General SAML2 Integration

The administrative workflow for setting up a SAML2 identity provider (IdP) consists of the following steps:

1. Enable SAML2 Providers at the desired entity level (Customer, Organization, or Account).
2. Create a SAML2 identity provider in Frame.
3. Enter the necessary configuration information for your new SAML2 identity provider in Frame.
4. Enter the configuration information in your actual SAML2 identity provider.
5. Verify that both sides of the IdP integration are properly configured by attempting to login using your identity provider.
6. Add SAML2 Permissions (authorization rules) at the Customer, Organization, or Account entity level to authorize users to specific roles.

Depending on the specific SAML2 identity provider, you may need to perform Step 4 before Step 3.

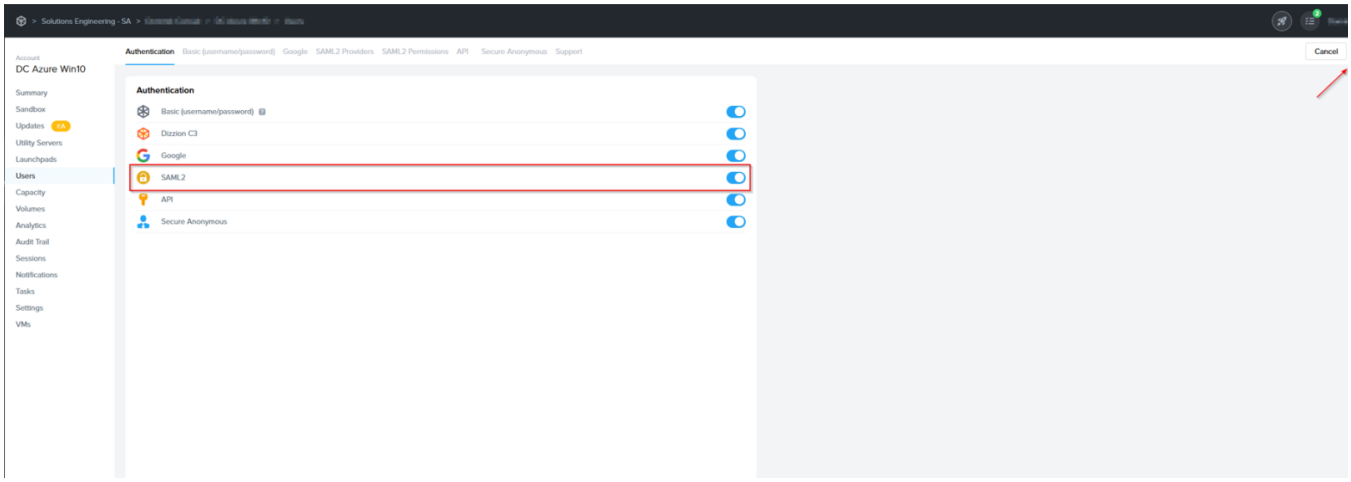
Frame supports both IdP-initiated and SP-initiated authentication workflows. In general, most customers implement SP-initiated authentication workflows by directing users to a Frame URL and letting Frame redirect the user to the SAML2 identity provider.

Getting started

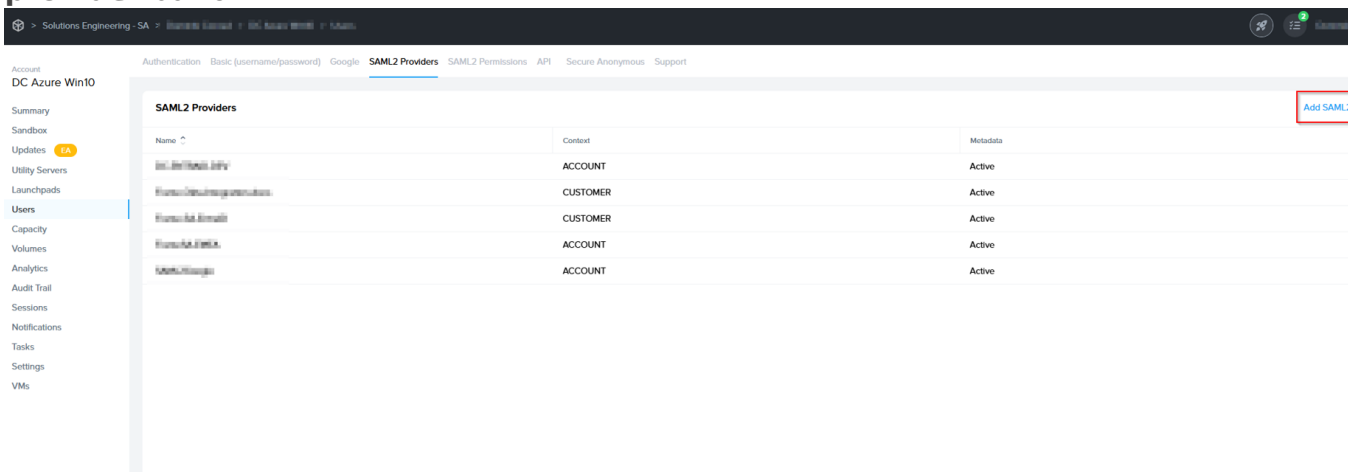
> Before a SAML2 identity provider can be added, the administrator must enable SAML2 Providers at a given level by navigating to the Admin Console. From there, navigate to the **Customer** or **Organization** page (depending on where you wish to add the IdP). Select **Users** from the left-hand menu.

