

# Vorex and Okta - SAML 2.0 Single Sign-On (SSO) Just-in-Time (JIT) Provisioning

Release 4.0.27 | Version 1.0



# Copyright Agreement

The purchase and use of all Software and Services is subject to the Agreement as defined in Kaseya's "Click-Accept" EULATOS as updated from time to time by Kaseya at <http://www.kaseya.com/legal.aspx>. If Customer does not agree with the Agreement, please do not install, use or purchase any Software and Services from Kaseya as continued use of the Software or Services indicates Customer's acceptance of the Agreement.

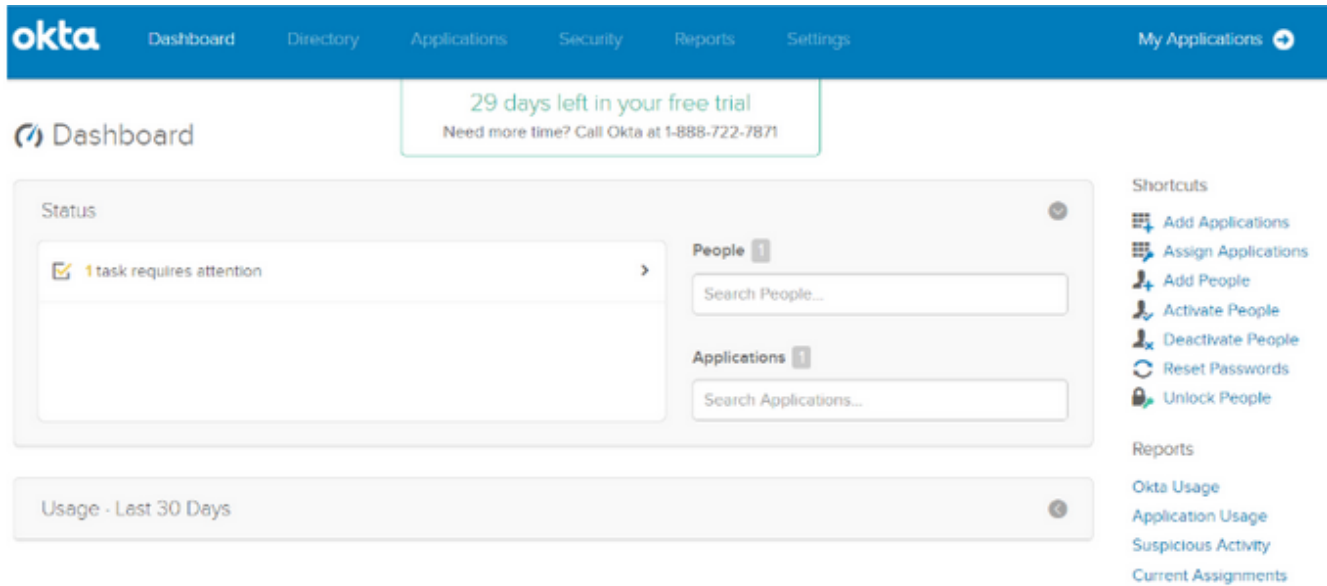
# Contents

---

<b>Okta Setup</b> .....	<b>4</b>
<b>Download the Certificate</b> .....	<b>12</b>
<b>Vorex Setup</b> .....	<b>14</b>
<b>Okta Application Assignment</b> .....	<b>15</b>
<b>Enable Two Way SAML Login</b> .....	<b>16</b>
<b>Enable JIT Provisioning</b> .....	<b>19</b>

# Okta Setup

Assuming we have an active Okta (<https://www.okta.com/>) account, we need to login and navigate to the admin dashboard.

