

Okta

Okta provides a flexible yet simple Identity Provider solution that integrates easily with the Frame platform. Following the steps below, you simply need to locate, copy, and paste certain values between platforms. This process should take less than fifteen minutes. Refer to Okta documentation for additional information on how to configure Okta.

Attention

Please be aware that while Okta does have a pre-built Frame app, this app does not yet support group attributes. In order to use group attributes, you must configure the application manually as described below.

Getting Started

To begin, let's create a URL-friendly SAML2 Application ID (also referred to as Entity ID) that we'll use in a few places throughout our setup, as well as a Custom Label which will be displayed on the login page for users, for example.

Application ID: DC-OKTA-DEV
Custom Label: Frame-OKTA

Also copy the Assertion URL

Click "add" to save the changes for later

Follow the steps to create a SAML 2 Provider explained in the [General SAML2 Integration](#) section, until you see until you see the template with the missing configuration info, and copy the Metadata URL which will be needed later in the setup. From here leave the tab open, and continue with the configuration in the Azure console.

Update SAML2 identity provider



Application Id

DC-OKTA-DEV

This field is sometimes referred to as the "Entity ID" or "Audience URI." It can technically be any text but is usually in the form of a URL and is often simply "https://use.difr.com".

Auth provider metadata

URL XML

https://integrator-6483706.okta.com/app/exkxf17vi0EUxXraE697/sso/saml/metadata

Your Identity Provider provides this metadata. It's best practice to use a publicly accessible URL, but some situations require the use of static XML metadata.

Custom Label

Frame-OKTA

This label is visible on the Frame log-in page for your users.

Authentication token expiration

5 minutes 7 days
1 hour

Signed response



Signed assertion



Frame Login URL (Optional)

User is directed to this URL when the user wants to log back into Frame after being logged out due to inactivity.

Frame Logout URL (Optional)

User is directed to this URL when the user logs out of the Launchpad or if they decide to leave Frame after being logged out due to inactivity.

Assertion URL:

https://api.staging.difr.com/iam/acdee5d3-cc7b-48a5-bad7-48d85f3a83da/login/done

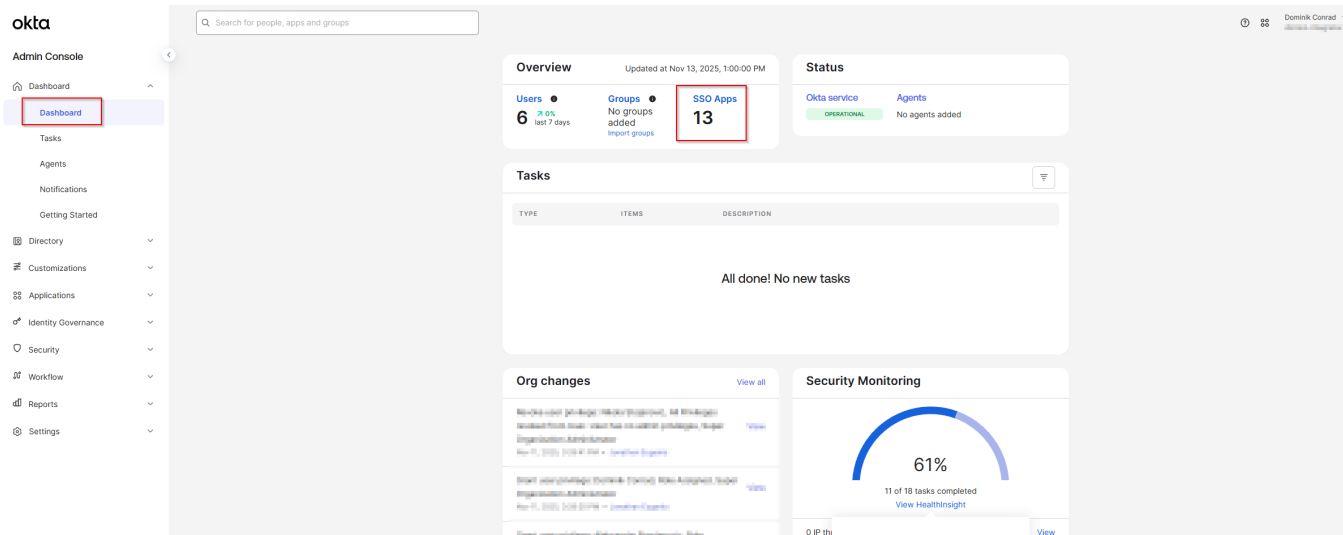
Metadata URL:

https://api.staging.difr.com/iam/acdee5d3-cc7b-48a5-bad7-48d85f3a83da/metadata

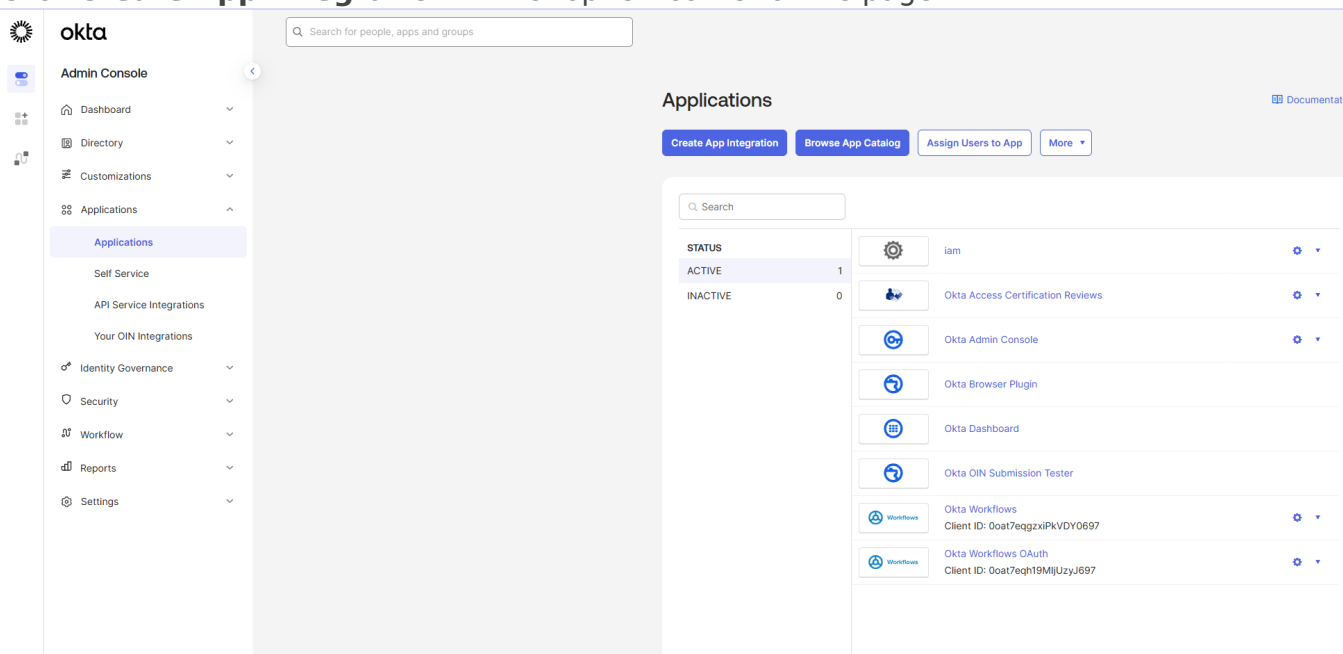
Cancel

Update

1. In a *separate/new tab*, log in to your Okta account as an Admin and open the Dashboard. Select **SSO Apps**.



2. Click **Create App Integration** in the top-left corner of the page.



3. 2. Select **SAML 2.0** and click **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.

[Cancel](#) [Next](#)

4. Provide an app **name** and **icon**. We've provided a Frame icon below for convenience:



🏠 Create SAML Integration

1 General Settings

2 Configure SAML

3 Feedback

1 General Settings

App name

Frame-Okta

App logo (optional)



App visibility

Do not display application icon to users

[Cancel](#)

[Next](#)

- From there, you will be taken to the **SAML Settings** page.

The screenshot shows the 'Create SAML Integration' page. At the top, there are two tabs: '1 General Settings' and '2 Configure SAML'. The 'Configure SAML' tab is active. Below the tabs, there is a section titled 'A SAML Settings'. Underneath, there is a 'General' section with several fields:

- Single sign-on URL**: A text input field containing 'https://api.staging.difr.com/iam/5cdbd7c7-5acd-4152-ξ'. Below it is a checked checkbox labeled 'Use this for Recipient URL and Destination URL'.
- Audience URI (SP Entity ID)**: A text input field containing 'DC-OKTA-DEV'.
- Default RelayState**: An empty text input field. Below it is the text 'If no value is set, a blank RelayState is sent'.
- Name ID format**: A dropdown menu with 'Unspecified' selected.
- Application username**: A dropdown menu with 'Okta username' selected.
- Update application username on**: A dropdown menu with 'Create and update' selected.

At the bottom right of the 'SAML Settings' section, there is a link that says 'Show Advanced Settings'.