Unless there is a specific reason to do otherwise, adding the SAML2 Provider at the Customer or Organization level is best practice.

2. Enable the **SAML2** toggle under the Authentication tab and click **Save**.

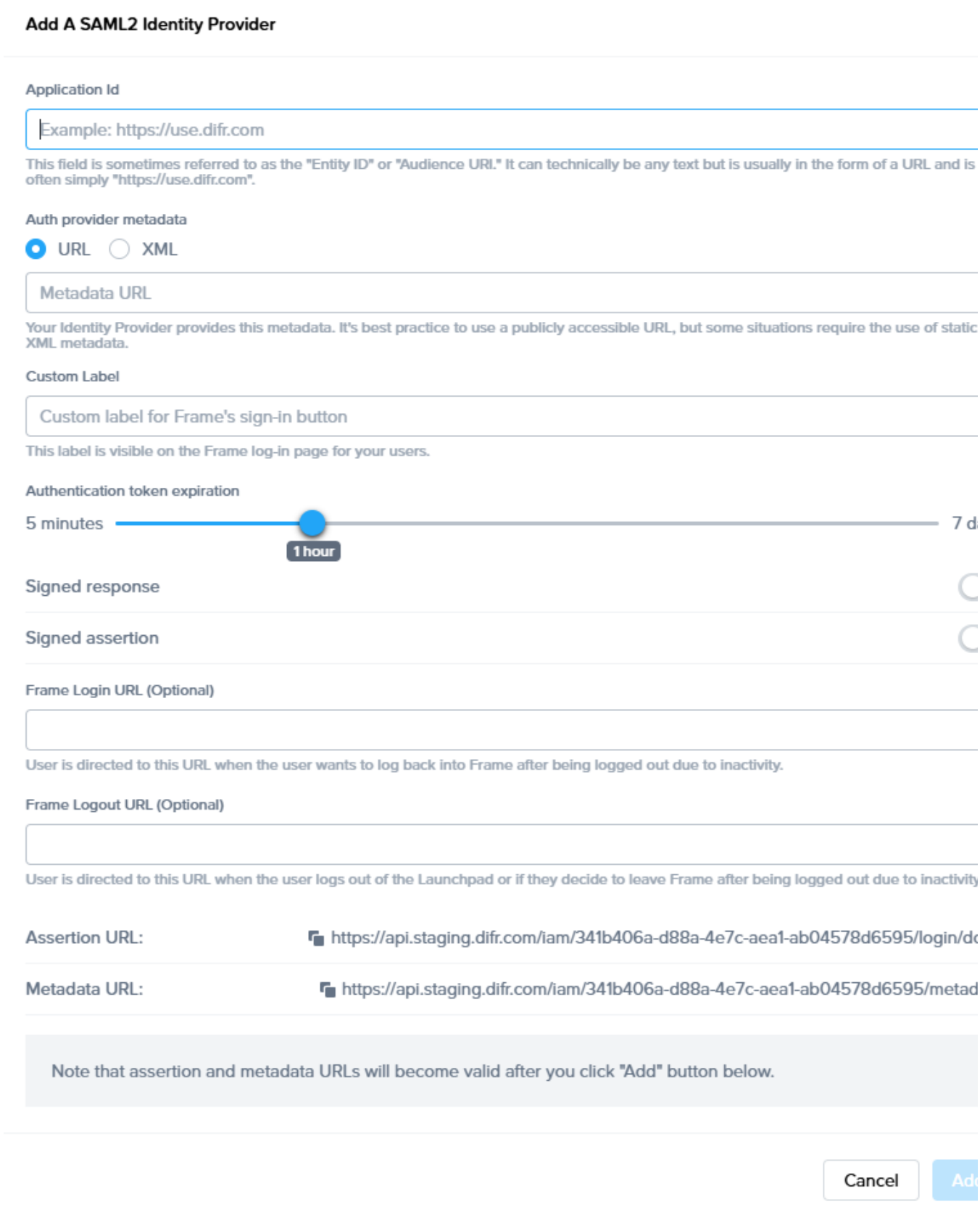


3. You'll see a new "SAML2 Providers" tab appear; click it and you'll see a **Add SAML2 provider** button.



Creating a SAML2 Provider

1. In the SAML2 Providers tab, click **Add SAML2 Provider** at the top right. A dialog to add a SAML2 provider will appear.



- **Application Id**: This field is sometimes referred to as Service Provider (SP) "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. For successful authentication, it is important that value entered in this field matches at least one of the values within "Audience Restriction" list that is part of the SAML2 assertion created by Identity

Provider (IdP).

- **Auth provider metadata**: Check the "URL" option and paste the Identity Provider metadata URL from your SAML2 IdP. The metadata URL must be publicly accessible to Frame Platform on the Internet.
- **Custom Label**: When specified, this value will be used in the login page as `Sign in with <Custom Label>`.

- **Authentication token** expiration: Set the desired expiration time for the authentication token. This can range from 5 minutes to 7 days. If the user is inactive for the configured amount of time, Nutanix Console will logout the user from Nutanix Console. If the user is active within the console (e.g., clicks on hyperlinks, moves the mouse/cursor, scrolls, or presses keys), the token will be renewed just before the user token expires. If the user is in a Frame session, the token is automatically renewed so the user is not disconnected while in session.

- **Signed response**: Disable or enable based on your SAML2 identity provider.
- **Signed assertion**: Disable or enable based on your SAML2 identity provider.

Service Provider URLs
Upon creating a new Integration, your Service Provider is assigned two important URLs:

- **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.

The SAML2 identity provider is typically configured to sign the SAML2 Authentication Response message or the SAML2 Assertion embedded within the Authentication Response message (and not both). The choice of what is signed by the SAML2 IdP must be the same choice in the Frame SAML2 IdP configuration. Otherwise, Frame will return a identity provider misconfiguration error when Frame processes the SAML2 Authentication Response from the SAML2 IdP.

Click Add when ready to create the SAML2 Provider definition.

Configure your SAML2 IdP

