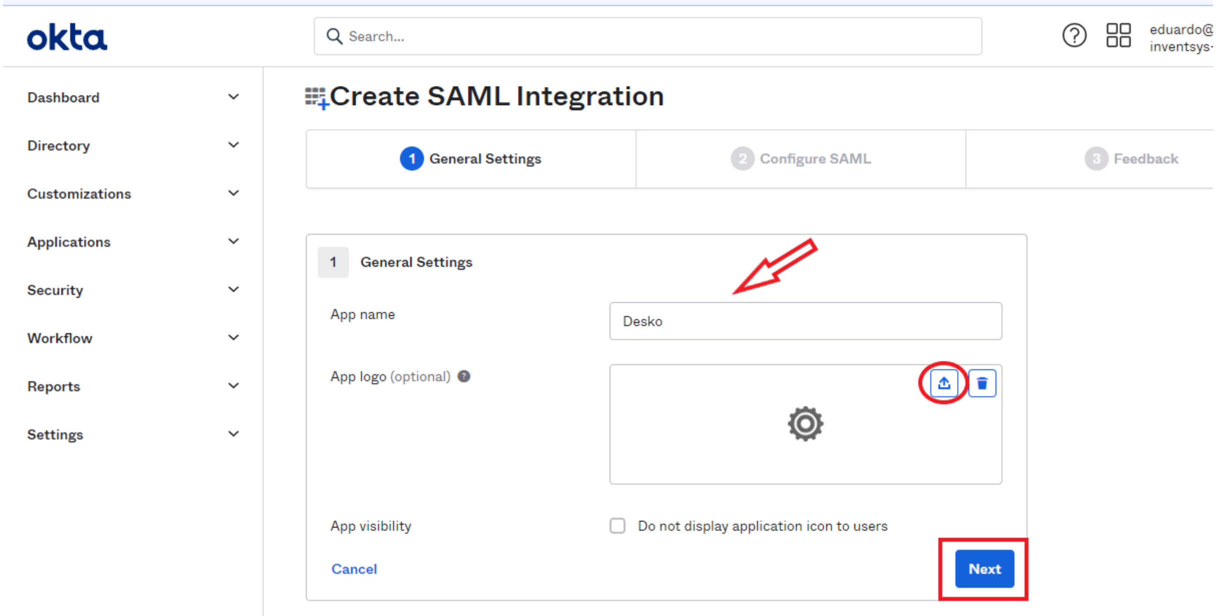
○ OIDC - OpenID Connect
Token-based OAuth 2.0 authentication for Single Sign-On (SSO) through API endpoints. Recommended if you intend to build a custom app integration with the Okta Sign-In Widget.

● SAML 2.0
XML-based open standard for SSO. Use if the Identity Provider for your application only supports SAML.

○ SWA - Secure Web Authentication
Okta-specific SSO method. Use if your application doesn't support OIDC or SAML.

○ API Services
Interact with Okta APIs using the scoped OAuth 2.0 access tokens for machine-to-machine authentication.

3. Enter a name for your application, add a logo (optional) by clicking on the **upload button**, and click on **Next**



1 General Settings

App name: Desko

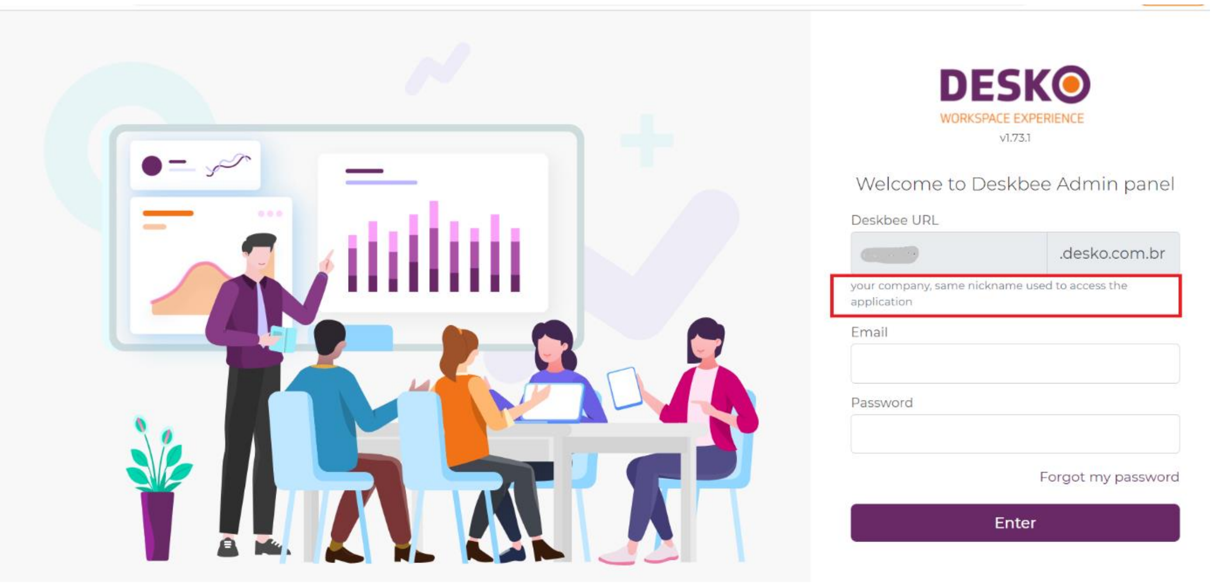
App logo (optional)

App visibility: □ Do not display application icon to users

Note: Before move on to the **SAML settings**, it is necessary to get the *Desko*’s URLs that is going to be inserted into the URL fields in the next step.

4. Go to your *Desko* panel heading over to **https://<YourCompanyName>.painel.desko.com.br**

   Note: You have to log in using a Master or Admin account.