- Next, it's time to paste our **AsseractionURL** from the **Getting Started** section of this page.
- Next, we'll enter the following information:**Audience URI**: A DNS-compliant string. For this example, we will use `DC-OKTA-DEV`. This customer-defined string will be entered on the Frame side as our **Application ID** later on. You must use a unique Audience URI for your own IdP integration.
- Default RelayState**: This field can be left blank for SP-initiated SSO scenario. For IdP-initiated SSO scenarios, you will need to specify the URL your IdP will redirect the user to once the user has authenticated to Okta. The value can be a **custom entity endpoint**

URL or a Launch Link URL.

9. Configure how Okta will specify the Subject for the SAML2 assertion.

Name ID format ?	EmailAddress ▼
Application username ?	Email ▼
Update application username on	Create and update ▼

[Hide Advanced Settings](#)

Name ID format: Use value of **EmailAddress**

Application username: Use value of **Email**

10. Select **Show Advanced Settings** in the bottom right corner and the Okta fields shown in the following screen will be visible.

[Hide Advanced Settings](#)

Response ?	<input type="text" value="Unsigned"/>									
Assertion Signature ?	<input type="text" value="Signed"/>									
Signature Algorithm ?	<input type="text" value="RSA-SHA256"/>									
Digest Algorithm ?	<input type="text" value="SHA256"/>									
Assertion Encryption ?	<input type="text" value="Unencrypted"/>									
Signature Certificate ?	<input type="text" value=""/> <input type="button" value="Browse files..."/>									
Enable Single Logout ?	<input type="checkbox"/> Allow application to initiate Single Logout									
Signed Requests ?	<input type="checkbox"/> Validate SAML requests with signature certificates. SAML request payload will be validated. SSO URLs will be read dynamically from the request. Read more									
Other Requestable SSO URLs	<table><thead><tr><th>URL</th><th>Index</th><th></th></tr></thead><tbody><tr><td><input type="text"/></td><td><input type="text"/></td><td><input type="button" value="x"/></td></tr><tr><td colspan="3"><input type="button" value="+ Add Another"/></td></tr></tbody></table>	URL	Index		<input type="text"/>	<input type="text"/>	<input type="button" value="x"/>	<input type="button" value="+ Add Another"/>		
URL	Index									
<input type="text"/>	<input type="text"/>	<input type="button" value="x"/>								
<input type="button" value="+ Add Another"/>										

Update the following fields:

Response: Use value of **Unsigned**

Assertion Signature: Use value of **Signed**

Other Requestable SSO URLs: If you plan to use the Frame Login Page, add a second **Single sign-on URL** with the FQDN **api.difr.com.com** with an index of **1**. For example, <https://img.frame.nutanix.com/saml2/done/docs-frame-okta/> for the above example.

11. **Add three Attribute Statements.** They must be exactly as shown here, including capitalization. Additionally, you can add "Group Attribute Statements" if you wish. We go into detail for passing group attributes/claims in later steps.

Attribute Statements (optional)

[LEARN MORE](#)

Name	Name format (optional)	Value	
sn	Basic ▼	user.lastName ▼	
givenName	Basic ▼	user.firstName ▼	×
mail	Basic ▼	user.email ▼	×

[Add Another](#)


12. Click **Next** and fill out the feedback page as desired.

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

Contact app vendor

- It's required to contact the vendor to enable SAML

Which app pages did you consult to configure SAML?

Enter links, describe where the pages are, or anything else you think is helpful

Did you find SAML docs for this app?

Enter any links here

Any tips or additional comments?

Placeholder text

[Previous](#)

[Finish](#)

13. Click **Finish**.

14. You will automatically be taken to the **Sign On** page/tab where we'll obtain the final piece of information. Scroll down to the bottom box under the *Sign On Methods* section and right-click on the blue **Identity Provider metadata** link. Copy the link URL and save it somewhere to reference in later steps.

The screenshot shows the Okta dashboard interface for a 'Frame-Okta' integration. At the top, there is a logo, a status indicator 'Active', and links for 'View Logs' and 'Monitor Imports'. Below this is a navigation bar with tabs for 'General', 'Sign On', 'Import', and 'Assignments'. The 'Sign On' tab is selected. The main content area is titled 'Settings' and includes an 'Edit' link. Under 'Sign on methods', there is explanatory text about sign-on methods and a link to 'Configure profile mapping'. The 'SAML 2.0' method is selected. A 'Metadata details' section shows the 'Metadata URL' as 'https://integrator-6483706.okta.com/app/exkxf17vi0EUxXraE697/sso/saml/metadata'. A 'Copy' button is highlighted with a red box. A 'More details' link is also visible.

15. The Okta side of the setup is now complete. Next, we'll configure the Frame side of the integration using the the values we've copied from these steps in the Okta Dashboard.

