Authentication

A service that the Frame system can trust to verify the identity of a user is called an “Identity Provider” or IdP. This is a technical term that is commonly used in authentication standards and tools, so we will also use this term in this solution guide.

Broadly, integrating Frame with an Identity Provider means telling Frame which Identity Provider to trust to authenticate users and telling the Identity Provider how to respond to Frame.

Authentication by tier

Auth integration options can be configured at any level within the Frame platform. While most use cases will likely only need authentication at the Customer level, there are scenarios where utilizing custom authentication at different tiers could be beneficial. We will outline some of these scenarios below, starting with the default Customer-level tier.

Customer

Any integrations configured at this level will be used by all users/admins accessing the Platform. This is the default and most common configuration for the Frame platform.

Organization

By setting up authentication at the organizational level, a Customer admin can configure unique integrations for different organizations.

For example, a company with multiple subsidiaries may want to allow those subsidiaries to bring their own authentication. In this case, the company (Customer tier) would allow each subsidiary (Organizational tier) to set up their own authentication.

Account

Account level authentication can be configured by a Customer or Organization admin. While this isn't very common, there are some use cases that would benefit from this arrangement. For instance, a Managed Service Provider (MSP) would benefit from letting each of their customers (divided by Accounts) integrate with their own authentication provider.

Choosing the Right Authentication Option

Choosing the right authentication option depends on the particular use case an organization would like to make of the Frame platform and what authentication options that organization already has in place. This can be determined by answering the following questions:

Do you need to know who the users are?

It's not always necessary to know who is using the applications on Frame. An example might be a software vendor who wants to use Frame to provide a 15 minute demo of their product. Individual users will be arriving from a link in an email or promotional page and the goal may be to have them fill out a feedback form at the end of the demo so that a sales representative can contact them. In this case, the application doesn't need to know who the user is, even though the feedback form may ask for contact information. Anonymous Users would be a good option in this case.

On the other hand, an enterprise who needs to track individual user licensing for software tools used throughout the day by employees would want to each user to be authenticated. Likewise, if it's necessary to remember individual preferences and settings for each user, it's first necessary to know who the user is. Of course, if these users need to gain access to sensitive and confidential information, it's required to know who the user is. In these cases, user authentication would be necessary, but we need to ask another question before we know which one.

Do you already keep track of all of these users somewhere?

Many organizations already have an Identity Provider in place. Therefore, it makes sense to extend that Identity Provider to work with Frame as well. This is often called a Single Sign-On (SSO) solution. SSO is another way to talk about authentication, and an SSO provider and an Identity Provider are different ways of talking about the same thing.

On the other hand, if an organization does not have an existing Identity Provider (SSO solution) in place, Frame has a built-in Identity Provider that the organization can use. This built-in Identity Provider would only be used to authenticate users to the Frame platform and cannot be used to provide an SSO solution across all platforms for an organization. The Frame Identity Provider only provides authentication using a username and password. It does not support 2-factor authentication, or user groups. Account administrators manage users and other account administrators in the Basic Authentication through the Frame Launchpad web application.

If the organization needs an SSO solution for all of its platforms, then a SAML2 Identity Provider is appropriate.

Are you using a SAML2 identity provider already?

An organization with an existing Identity Provider may already be using a SAML2 Identity Provider. In that case, it makes sense to integrate (federate) that same provider with Frame rather than adopting a new IdP for only a single integration (to Frame).

An organization may, however, have an Identity Provider that is not SAML2-based and which is only visible within that organization's corporate network. An example might be an organization using Active Directory to manage users and provide SSO. Rather than exposing the Active Directory server to the public Internet using the Active Directory Federation Service (ADFS) and incur the cost and upkeep of managing and protecting that service from threats and downtime, it can make sense to connect the internal IdP to a SAML2 IdP using the plugins provided by all SAML2 providers. Then, the SAML2 IdP takes on the responsibilities for managing a service exposed on the public Internet. For our example, that Active Directory instance might be connected to Microsoft's Azure Active Directory (Azure AD) using Azure AD Connect. Then Azure AD becomes the SAML2 Identity Provider. Frame can integrate with Azure AD, and the organization can continue to manage all users, right in the same Active Directory that it already has in place.

After selecting a particular authentication option, the details of the next steps will differ, but each option is designed to provider a quick and easy setup for the most common cases. Special cases may require some help from a Frame Solution Architect.

Authentication Option Quick Reference

	Frame IdP	**SAML2 IdP**
Requires SSO Configuration	No	Yes
Granular control of Authentication Security	Yes	Yes
User Attribution	Yes	Yes
Custom Password Policies	No	Yes
2-Factor Authentication	No	Yes
Requires Launchpad	Yes	No
Works With Launchpad	Yes	Yes
Works with Frame Application API	No	Yes

Frame Basic Authentication

By default, Frame provides an Identity Provider for authenticating Frame users. Users are listed in User Settings as part of Frame Dashboard, and can be invited, promoted to admins themselves or retired. Using this option, user names must be unique email addresses. Users are able to set and reset their own passwords.