Welcome to Deskbee Admin panel

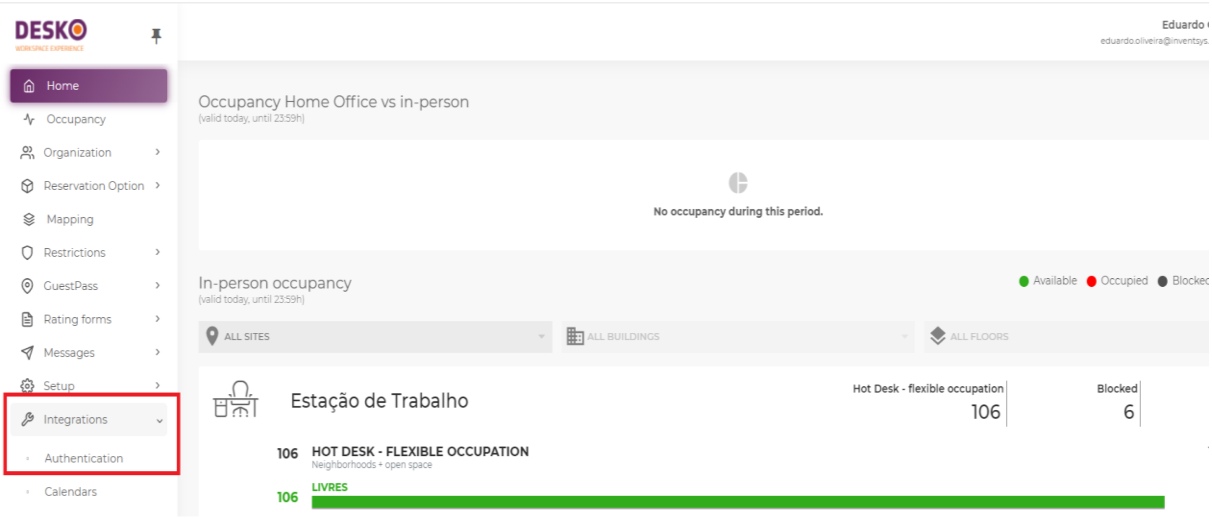
Deskbee URL: [redacted] .desko.com.br

your company, same nickname used to access the application

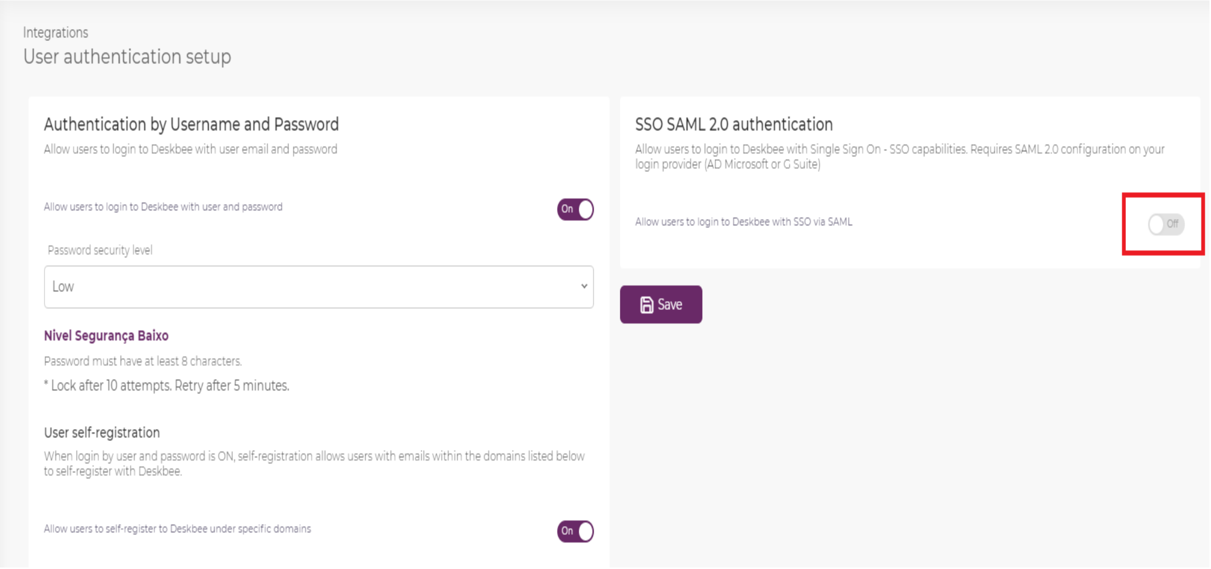
Email

Password

5. Expand **Integrations** and click on **Authentication**



6. Turn on **SSO SAML 2.0 authentication**,



Integrations

User authentication setup

Authentication by Username and Password

Allow users to login to Deskbee with user email and password

Allow users to login to Deskbee with user and password — On

Password security level: Low

Nivel Segurança Baixo

Password must have at least 8 characters.

* Lock after 10 attempts. Retry after 5 minutes.

User self-registration

When login by user and password is ON, self-registration allows users with emails within the domains listed below to self-register with Deskbee.

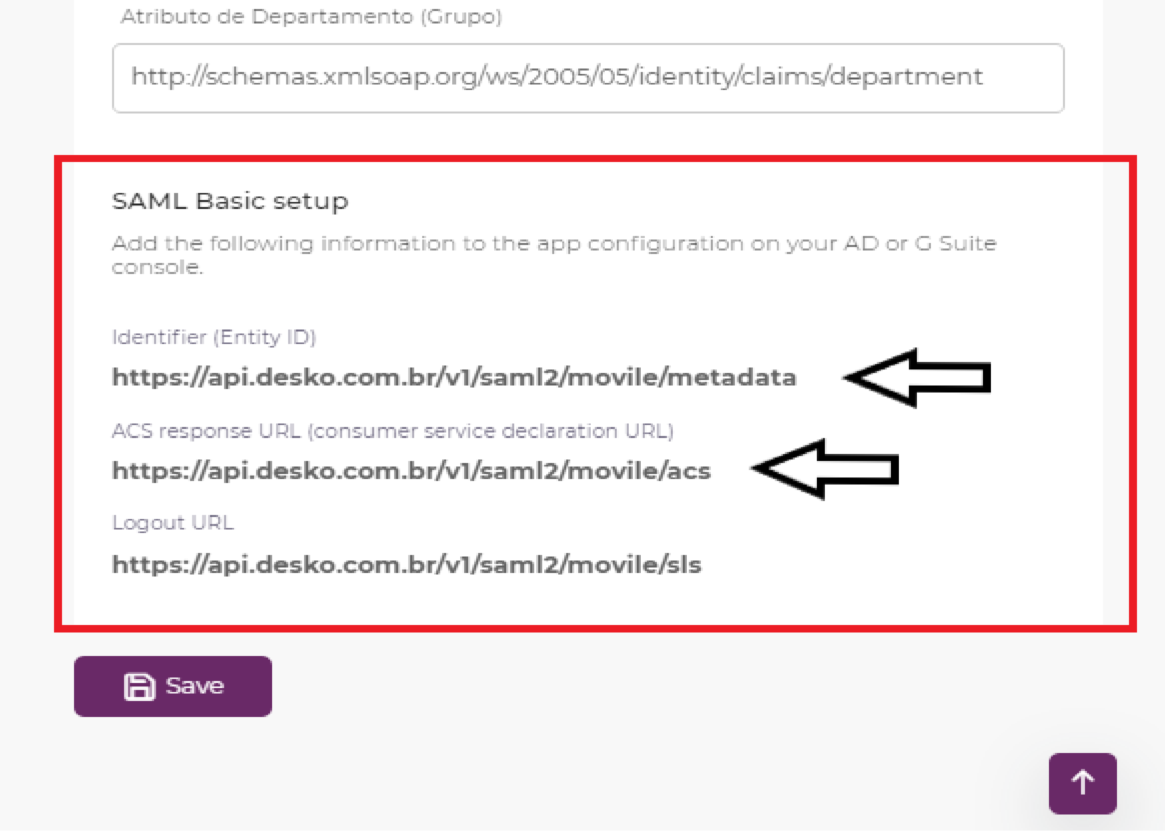
Allow users to self-register to Deskbee under specific domains — On

SSO SAML 2.0 authentication

Allow users to login to Deskbee with Single Sign On - SSO capabilities. Requires SAML 2.0 configuration on your login provider (AD Microsoft or G Suite)

Allow users to login to Deskbee with SSO via SAML — Off

7. Go to the bottom of the page at **SAML Basic setup** and copy the **Entity ID** and the **ACS response URL** as shown below. The **Logout URL** is optional.



Atributo de Departamento (Grupo)

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department

SAML Basic setup

Add the following information to the app configuration on your AD or G Suite console.