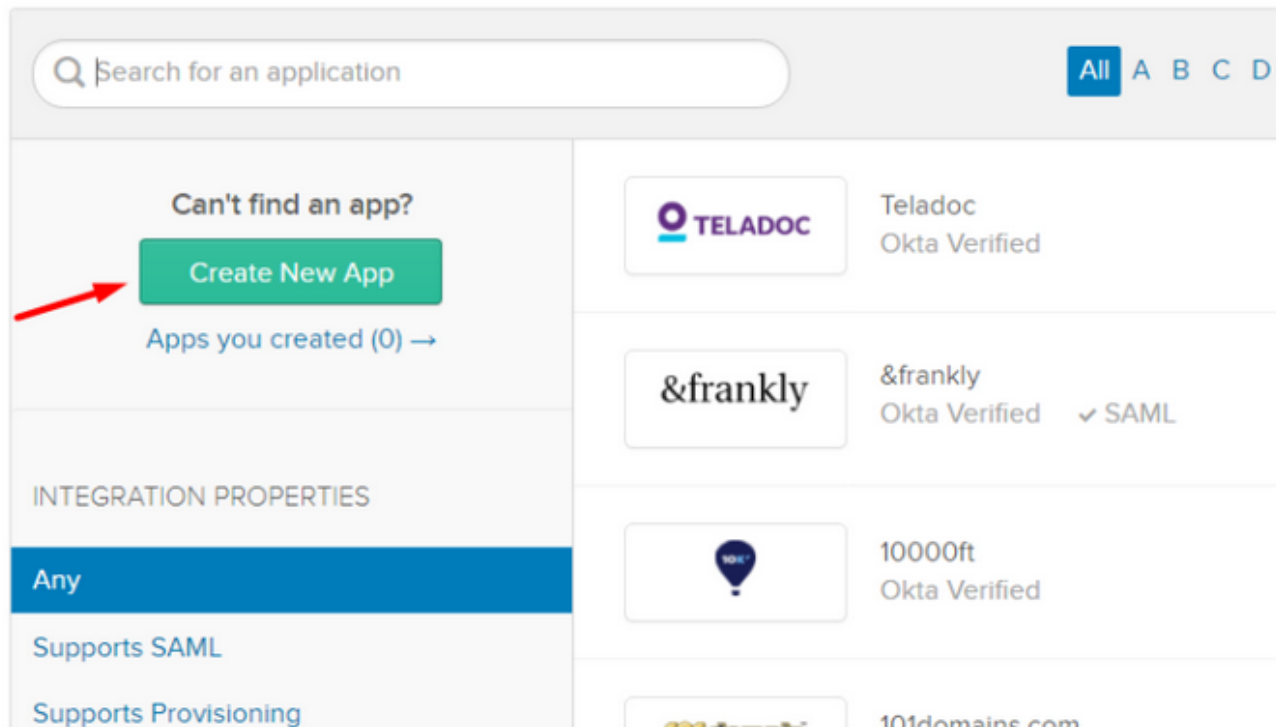


The screenshot displays the Okta Admin Dashboard. At the top, a blue navigation bar contains the Okta logo and menu items: Dashboard, Directory, Applications, Security, Reports, and Settings. On the right side of the navigation bar is a "My Applications" link with a dropdown arrow. Below the navigation bar, a green banner indicates "29 days left in your free trial" and provides the contact number "1-888-722-7871". The main content area is titled "Dashboard" and features a "Status" section with a notification for "1 task requires attention". To the right of the status section are search boxes for "People" and "Applications". Below the status section is a "Usage - Last 30 Days" section. On the right side of the dashboard, there is a "Shortcuts" menu with options: Add Applications, Assign Applications, Add People, Activate People, Deactivate People, Reset Passwords, and Unlock People. Below the shortcuts is a "Reports" menu with options: Okta Usage, Application Usage, Suspicious Activity, and Current Assignments.

In order to setup Vorex with Okta we need to add it as a new application. Adding a new application can be done from the "Applications" section in the menu, or by clicking the shortcut in the dashboard right menu "Add Applications".

[← Back to Applications](#)

## Add Application



Q Search for an application All A B C D

Can't find an app?

[Create New App](#)