> Basic Authentication should be used for proof of concept, development, and testing purposes **only**. Basic Authentication does not provide user/password management capabilities (password expiration, password complexity policies, or multi-factor authentication). Frame strongly recommends customers use a third-party SAML2 identity provider for user authentication.

Benefits

Frame's Basic Authentication is an easy way to manage users and it requires no special setup, integration or configuration. Users will be authenticated to Frame which provides the unique user identities required for optional features like persistent user profiles and end-user billing.

Applicability

Basic Authentication can be a convenient authentication solution for a single classroom, small business or a single workgroup under 100 members. It can become cumbersome with more users or if there is a frequent need to add and remove users.

Requirements

There are no special requirement for this option. All authentication options except Anonymous Users require that user identities (email addresses) be unique across all Frame accounts. This option requires the administrator to use the Frame Dashboard to manage the users.

Limitations

The Frame Basic Authentication option can only provide a simple, username and password based, authentication. This option does not support 2-factor authentication, user groups, custom password strength policies or password expiration policies. For these reasons, Basic Authentication should be used for proof of concept, development, and testing purposes **only**.

SAML2 Identity Provider

SAML2 Identity Providers assume the responsibility of maintaining and protecting a publicly visible web service while providing convenient ways to connect that service to on-premises directories and identity providers like Active Directory, Shibboleth, or LDAP servers.

Benefits

SAML2 Identity Providers assume the responsibility of maintaining and protecting a publicly visible web service while providing convenient ways to connect that service to on-premises directories and identity providers like Active Directory, Shibboleth, or LDAP servers.

Applicability

If your organization already manages users in a central place, then a SAML2 Identity Provider can be a convenient way to extend that control to external services like Frame.

Requirements

SAML2 providers typically require access to your user information through a plug-in or adapter installed in your directory server. These are provided by SAML2 providers themselves. For instance, Microsoft provides Azure AD Connect which provides an easy way to setup Azure AD as a SAML2 Identity Provider using your existing Active Directory server as the single source or truth for all user authentication. Identity providers charge for their service, but many include a free tier which may be appropriate for many Frame integrations.

Limitations

Using a SAML2 Identity Provider is the most flexible option for authentication. The only limitations are those shared with the other options described in this Solution Guide. Frame does not support fine-grained permissions, for instance allowing some authenticated users to launch an application while others cannot, based solely on groups or information in the user profile.

Entity Endpoint URLs

When each Frame entity is being created, they're given a URL slug. Using these slugs, you can construct landing pages for your users for them to sign into Frame and get straight to their resources.

url_hierarchy.png

Important: If you want to direct your users to your specific identity provider (and bypass the default login page), add this query string to your Frame URLs:

```
?idp=your-IdP-integration-name to your URL.
```

IMPORTANT

With the new iam integration (if your SAML2) integration has difr icon in front of the SAML2:

Screenshot 2026-05-12 at 13.14.16.png

the **?idp** part is different. You don't use the SAML2 name, but the SAML2 ID:

Screenshot 2026-05-12 at 13.25.30.png

So the URL looks like this:

```
?idp=your-IdP-ID to your URL.
```

An example:

> https://use.difr.com/frame-support/testorg/test-2022-aws/launchpad/test-desktop-1/ **?idp=7ebca6fa-ad02XXXXX77-d2f2c754905f**

Endpoint-specific URLs

Launchpad

Launchpad URLs are usually provided to end-users, allowing them to access sessions. You can copy this URL when you navigate to your desired Launchpad.

```
----USE Backend----
https://use.difr.com/customer-slug/organization-slug/account-slug/launchpad/launchpad-slug

----DEU Backend----
https://deu.difr.com/customer-slug/organization-slug/account-slug/launchpad/launchpad-slug
```

Account Admin

Useful if you need to provide direct links to an account's Dashboard. Users that do not have Account Admin access will simply be redirected to a Launchpad they've acccess to. You can copy this URL when you navigate to an account's Dashboard.

```
----USE Backend----
https://use.difr.com/frame/customer-slug/organization-slug/account-slug/

----DEU Backend----
https://deu.difr.com/frame/customer-slug/organization-slug/account-slug/
```

Admin URL's

These URLs are perfect for your Admins. You can simply navigate to your customer or organization and copy the URL.

Customer Admin URL

```
----USE Backend----
https://use.difr.com/frame/customer-slug/
```

Org Admin URL

```
----USE Backend----
https://use.difr.com/customer-slug/organization-slug/

----DEU Backend----
https://deu.difr.com/customer-slug/organization-slug/
```

Revision #12
Created 1 October 2025 04:49:22
Updated 12 May 2026 11:35:34 by Dragan Mladenovic