Identifier (Entity ID)

https://api.desko.com.br/v1/saml2/movile/metadata

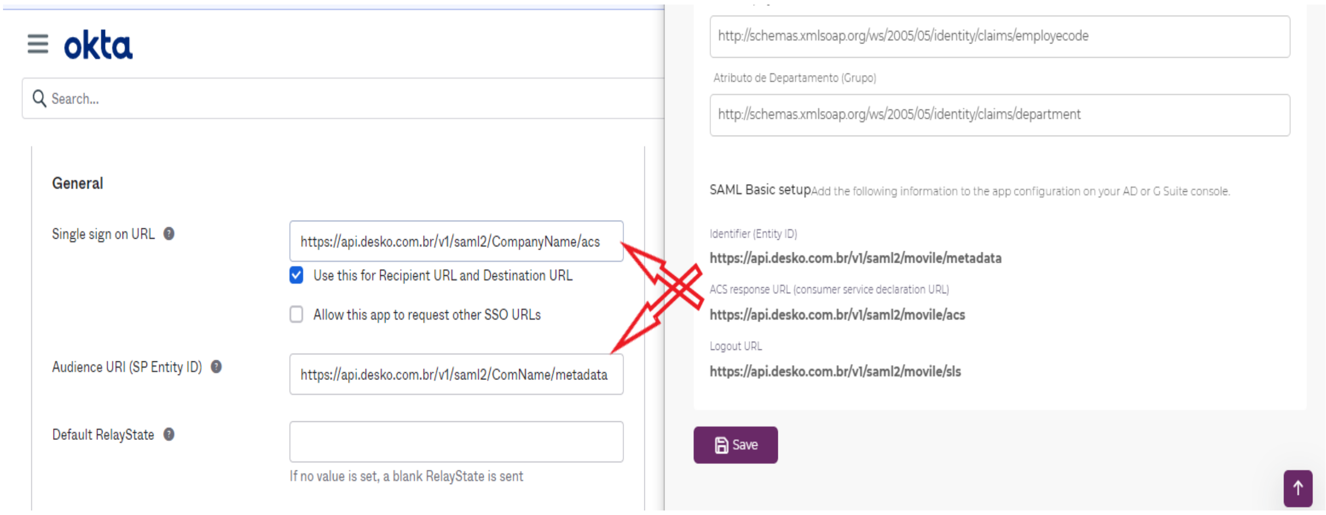
ACS response URL (consumer service declaration URL)

https://api.desko.com.br/v1/saml2/movile/acs

Logout URL

https://api.desko.com.br/v1/saml2/movile/sls

8. Go back to your Okta Admin portal, and paste the 2 URLs mentioned in the previous item into the proper fields as shown below:



General

Single sign on URL: https://api.desko.com.br/v1/saml2/CompanyName/acs

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://api.desko.com.br/v1/saml2/ComName/metadata

Default RelayState:

If no value is set, a blank RelayState is sent

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/employeecode

Atributo de Departamento (Grupo)

http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department

SAML Basic setupAdd the following information to the app configuration on your AD or G Suite console.

Identifier (Entity ID)

https://api.desko.com.br/v1/saml2/movile/metadata

ACS response URL (consumer service declaration URL)

https://api.desko.com.br/v1/saml2/movile/acs

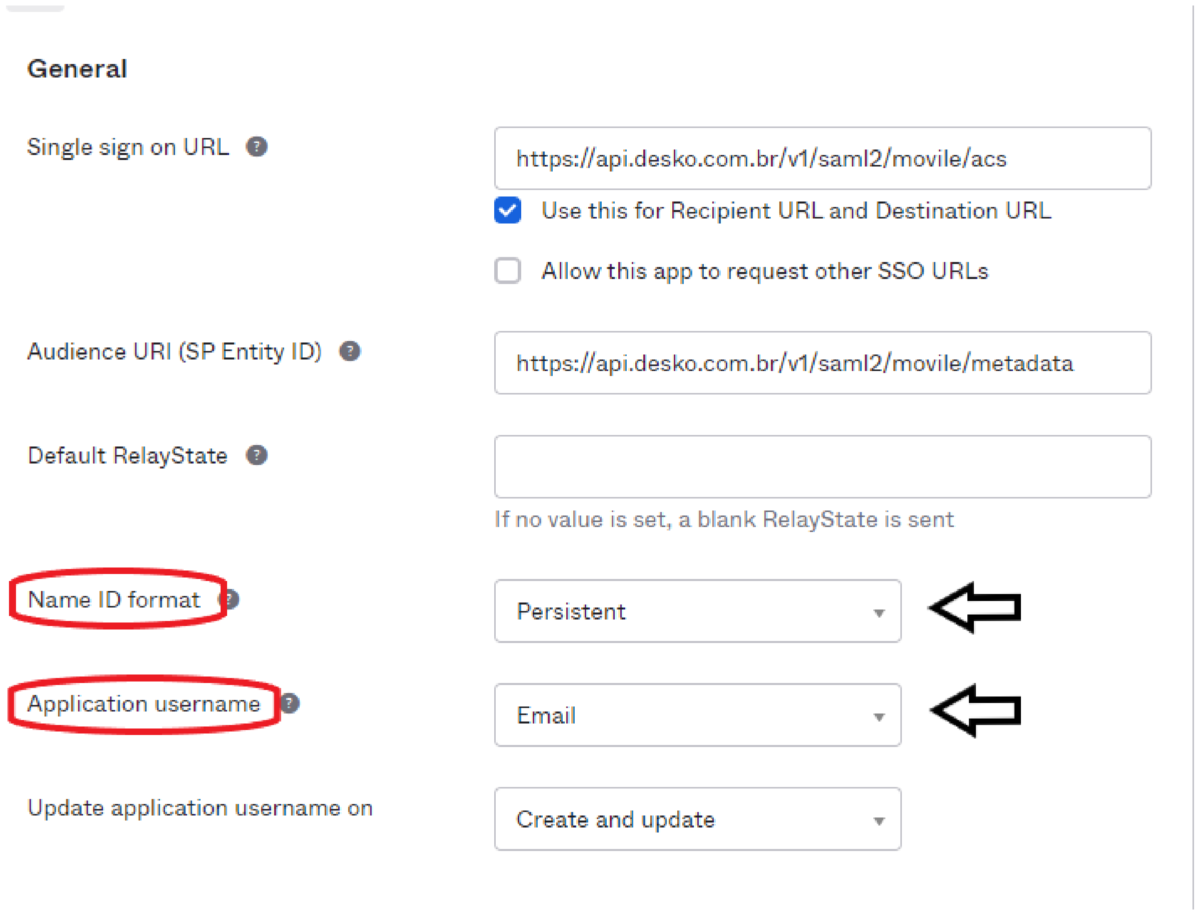
Logout URL

https://api.desko.com.br/v1/saml2/movile/sls

URLs from *Desko* Panel that should match on Okta Admin Portal:

***Desko* Panel**	**Okta Admin Portal**
Identifier (Entity ID)	Audience URI (SP Entity ID)
ACS response URL (consumer service declaration)	Single sign on URL

9. Change the fields **Name ID format** and **Application username** to the values ***"Persistent"*** and ***"Email"*** respectively as shown below



General

Single sign on URL: https://api.desko.com.br/v1/saml2/movile/acs

☑ Use this for Recipient URL and Destination URL

□ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://api.desko.com.br/v1/saml2/movile/metadata

Default RelayState:

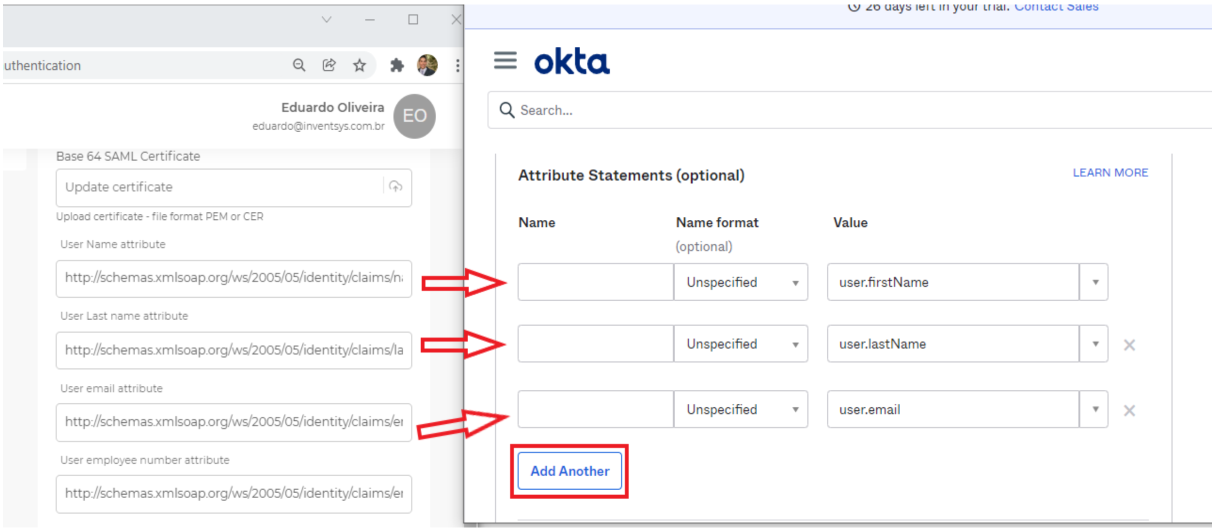
If no value is set, a blank RelayState is sent

Name ID format: Persistent

Application username: Email

Update application username on: Create and update

10. On **Attribute Statements** section, add the first Claim value as ***"user.firstName"***, and insert the **User Name attribute** from *Desko* panel as shown below. Keep **Name format** option as ***"Unspecified"***. Click on **Add Another** button and do the same for the Claims ***"user.lastName"*** and "***user.email"*** just like shown below.



Base 64 SAML Certificate

Update certificate

Upload certificate - file format PEM or CER

User Name attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/n

User Last name attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/la

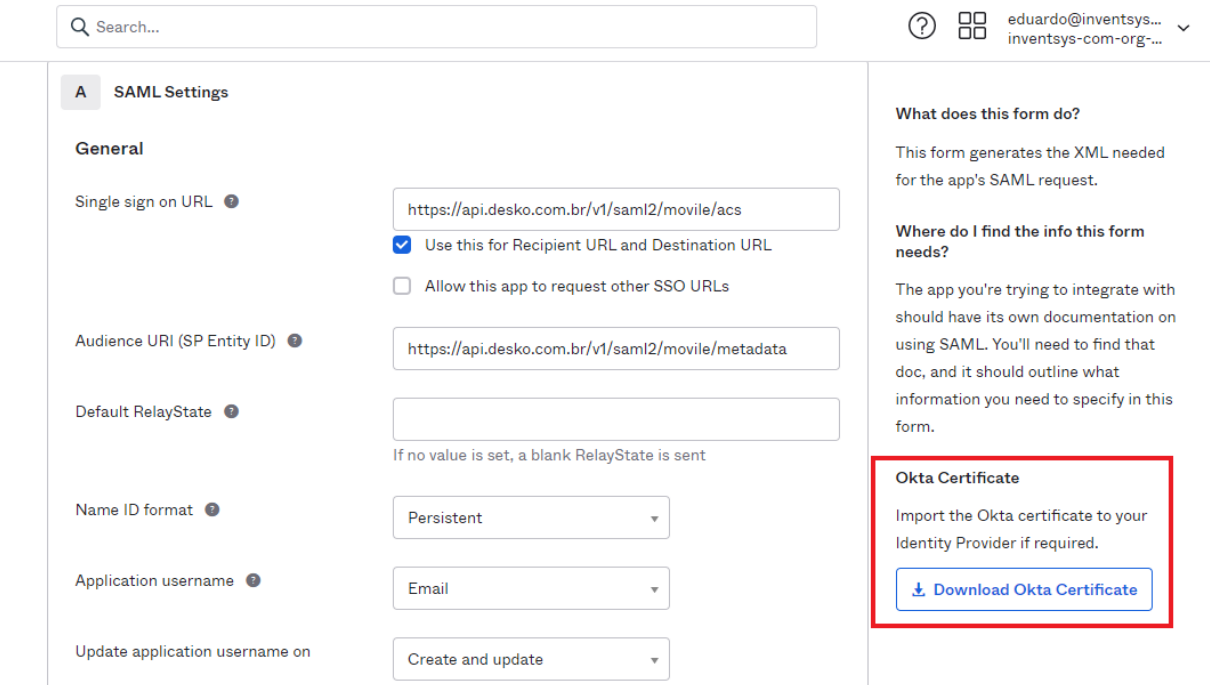
User email attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/e

User employee number attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/e

Attribute Statements (optional)

Name	Name format (optional)	Value
	Unspecified	user.firstName
	Unspecified	user.lastName
	Unspecified	user.email

11. Download and save the **Okta certificate**, you will need to upload on *Desko* panel later on



A SAML Settings

General

Single sign on URL: https://api.desko.com.br/v1/saml2/movile/acs

☑ Use this for Recipient URL and Destination URL

☐ Allow this app to request other SSO URLs

Audience URI (SP Entity ID): https://api.desko.com.br/v1/saml2/movile/metadata

Default RelayState:

If no value is set, a blank RelayState is sent

Name ID format: Persistent

Application username: Email

Update application username on: Create and update

What does this form do?

This form generates the XML needed for the app's SAML request.

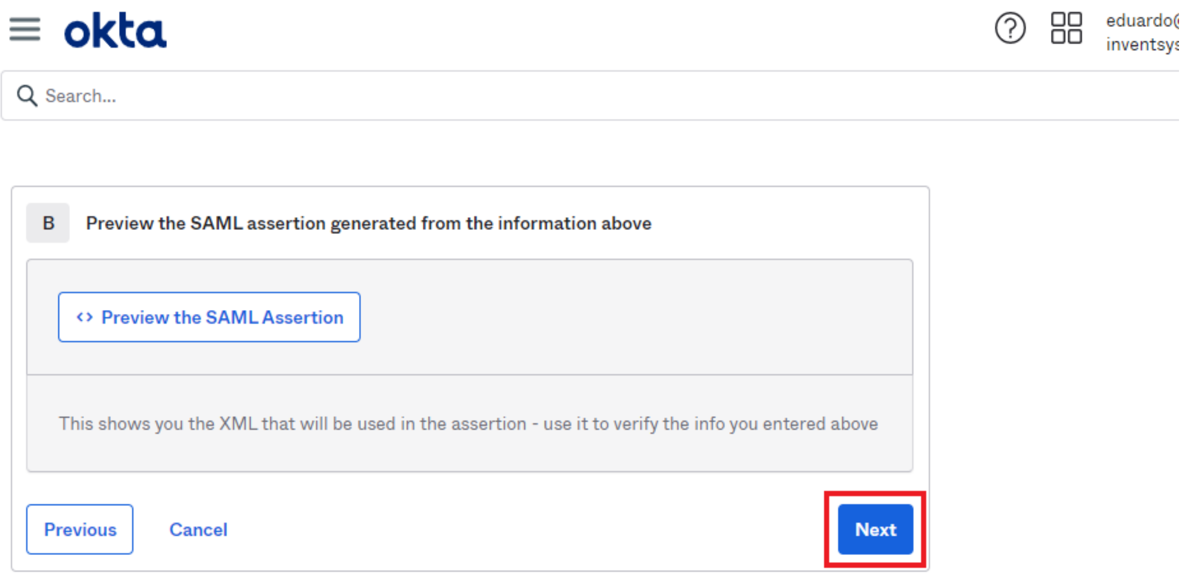
Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

Okta Certificate

Import the Okta certificate to your Identity Provider if required.