Apps you created (0) →

INTEGRATION PROPERTIES

Any

Supports SAML

Supports Provisioning

TELADOC Teladoc Okta Verified

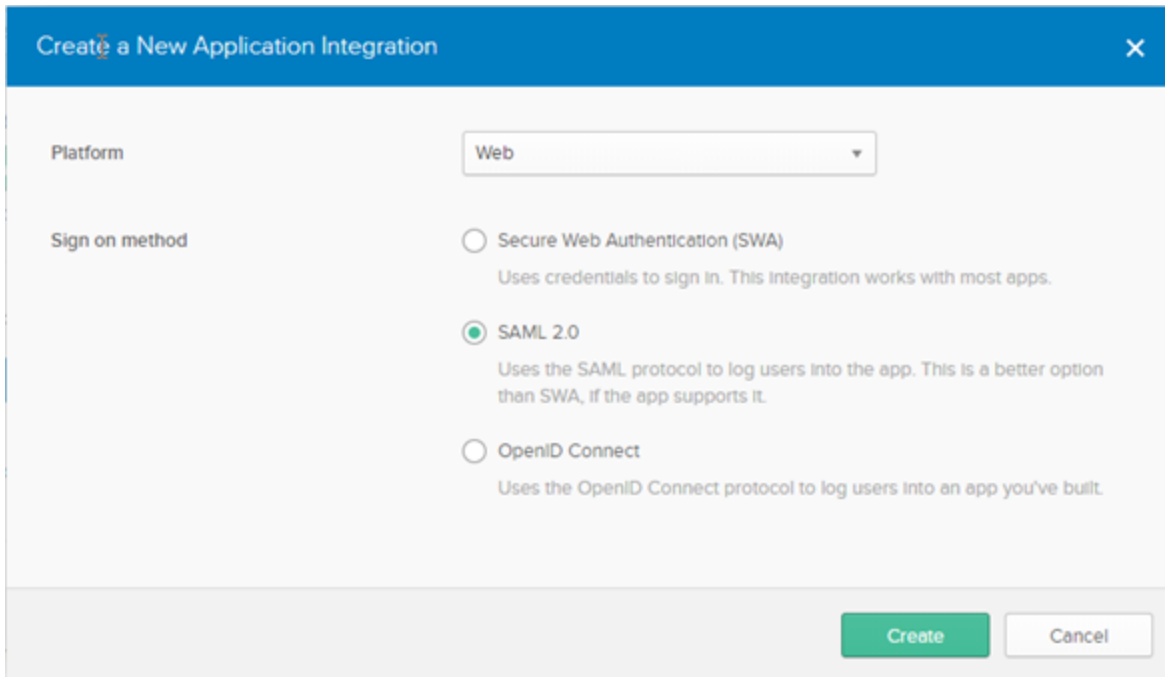
&frankly &frankly Okta Verified ✓ SAML

10000ft 10000ft Okta Verified

101domains.com

In the wizard following the click of Create New App, select the following options:

- **Platform:** Web
- **Sign on method:** SAML 2.0



**Create a New Application Integration** [X]

Platform: Web

Sign on method:

- Secure Web Authentication (SWA)  
Uses credentials to sign in. This integration works with most apps.
- SAML 2.0  
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect  
Uses the OpenID Connect protocol to log users into an app you've built.

[Create] [Cancel]

Then we can start setting up our application starting by the (1) General Settings:

- **App name:** Kaseya BMS
- **App logo:** Provide a logo for the application
- **App visibility:** Keep the defaults

Hit Next and let's configure the SAML (2):

- **Single sign on URL:**
  - We can get this URL from BMS by navigating to Admin > My Company > Authentication
  - Under the single sign on URL, copy the URL in the field and set it in Okta
  - **Example:** <https://vorex.kaseya.com/SAML/Connect.aspx>
- Check the checkbox saying: "Use this for Recipient URL and Destination URL"
- **Audience URI (SP Entity ID):** KaseyaVorex
- **Application username:** Email

**GENERAL**

Single sign on URL ?

Use this for Recipient URL and Destination URL

Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ?

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

---

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text"/>

---

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/>

Select the link ["Show Advanced Settings"](#) to expand the advanced settings section.

Keep the defaults and change the following:

- **Assertion Signature:** Unsigned
- **Authentication context class:** Unspecified

Response	Signed
Assertion Signature	Unsigned
Signature Algorithm	RSA-SHA256
Digest Algorithm	SHA256
Assertion Encryption	Unencrypted
Enable Single Logout	<input type="checkbox"/> Allow application to initiate Single Logout
Authentication context class	Unspecified
Honor Force Authentication	Yes
SAML Issuer ID	http://www.okta.com/\${org.externalKey}

Now we can set the additional attribute statements needed for the SAML setup. Under the section saying “ATTRIBUTE STATEMENTS (OPTIONAL)” add two (2) new attributes:

- **Attribute 1:**
  - Name: email
  - Format: Basic
  - Value: user.firstname
- **Attribute 2:**
  - Name: CompanyName
  - Format: Basic
  - Value: {tenant-name}
- **Attribute 3:**
  - Name: firstname
  - Format: Basic



- Value: user.firstname

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

Name	Name format (optional)	Filter
securitygroup	Unspecified ▼	Matches regex ▼ .*

- **Attribute 4:**
  - Name: lastname
  - Format: Basic
  - Value: user.lastname
- **Attribute 5:**
  - Name: username
  - Format: Basic
  - Value: user.login
- **Attribute 6 (Group Attribute):**
  - Name: securitygroup
  - Format: Unspecified
  - Matches regex: .\*

**ATTRIBUTE STATEMENTS (OPTIONAL)** [LEARN MORE](#)

Name	Name format (optional)	Value	
email	Basic	user.email	
CompanyName	Basic	My Company Name	×
firstname	Basic	user.firstName	×
lastname	Basic	user.lastName	×
username	Basic	user.login	×

[Add Another](#)

---

**GROUP ATTRIBUTE STATEMENTS (OPTIONAL)**

Name	Name format (optional)	Filter
securitygroup	Unspecified	Matches regex .*

[Add Another](#)

For the Final step of the configuration (3) Feedback, you can set the application is internal as shown in the following screenshot, and finish the setup.