16. Final Steps

Configure the SAML2 Authentication Integration Provider in Frame

1. Navigate back to your Frame tab and enter the following data into our **Add a SAML2 Identity Provider** form:

Update SAML2 identity provider

Application Id

This field is sometimes referred to as the "Entity ID" or "Audience URI." It can technically be any text but is usually in the form of a URL often simply "https://use.difr.com".

Auth provider metadata


URL XML

Your Identity Provider provides this metadata. It's best practice to use a publicly accessible URL, but some situations require the use of XML metadata.

Custom Label

This label is visible on the Frame log-in page for your users.

Authentication token expiration

5 minutes 

Signed response

Signed assertion

Frame Login URL (Optional)

User is directed to this URL when the user wants to log back into Frame after being logged out due to inactivity.

Frame Logout URL (Optional)

User is directed to this URL when the user logs out of the Launchpad or if they decide to leave Frame after being logged out due to inactivity.

Assertion URL: <https://api.staging.difr.com/iam/5cdbd7c7-5acd-4152-9b11-d1e4cfe3ea53/k>

Metadata URL: <https://api.staging.difr.com/iam/5cdbd7c7-5acd-4152-9b11-d1e4cfe3ea53/>

Cancel

- **Application ID:** The value here **needs to match** the value set as the "Entity ID" from Step 5.
- **Auth provider metadata:** Click the "XML" option and paste the contents of the Metadata XML file from Step 4.

- **Custom Label:** Allows Admins to customize Frame's Sign in page chiclets/buttons associated with this SAML2 integration.
- **Authentication token expiration:** Choose a token expiration duration that supports your end-user workflows and complies with your security policies.
- **Enable “Signed assertion”**
- **Assertion Consumer Service (ACS) URL:** The endpoint where the Identity Provider (IdP) delivers SAML authentication responses after a successful login.
- **Metadata URL:** A publicly accessible URL providing your Service Provider's SAML metadata, used by Identity Providers to configure and establish trust.

Optional

- **Frame Login URL:** user is directed to this URL when the user wants to log back into Frame after being logged out due to inactivity.
- **Frame Logout URL:** user is directed to this URL when the user logs out of the Launchpad or if they decide to leave Frame after being logged out due to inactivity.

Click **Add**.

You have successfully created your Okta integration with the Frame platform! Move on to the next section for configuring roles and permissions for your users, as well as information for passing Group attributes to Frame.

Configuring SAML2 Permissions

1. Once the IdP is successfully configured on Frame, administrators will need to configure the authorization rules for the account from the **SAML2 Permissions** tab listed to the right of the **SAML2 Provider** tab, as discussed in our [Roles](#) and [User Permissions with a SAML2 IdP](#) sections.
2. Passing Group Attributes
3. You can authorize any groups of users you want to allow to use the Frame platform based on the user-group assignments you have configured in Okta. We recommend following the guidance of Okta's support team provided [in this link](#) regarding group attribute statements with custom SAML applications.
4. Groups attribute and the associated set of Okta groups to insert in the SAML2 Response can be defined in Okta. In this example, enter `groups` for the group name attribute and define the group name inclusion filter.

Group Attribute Statements (optional)

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

[Add Another](#)

5. Here's an example of a list of groups in Okta:




Groups Help

All Rules

Search by group name

Advanced search ▾

Group source type Showing 3

Group name	People	Applications
 Frame_User No description	1	0
 Everyone All users in your organization	6	0
 Okta Administrators Okta manages this group, which contains all administrators in your organization.		

6. Assuming that one of the Okta groups that is passed to Frame is **Okta-Contractors**, the Frame administrator would specify a SAML2 permission where any user's SAML2 response contains a value of `Okta-contractors` in the `groups` SAML2 attribute will be granted Account Administrator role on Frame account Contractor Account.

Update a rule ✕

For provider

Frame-Okta-Integration-docs

Description

This rule grants basic VDI users access to an application launchpad

Allow access

Always

When all conditions are satisfied

When any condition is satisfied

Conditions

groups contains Text Frame-User

Add

Grant roles

Launchpad User on Applications






Account: Documentation, Organization: William Wong, Customer: Solutions Architecture

Add

7. Signing into Frame with Okta

- Your new SAML2 auth integration will appear as button on your Frame login page. The URL for navigating to your Frame login page will vary depending on which level the SAML2 integration was configured. See our section about [Entities and URLs](#) to help pick the right one for you and your end-users and/or staff.
- When landing on a URL configured for your Okta SAML2 Integration, your end-users should see an option like this:



-  Sign in with email and password
-  Sign in with Google
-  Sign in with Google
-  Sign in with Frame-OKTA
-  Sign in with Google

Revision #8

Created 1 October 2025 04:49:43

Updated 13 January 2026 12:16:29 by Nikola Savic