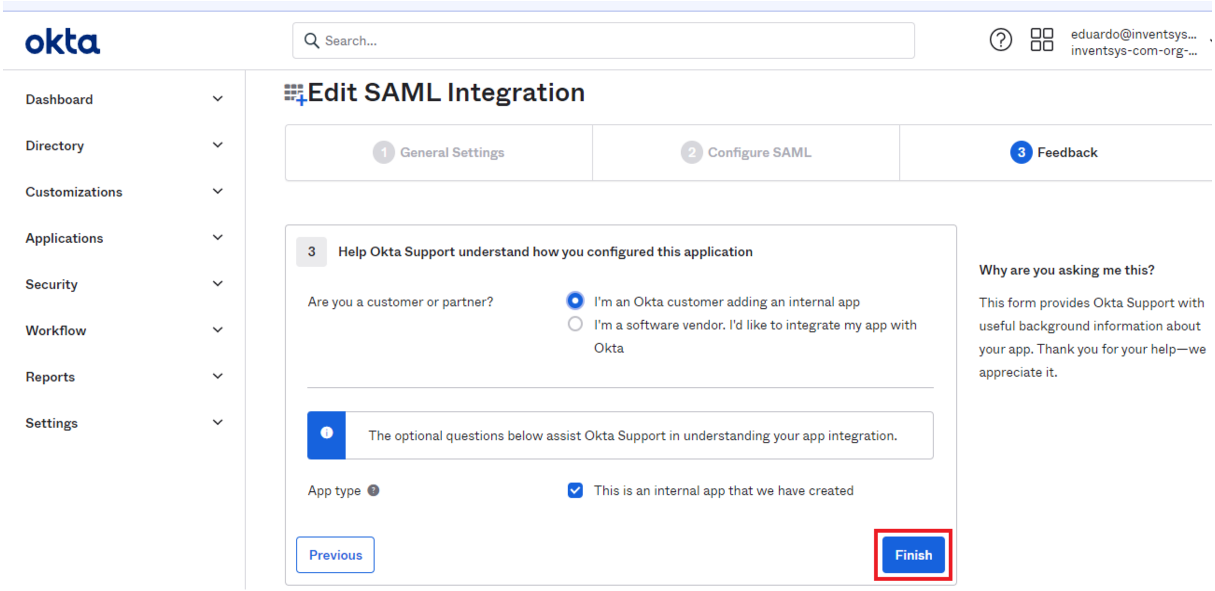
12. Click on **Next**



B Preview the SAML assertion generated from the information above

This shows you the XML that will be used in the assertion - use it to verify the info you entered above

13. On **Feedback** tab, just select the proper options according to your Okta client profile and click on **Finish** button.



Edit SAML Integration

1 General Settings | 2 Configure SAML | 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?
● I'm an Okta customer adding an internal app
○ I'm a software vendor. I'd like to integrate my app with Okta

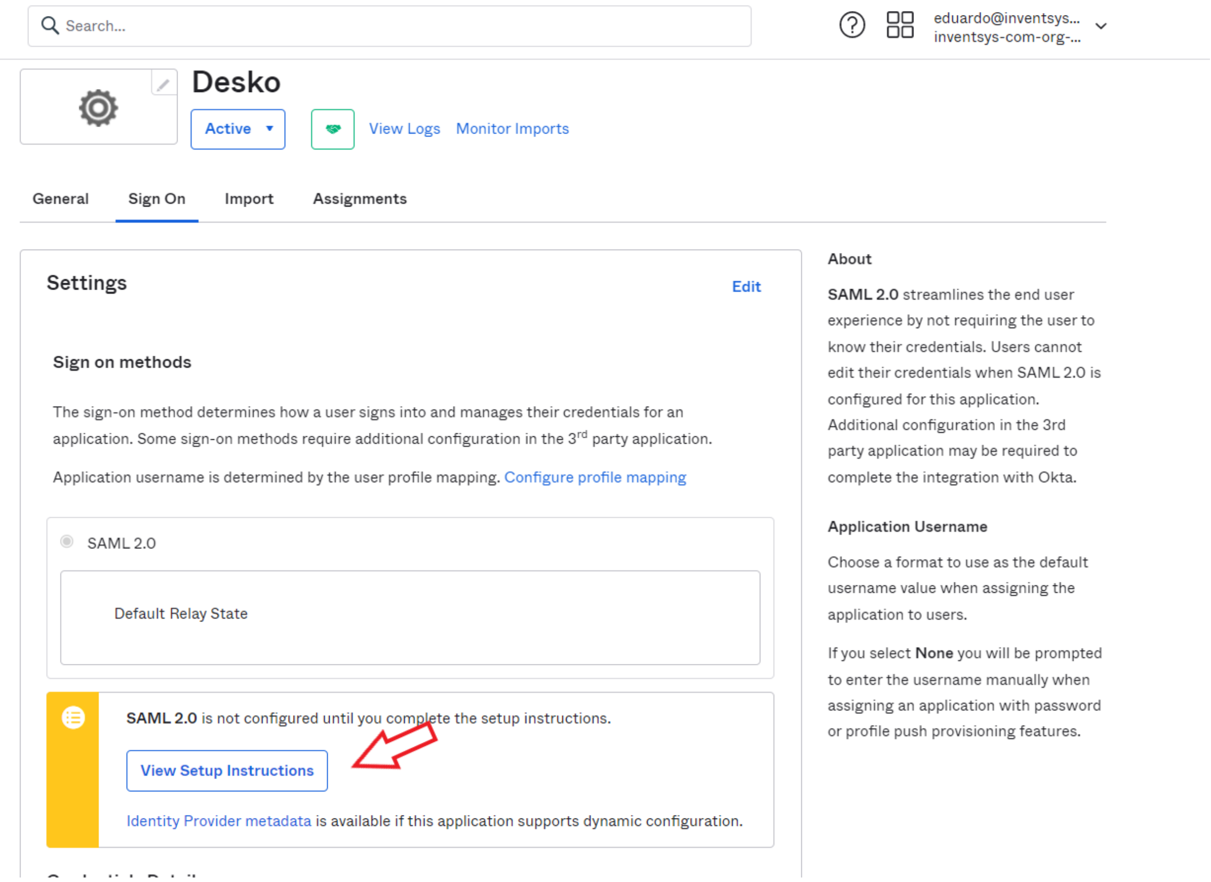
The optional questions below assist Okta Support in understanding your app integration.