## Create 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

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

App type **i**       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.

Previous      Finish

# Download the Certificate

Once the setup is completed, you will be redirected to the application configuration page. Under the tab called “Sign On”, click in the content on the button stating “View Setup Instructions”, this will redirect to a page holding the certificate which can be downloaded to be used when setting up Vorex.

← Back to Applications



Kaseya BMS

Active ▾



View Logs

General

Sign On

Import

Assignments

Settings

Edit

## 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.

SAML 2.0

Default Relay State

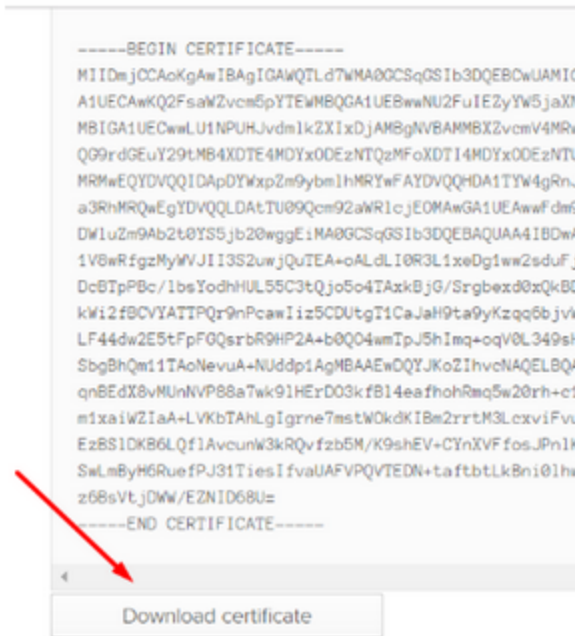


SAML 2.0 is not configured until you complete the setup instructions.

View Setup Instructions

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

After being redirected look for the Download Certificate button and click it to save the file.



After downloading the certificate we just need to rename the extension of the file from “.Cert” to “.Cer”

# Vorex Setup

In Vorex we need to setup the system to enable SAML authentication and that can be achieved under *Admin > My Company > Authentication*.

- 1 In the “Single Sign On” Tab, upload the certificate downloaded previously, and set **Yes** to the radio button “Enable Single Sign On via SAML”, then click **Save**.

Single Sign On **Authenticator**

Enable Single Sign On via SAML:  
 Yes  NO

Single sign on URL:

SAML Login Endpoint URL:

**Certificate Information**

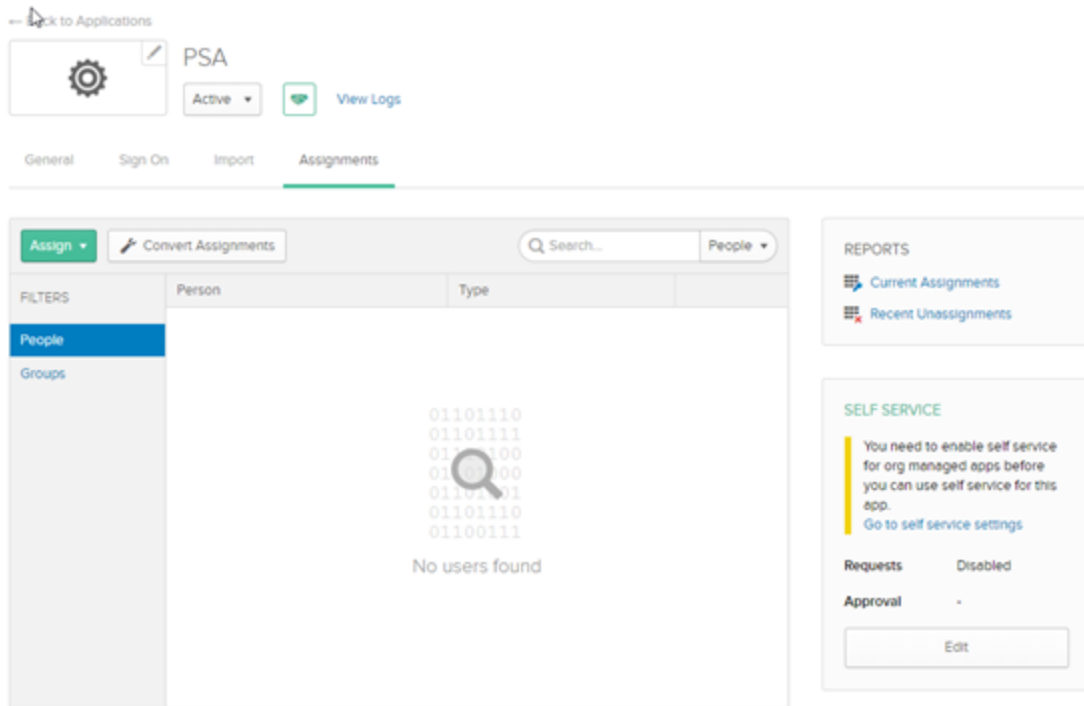
<b>Certificate Name:</b> ADFS Signing - getmytools.io	<b>Certificate Created Date:</b> 08/09/2019
<b>Certificate Version:</b> 3	<b>Certificate Expiry:</b> 08/08/2020
<b>Certificate Signature Algorithm:</b> sha256RSA	<b>Certificate Serial Number:</b> 5B1298C48D3C39B0478D29C60C3BBDF4

This will enable Vorex SAML authentication.

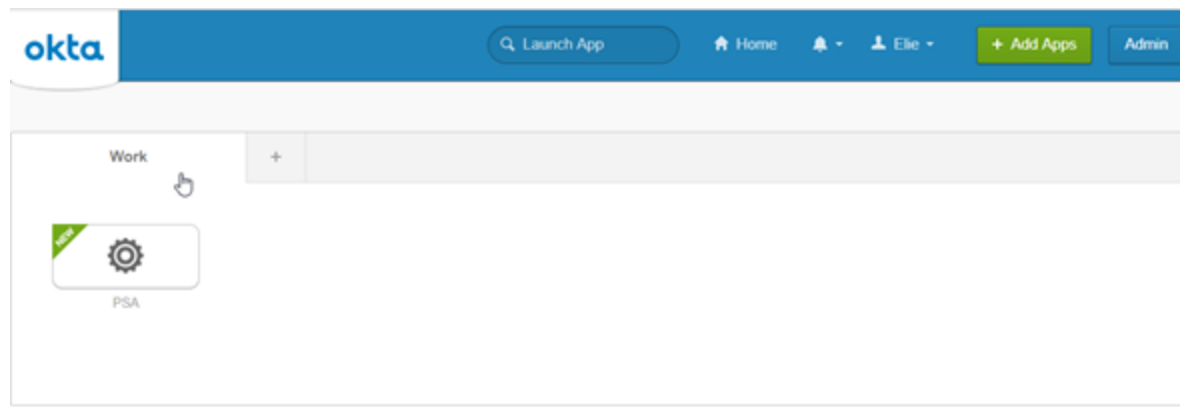
# Okta Application Assignment

In order to launch Vorex using Okta, we must first assign the users in Okta to the created application, and second we need to make sure that the users we are assigning, have **the same email address in OKTA as a username in Vorex**.

Under the application settings page, navigate to the Assignments tab, click Assign button and add Okta users to the application.



Now when the user assigned, login to OKTA and navigate to his applications Dashboard he will see Vorex as one of the applications and can click on it to directly open Vorex logged in.



# Enable Two Way SAML Login

In order to launch Okta during the Log in from Vorex. You need to enable two-way SAML integration. In order to do this, you will need your Authnurl Login URL that can be found here:

The following is needed to configure PSA

1 Identity Provider Single Sign-On URL:

https://newcoredigitaldev.okta.com/app/newcoredigitalorg596301\_psa\_1/exk17tzwi0d15k25C357/sso/saml

2 Identity Provider Issuer:

http://www.okta.com/exk17tzwi0d15k25C357

3 X.509 Certificate:

-----BEGIN CERTIFICATE-----
MIIDeJOCAPqA...
Download certificate

Once you have this URL, you will need to save it in Vorex under the Authentication Page:



Single Sign On

Authenticator

Enable Single Sign On via SAML:  
 Yes  NO

Single sign on URL:  
https://na1bmspreview.kaseya.com/SAML/Connect.aspx

SAML Login Endpoint URL:

Certificate Information

<b>Certificate Name:</b> info@okta.com, CN	<b>Certificate Created Date:</b> 08/09/2019
<b>Certificate Version:</b> 3	<b>Certificate Expiry:</b> 08/09/2029
<b>Certificate Signature Algorithm:</b> sha256RSA	<b>Certificate Serial Number:</b> 016C7551D71B

Upload Certificate Delete Certificate

Auto-Provision Users:  
 Yes  NO

This will allow you to leverage the Okta Log in screen when users are trying to log in to Vorex. You can enable this on the User Level by updating the Authentication Type on the Employee Level:

✓ Save (S) Save and Add New Cancel (C) Delete (D) Refresh (R)

Personal Details | Contact Info | Wages | Shifts | Associated Accounts | Associated Queues | Cl

User Name:\*  
Employe

Emp ID:\*  
4596

First Name:\*  
First

Middle Name:

Last Name:

Email Address:\*  
email

Job Title:\*  
Administrator

Department:\*  
Administration

Location:\*  
Main Branch

Employment Type:\*  
Full Time

Manager:\*  
Belle

Hire Date:

Termination Date:

Birth Date:

SSN:


Marital Status:

Status:  Active  InActive External:  Yes  No

Gender:

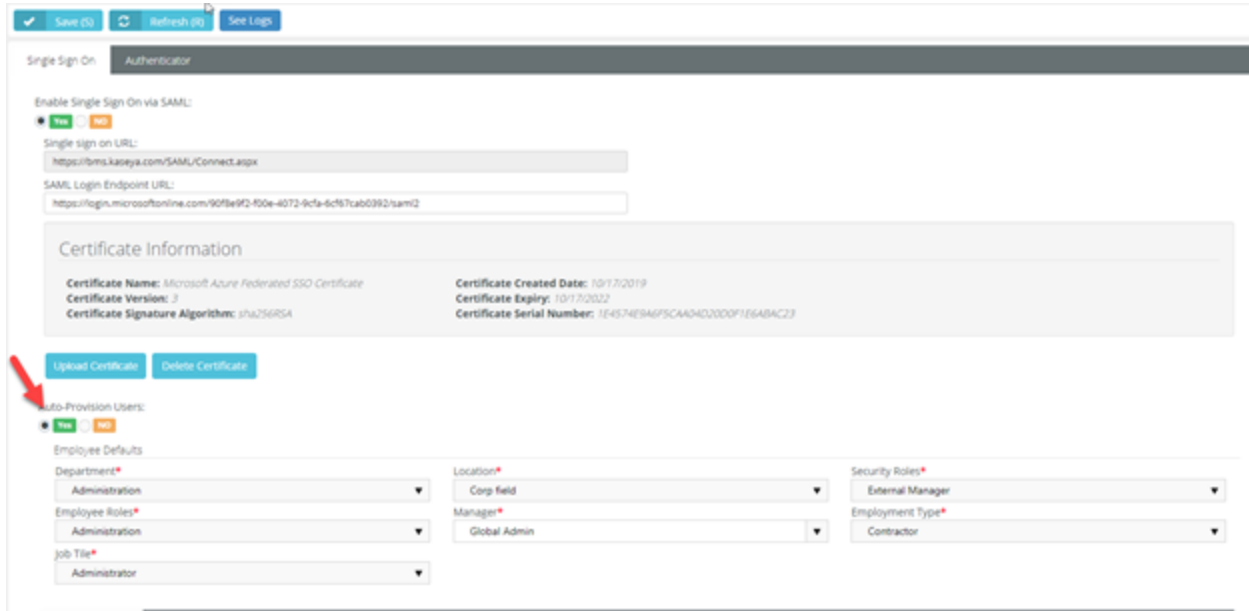
External Authentication Type:  
 None  AuthArvill  SAML SSO

Notes:



# Enable JIT Provisioning

In order to enable Just-in-Time(JIT) provisioning, you will need to do it from the Vorex Authentication page.



By default, all Users will take the Default Security Roles specified in the above Employee Defaults Section. In order to start mapping Active Directory Groups to Vorex Security Roles you will need to Add Mapping Rules as following:

☰ Add/Edit ✕


---

### Add/Edit Mapping Rule


---

Domain

Security Group\*

Map user to  
 **Employee**   
 **Contact with Client Portal Access**

Order

Security Roles\*  
 

By adding multiple Rules, you can now start routing Active Directory Users to Vorex Security Roles based on Domain and Security Group.