3. Each SAML2-compliant identity provider will have its own configuration requirements. However, there are some common configuration parameters used by SAML2 identity providers:
   - **Frame Metadata URL**: This URL is in the form: https://api.use.difr.com/iam/<ID>/metadata.
   - **Single Sign-on URL** or **Assertion Consumer Service (ACS) URL:** This URL is in the form: https://api.use.difr.com/iam/<ID>/login/done.
     The SAML2 IdP will send the SAML2 Authentication Response to this URL.

Caution

> Administrators choosing to cache or store the Frame public key certificates in their SAML2 IdP will need to update those public key certificates when Dizzion renews them.

Note

> Frame does not support the SAML2 Single Logout Request.

Mandatory SAML2 Attributes

1. In order for Frame to display properly the user's first name, last name, and email address in the Dashboard and Launchpad, your SAML2 identity provider configuration must provide these four mandatory user attributes/values using the specified SAML2 attribute names, as described in the following table:

User attribute	SAML2 attribute name

First name	**Use** `givenName`, `/urn:mace:dir:attribute-def:givenName/`, **or** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname` **SAML2 nameFormat:** `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`
Last name	**Use** `sn`, `/urn:mace:dir:attribute-def:sn/`, **or** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname` **SAML2 nameFormat:** `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`
Email address	**Use** `mail`, `/urn:mace:dir:attribute-def:mail/`, `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress`, **or** `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name` **SAML2 nameFormat:** `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`
Name ID	`NameID` **SAML2 nameFormat:** `urn:oasis:names:tc:SAML:2.0:nameid-format:persistent`

Optional SAML2 Attributes

Customers can configure their SAML2 IdP to include additional SAML2 attributes in the SAML2 Authentication Response messages to Frame Console. These SAML2 attributes and their user-specific values can then be referenced when configuring Frame SAML2 Permissions to enforce role-based access control (RBAC).

The most common SAML2 attribute included by administrators in SAML2 Authentication Response messages would be a SAML2 attribute that is associated with a list of groups, such as a list of Active Directory groups, that the user is a member of. This allows the administrator to the SAML2 Permissions based on groups (and not individual user email addresses) and then associate the users to those groups in their IdP (or Active Directory, if their SAML2 IdP is connected to their Active Directory).