App type ☑ This is an internal app that we have created

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

14. In the next screen, click on **View Setup Instructions** and a new tab will be open with the settings needed to configure *Desko* application



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

○ SAML 2.0

Default Relay State

SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

About

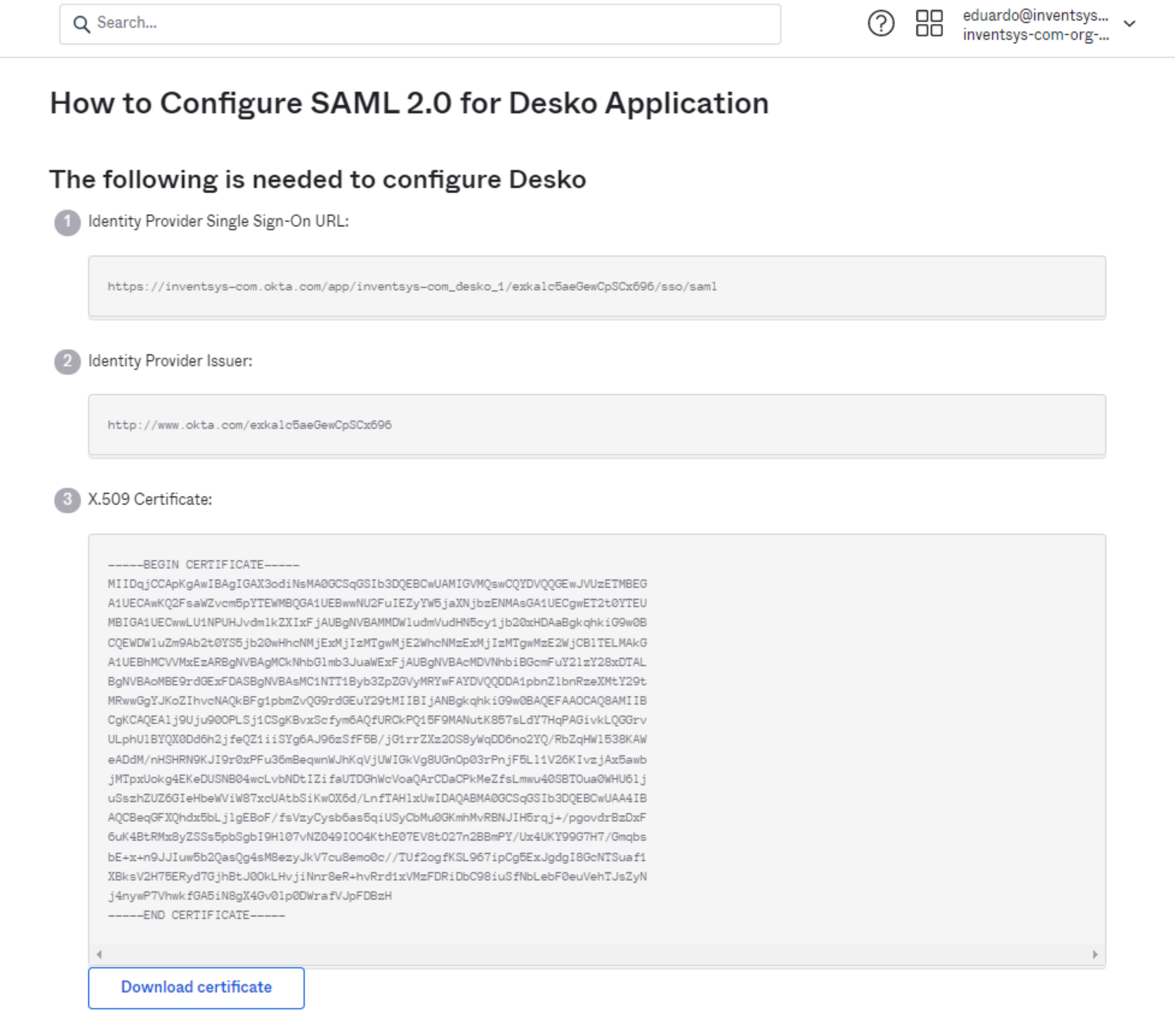
SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.

Application Username

Choose a format to use as the default username value when assigning the application to users.

If you select **None** you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

Here you have all the information needed to set up *Desko* application:



How to Configure SAML 2.0 for Desko Application

The following is needed to configure Desko

1. Identity Provider Single Sign-On URL:

```
https://inventsys-com.okta.com/app/inventsys-com_desko_1/exkalc5aeGewCpSCx696/sso/saml
```

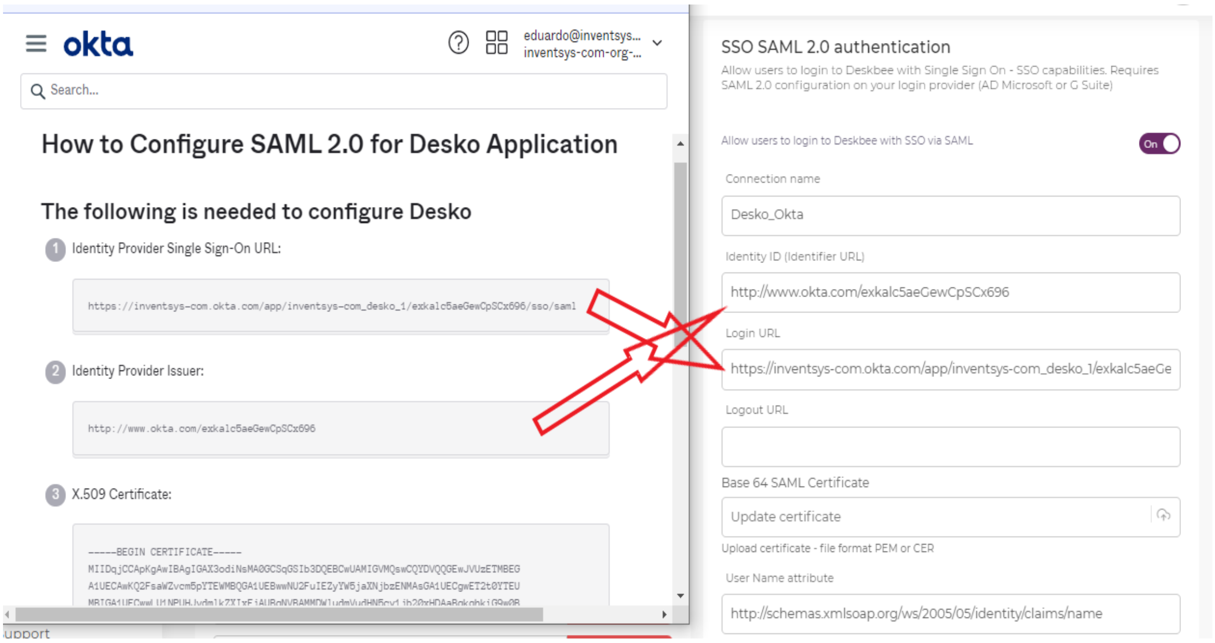
2. Identity Provider Issuer:

```
http://www.okta.com/exkalc5aeGewCpSCx696
```

