Duo

Integrating Duo Single Single-On (SSO) is a quick and easy process. Continue reading to learn how to configure your Duo Single Sign-On users with Frame.

Prerequisites

- Administrator access to a Duo Account
- Duo Single Sign-On must be enabled in the Duo Admin Panel
- A configured authentication source such as Active Directory or a SAML IdP (Okta, OneLogin, Google, etc.)

Getting started

Use the URL-friendly SAML2 **Integration Name** that you created in the previous section.

1. First, we will add a new Application in the Duo Admin Panel. Click Applications on the sidebar, then click Protect an Application.

   Protect an Application

2. Next, type generic in the search field to filter applications. Look for “Generic Service Provider for Single Sign-On (hosted by Duo),” and click Protect.

   Generic Service Provider

3. You should see the new Application page. You may see a dialog box requesting you activate Duo's Universal Prompt. This is optional but we recommend it for a better user experience.

   Activate Universal Prompt

When the dialog disappears, you will be taken to your Application's settings page.

4. Scroll down on the Application Page until you see the **Entity ID** form field under **Service Provider**.
5. Now it's time to come up with an **Entity ID** and a URL-friendly **Integration Name** that we will use in the configuration forms between Duo's Application page and Nutanix

Console.

- **Entity ID**: This is typically a URL for the Service Provider, e.g. `https://console.nutanix.com/`. This value will need to match in both Duo and Nutanix Console.

    The Entity ID

6. In the Assertion Consumer Service (ACS) URL field, enter the ACS URL as defined in the Getting Started section of this page.

The forward slash at the end of the URL is required for the integration to work correctly.

```
<figure>

![Assetion Consumer Service (ACS) URL](https://docs.difr.com/uploads/images/gallery/2025-10/duo-sp-acs-url.png)

</figure>
```

7. Leave the **Single Logout URL** and **Service Provider Login URL** blank.
8. Enter `https://console.nutanix.com` in the **Default Relay State** field.

    Mapping SAML attributes

9. Under the **SAML Response** section, change the following:

    SAML Response Settings

    - **NameID format** to `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`.
    - **NameID attribute** you can skip, its default value is exactly what we're looking for (`<Email Address>`).
    - **Signature Algorithm** should be **SHA256**.
    - **Signing Options**, both checked.
10. Under the **Map attributes** subsection of **SAML Response**, we need to specify three custom attributes as follows:

    Default Relay State

    - IdP Attribute `<Email Address>` - SAML Response Attribute: `mail`.
    - IdP Attribute `<First Name>` - SAML Response Attribute: `givenName`.
    - IdP Attribute `<Last Name>` - SAML Response Attribute: `sn`.
11. Scroll down to the **Settings section**, enter `Nutanix Frame` in the **Name field**.
12. Feel free to customize the remaining settings as desired. When you're done, click **Save** at the bottom.

Configure Duo in Frame Admin Console

Open a new browser tab and navigate to https://console.nutanix.com to log in. We will be switching back to this Duo tab to grab a few values shortly.

10. Before a SAML2 identity provider can be added, the administrator must enable SAML2 Providers at a given level by opening a new tab and navigating to the Admin Console. From there, navigate to the **Customer** or **Organization** page (depending on where you wish to add the IdP). Select **Users** from the left-hand menu.
11. Under **Authentication**, enable the **SAML2** toggle and click **Save** in the upper right corner.

```
![Customers Example for Configuring User
Access](https://docs.difr.com/uploads/images/gallery/2025-10/ohfadd-saml2-
2025.png)

</figure>
```

More options will appear next to the Authentication tab, click on the **SAML2 Providers** tab.

12. Click **Add SAML2 Provider**.

    Add a SAML2 Provider

13. A new dialog box will appear. Enter the following values as shown below:

    SAML Provider settings

    - **Application ID**: Paste the **Entity ID** value from Step 5 of the Duo section.
    - **Auth provider metadata**: paste in the metadata URL from our Duo Application page. Navigate to Duo in another tab and copy the metadata URL and paste it into here. This should look something like this: `https://sso-2e394ff8.sso.duosecurity.com/saml2/sp/EEFCL3C8EXAMPLEKA7DW/metadata`.
    - **Integration Name**: Enter the SAML2 Integration name defined in the Getting Started section of this page.
    - Custom Label: Set the label to "Duo" or your company name.
    - **Authentication Token Expiration**: Set the token expiration slider to a duration that makes sense for your users.
    - **Signed Response**: enabled.
    - **Signed assertion**: enabled.

When you're finished, click **Add**.

That's it! You have successfully created your Duo integration with Frame! Move on to the next section to learn more about configuring permissions.

note SAML2 Configuration Lock

Customer Administrators have the option to lock SAML2 IdP configurations at the Customer level of the Frame tenant. When the toggle pictured below is enabled, SAML2 IdP integrations cannot be added from the Organization or Account levels of the Frame tenant.

Configuration Lock

Accessing Frame with Duo

Your Duo integration will now appear to your users as a sign in button on your specific Frame Sign in Page.

Revision #4
Created 1 October 2025 04:50:25
Updated 20 October 2025 19:29:48 by Chris Tusa