Frame also supports two Frame-specific SAML2 attributes to customize the logout/login workflow:

- **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.

- **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.

When adding additional SAML2 attributes, make sure to record the optional attribute name(s) to be used (and possible values). For example:

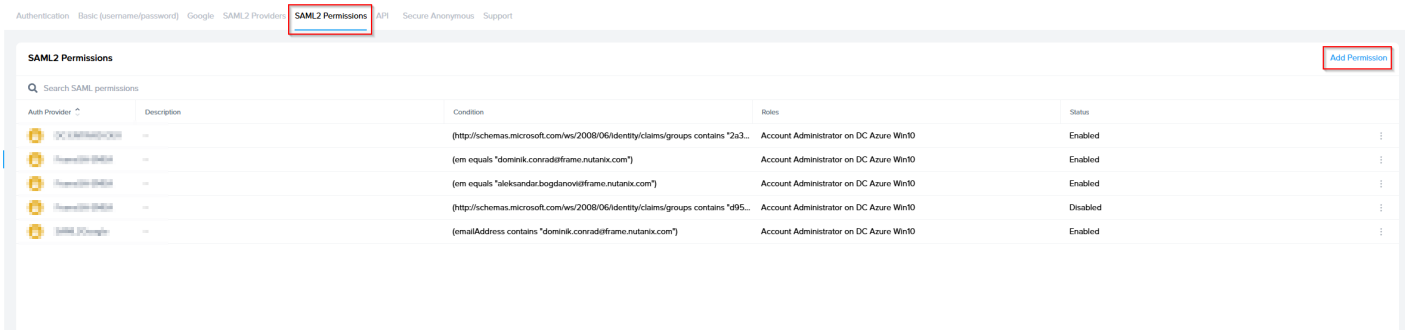
- `groups`
- `Department`
- `http://schemas.xmlsoap.org/claims/Group`
- `http://schemas.microsoft.com/ws/2008/06/identity/claims/groups`

as the exact attribute name must be referenced in the condition section with the appropriate values of a SAML2 Permissions authorization rule.

Configuring SAML2 Permissions

Once the SAML2 Provider is successfully configured in the Nutanix Console, administrators will need to add authorization rules from the SAML2 Permissions tab listed to the right of the SAML2 Provider tab.

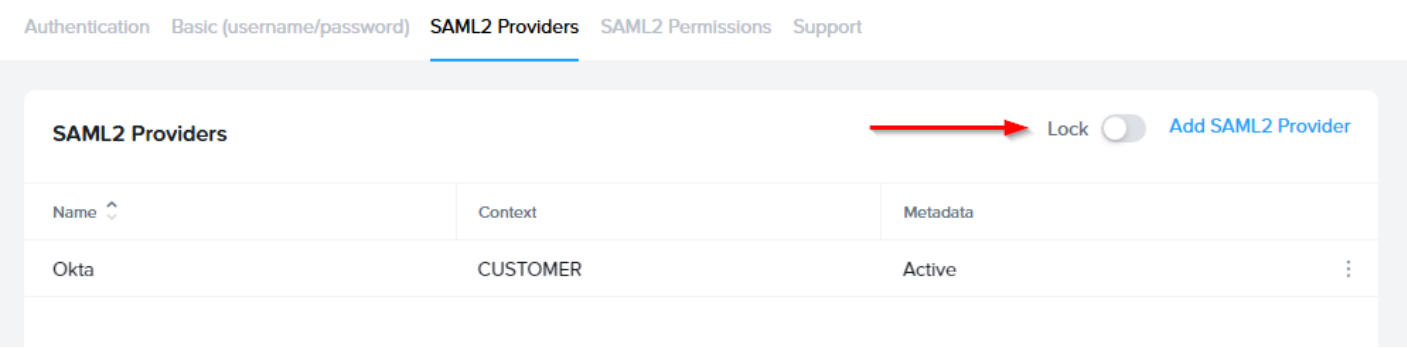
Add roles/permissions for your users by following our Roles and User Permissions with a SAML2 IdP guides.



The Group claim, created in the prior section, must be referenced as `http://schemas.xmlsoap.org/claims/Group` when creating the SAML2 Permission authorization rule.

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.



Signing into Frame with your SAML integration

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

Revision #9
Created 1 October 2025 04:49:40
Updated 3 March 2026 08:39:35 by Dominik Conrad