3. X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwIBAgIGAX3odiNsMA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDWludmVudHN5cy1jb20xHDAaBgkqhkiG9w0B
CQEWDWluZm9Ab2t0YS5jb20wHhcNMjExMjIzMTgwMjE2WhcNMzExMjIzMTgwMzE2WjCBlTELMAkG
A1UEBhMCVVMxEzARBgNVBAgMCkNhbGlmb3JuaWExFjAUBgNVBAcMDVNhbiBGcmFuY2lzY28xDTAL
BgNVBAoMBE9rdGExFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRYwFAYDVQQDDA1pbnZlbnRzeXMtY29t
MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB
CgKCAQEAlj9Uju90OPLSj1CSgKBvxScfym6AQfURCkPQ15F9MANutK857sLdY7HqPAGivkLQGGrv
ULphUlBYQX0Dd6h2jfeQZ1iiSYg6AJ96zSfF5B/jG1rrZXz2OS8yWqDD6no2YQ/RbZqHWl538KAW
eADdM/nHSHRN9KJI9r0xPFu36mBeqwnWJhKqVjUWIGkVg8UGnOp03rPnjF5Ll1V26KIvzjAx5awb
jMTpxUokg4EKeDUSNB04wcLvbNDtIZifaUTDGhWcVoaQArCDaCPkMeZfsLmwu40SBTOua0WHU6lj
uSszhZUZ6GIeHbeWViW87xcUAtbSiKwOX6d/LnfTAHlxUwIDAQABMA0GCSqGSIb3DQEBCwUAA4IB
AQCBeqGFXQhdx5bLjlgEBoF/fsVzyCysb6as5qiUSyCbMu0GKmhMvRBNJIH5rqj+/pgovdrBzDxF
6uK4BtRMx8yZSSs5pbSgbI9Hl07vNZ049IOO4KthE07EV8tO27n2BBmPY/Ux4UKY99G7H7/Gmqbs
bE+x+n9JJIuw5b2QasQg4sM8ezyJkV7cu8emo0c//TUf2ogfKSL967ipCg5ExJgdgI8GcNTSuaf1
XBksV2H75ERyd7GjhBtJ0OkLHvjiNnr8eR+hvRrd1xVMzFDRiDbC98iuSfNbLebF0euVehTJsZyN
j4nywP7VhwkfGA5iN8gX4Gv0lp0DWrafVJpFDBzH
-----END CERTIFICATE-----
```

15. Go back to your *Desko* panel. On **Connection name** field, enter a name for your connection and insert the proper URLs matching the fields as shown below



How to Configure SAML 2.0 for Desko Application

The following is needed to configure Desko

1 Identity Provider Single Sign-On URL:

```
https://inventsys-com.okta.com/app/inventsys-com_desko_1/exkalc5aeGewCpSCx696/sso/saml
```

2 Identity Provider Issuer:

```
http://www.okta.com/exkalc5aeGewCpSCx696
```

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDqjCCApKgAwIBAgIGAX3odiNsMA0GCSqGSIb3DQEBCwUAMIGVMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcm5pYTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZXIxFjAUBgNVBAMMDWludmVudHN5cy1jb20xHDAaBgkqhkiG9w0B
```

SSO SAML 2.0 authentication

Allow users to login to Deskbee with Single Sign On - SSO capabilities. Requires SAML 2.0 configuration on your login provider (AD Microsoft or G Suite)

Allow users to login to Deskbee with SSO via SAML: On

Connection name: Desko_Okta

Identity ID (Identifier URL): http://www.okta.com/exkalc5aeGewCpSCx696

Login URL: https://inventsys-com.okta.com/app/inventsys-com_desko_1/exkalc5aeGe

Logout URL:

Base 64 SAML Certificate: Update certificate

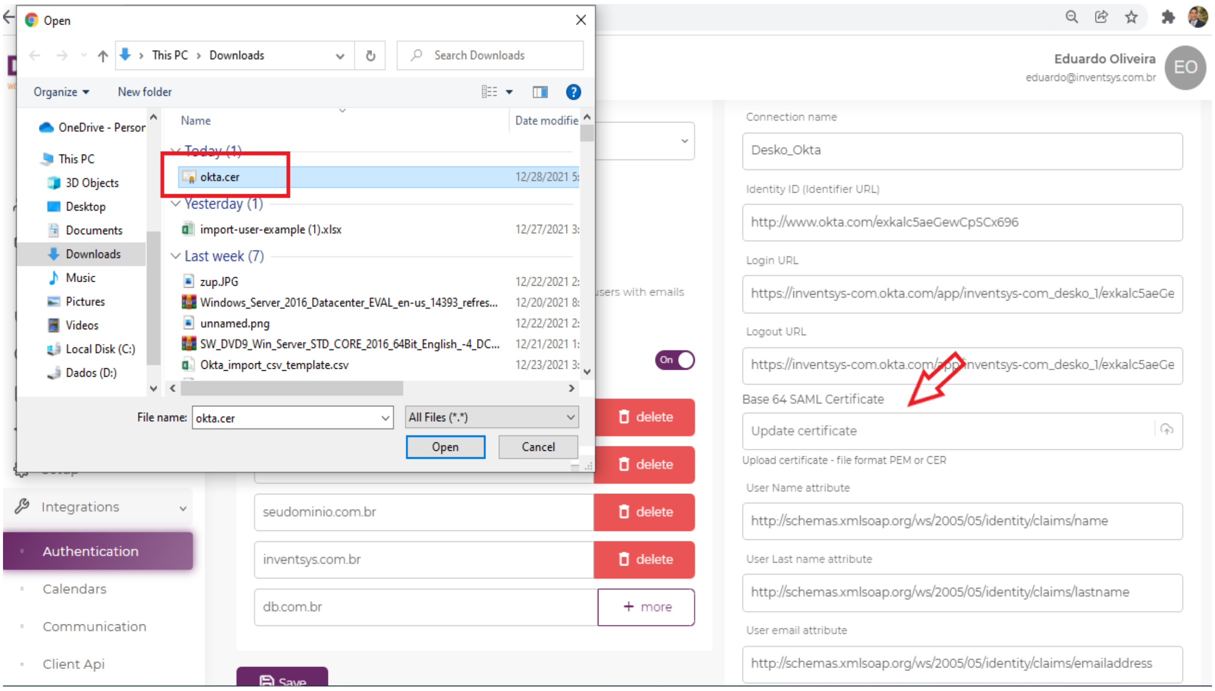
Upload certificate - file format PEM or CER

User Name attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

URLs from Okta Admin portal that should match on *Desko* Panel:

Okta Admin Portal	***Desko* Panel**
Identity Provider Single-Sign-On URL	Login URL
Identity Provider Issuer	Identity ID (Identifier URL)

16. Upload Okta Certificate that you downloaded in the item 11 by clicking on **Update certificate** field. Before select the cert file, rename it from ***okta.cert*** to ***okta.cer*** (just change the file extension). Then select **okta.cer** and upload it



seudominio.com.br

inventsys.com.br

db.com.br

Connection name: Desko_Okta

Identity ID (Identifier URL): http://www.okta.com/exkalc5aeGewCpSCx696

Login URL: https://inventsys-com.okta.com/app/inventsys-com_desko_1/exkalc5aeGe

Logout URL: https://inventsys-com.okta.com/app/inventsys-com_desko_1/exkalc5aeGe

Base 64 SAML Certificate: Update certificate

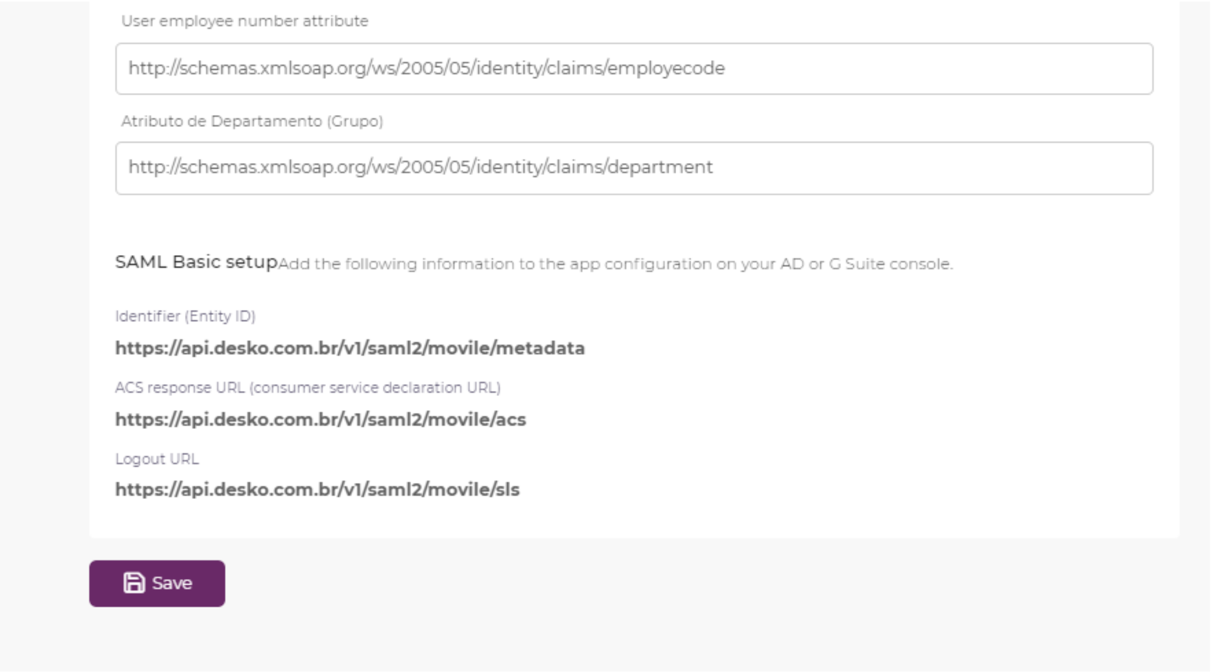
Upload certificate - file format PEM or CER

User Name attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name

User Last name attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/lastname

User email attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress

17. Scroll down to the bottom of the page and click on **Save** button



User employee number attribute: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/employecode

Atributo de Departamento (Grupo): http://schemas.xmlsoap.org/ws/2005/05/identity/claims/department

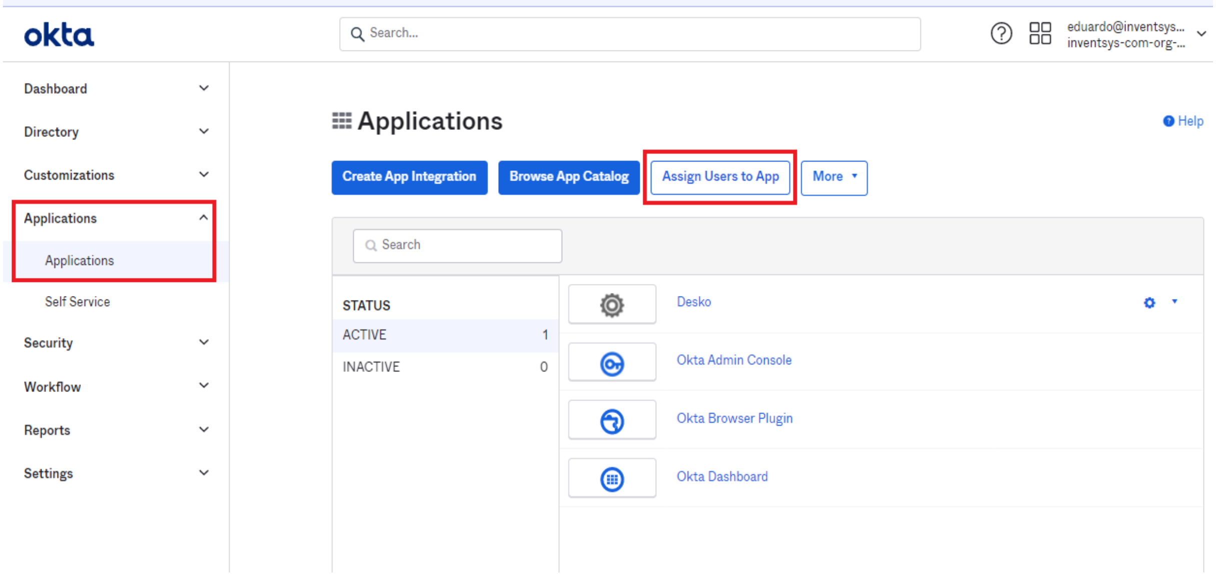
SAML Basic setupAdd the following information to the app configuration on your AD or G Suite console.

Identifier (Entity ID)
https://api.desko.com.br/v1/saml2/movile/metadata

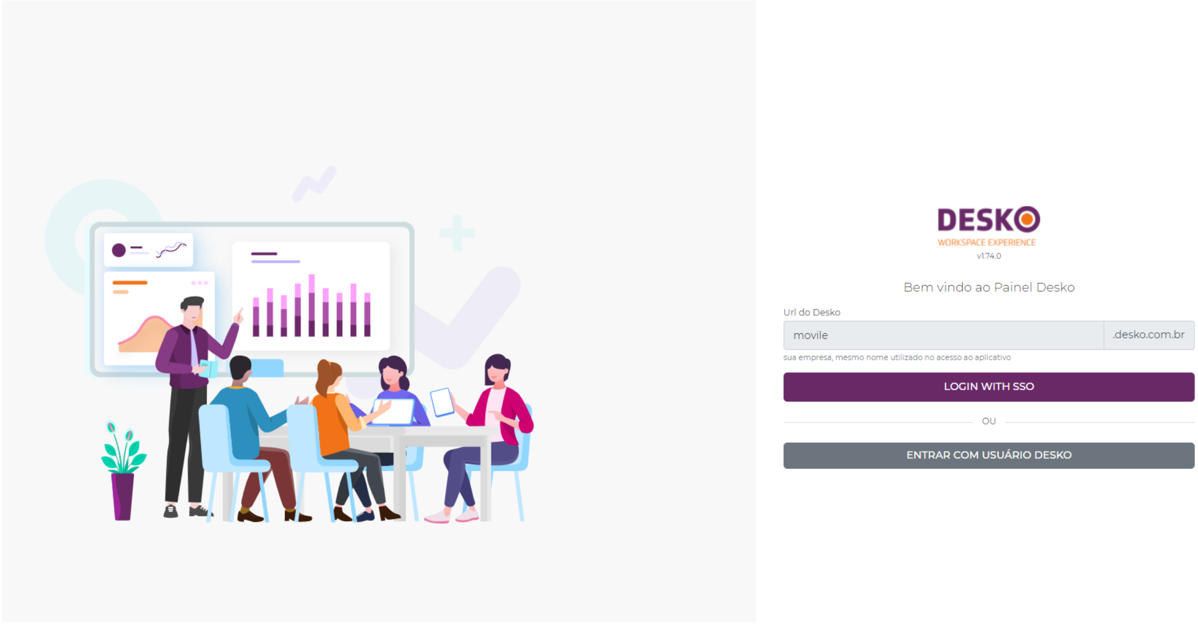
ACS response URL (consumer service declaration URL)
https://api.desko.com.br/v1/saml2/movile/acs

Logout URL
https://api.desko.com.br/v1/saml2/movile/sls

18. In order to make the *Desko* app available to allowed users, do not forget to add them in your Okta Admin portal by clicking on **Applications** and **Assign Users to App**



19. To access your *Desko* app, just head over to https://**<YourCompanyName>.desko.com.br** and click on the button you named for your login method.



Bem vindo ao Painel Desko

Url do Desko: movile .desko.com.br

sua empresa, mesmo nome utilizado no acesso ao aplicativo

Versioning

Version	Author	Date
v1.0	Eduardo de Oliveira	01/03/2022