Identity and Access Management

Roles, RBAC, Dizzion C3, Basic IdP, General SAML2 Integration, Duo, Google Workspace, Microsoft EntraID, ADFS, Okta

Available Roles

Role Permissions

Hierarchy	Role	Permissions
Customer	Customer Administrator	Highest level of access. Customer administrators are able to create and manage multiple organizations and accounts. Customer administrators can also modify permissions for any of the user roles listed below.
Customer	Customer Analytics	Customer Analytics users can only access the Analytics graphs at the customer level.
Customer	Customer Auditor	Customer Auditor users have read only access to functionality at the customer, organizations, and account levels.
Customer	Customer Security Administrator	Customer Security Administrator users can only access Audit Trail and Users functions at the customer level to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and manages users (if Frame IdP is enabled) for all organizations and accounts.

Hierarchy	Role	Permissions
Customer	Customer Support	Customer Support users can only access the Summary, Analytics, Audit Trail, and Status pages for Accounts under the customer level to review activity and research user sessions. They can reboot, terminate VMs, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.
Customer	Limited Customer Administrator	Limited Customer administrators possess the same permissions as Customer administrators for managing organizations and accounts. However, they do not have the ability to create organizations or accounts, manage users, or start sessions.
Organization	Organization Administrator	Organization administrators can manage any organizations assigned to them by the Customer or Limited Customer administrator and those organizations' accounts. Organization administrators can only be created by Customer or Limited Customer administrators.
Organization	Limited Organization Administrator	Limited Organization administrators can manage organizations assigned to them by Customer or Organization administrators and those organizations' accounts. However, they do not have the ability to create accounts, manage users, or start sessions.
Organization	Organization Analytics	Organization Analytics users can only access the Analytics graphs at the specified organization level.
Organization	Organization Auditor	Organization Auditor users have read only access to the organization and accounts under the organization.

Hierarchy	Role	Permissions
Organization	Organization Security Administrator	Organization Security Administrator users can only access Audit Trail and Users functions at the specified organization level to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and add users (if Frame IdP is enabled) for all accounts under the specified organization.
Organization	Organization Support	Organization Support users can only access the Summary, Analytics, Audit Trail, and Status pages for Accounts under the specified organization level to review activity and research user sessions. They can reboot, terminate VMs, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.
Account	Account Administrator	Account administrators can access and manage any accounts assigned to them by the Organization, Limited Organization, Customer, or Limited Customer administrators.
Account	Limited Account Administrator	Limited Account administrators possess the same permissions as Account administrators for managing accounts. However, they do not have the ability to manage users or start sessions.
Account	Account Analytics	Account Analytics users can only access the Analytics page in the account Dashboard.
Account	Account Auditor	Account Auditor users have read only access to the account Dashboard.

Hierarchy	Role	Permissions
Account	Account Security Administrator	Account Security Administrator users can only access the Users and Audit Trail pages in the account Dashboard to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and manage users (if Frame IdP is enabled) for the specified account. They are also able to access Audit Trail and Session Trail for the specified account.
Account	Account Support	Account Support users can only access, at the Account level, the Summary, Analytics, Audit Trail, and Status pages to review activity and research user sessions. They can reboot, terminate VMs, shadow sessions, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.
Account	Sandbox Administrator	Sandbox Administrator can only access the Sandbox page in the account Dashboard to manage the Sandbox (e.g., schedule a publish, power on/off VM, install and update applications, update the OS, backup Sandbox, restore from backup, change instance type, and clone to another Sandbox, if authorized).
Account	Utility Server Administrator	Utility Server Administrator can only access the Utility Server page in the account Dashboard to add, manage, and terminate utility servers.
Account	Launchpad Administrator	This account-level role can only add, delete, and change Launchpad definitions.

Hierarchy	Role	Permissions
End User	Launchpad User	End users or "Launchpad users" can only access Launchpads that are configured by the administrators. A Launchpad user can access multiple Launchpads from multiple accounts if configured this way by administrators.
API	API - Generate Anonymous Customer Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in all Frame accounts under the specified Customer entity.
API	API - Generate Anonymous Organization Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in all Frame accounts under the specified Organization entity.
API	API - Generate Anonymous Account Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in the specified Frame account.

Identity Provider Integrations

This section outlines the user authentication options for Frame customers. The following documentation will discuss how to choose the right authentication option and reviews the benefits, applicability, and requirements for each option.

The term “authentication” refers to how the system verifies the identity of a user. By requiring that only known users are allowed to use the system, a Frame customer can ensure that their applications and infrastructure are only used by the appropriate people and that the individual identities of those users are associated with their usage of the system.

> If you are attempting to set up an Identity Provider (IdP) integration, you must first navigate to the Customer entity level and unlock the Enforce settings slider.

Enforce Settings

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/
```

Basic Authentication

Basic Authentication is a manual approach for providing access; admins need to manually invite users **via email**, and have them **set their own** passwords. You manually reset their passwords, manually delete the users, and give users various roles/permissions for Frame Accounts, Organizations, or Customers. If you are planning on using Frame's Basic Authentication for your user management, continue reading to learn how to manage your users. If you are planning on using a third-party provider, we recommend reading through the information in the Identity Provider Integrations section.

> 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.

Invite Users

Once you have onboarded your apps, published your changes, and set up your Launchpad – you are ready to invite users. You can use the Frame Basic IdP by following the instructions below.

1. From the Dashboard, click on the **Users** page listed on the left. From there, go to the **Basic (username/password)** tab.

   Basic Authentication Users

2. Click the **Invite User** button in the upper right corner of the screen. A new window will appear prompting you to enter the email address of the user you would like to invite.

> The system will automatically check to see if the email address is already associated with the account.

Invite Users Panel

3. Once the email address has been entered, the **Roles** section will appear within the window. Select the role you would like to assign to your user. You can assign different

roles for different accounts for this user by clicking the **Add** button. If you would like to learn more about user roles, check out our documentation.

User Email Example

4. Click **Invite** when ready. The window will close and your user's information will automatically populate under the **Users** list. An invite will be sent to your user where they will fill out their name and set their password.

Reset a Deactivated User Account

Inevitably, some of your users will forget their passwords. User can reset their own password, as described in our end user documentation. However, if they fail to login successfully in 3 consecutive login attempts, Frame Basic IdP will deactivate their user account. Reactivating a Frame Basic IdP user account is simple and can be done with just a few clicks.

1. Depending on your assigned administrator role, go to the **Users** left-hand menu on the Customer or Organization Dashboard in your Admin Console or on the Account Dashboard.
2. Click on the **Basic (username/password)** tab.

   image.png

3. Locate your deactivated user from the Users list. You should see that their status has changed to "B" for **Blocked**.

   Dashboard > Users (Blocked User)

4. Find and click on the ellipsis listed next to their name on the far right side of the screen. Select **Reset Password** as shown below:

   Reset Password

5. Your user will be sent an email with a link to reset their Frame Basic IdP user password.

Voilà! You have successfully reactivated your user's Frame account.

Removing Users

Removing users from your account can be done with just a few clicks.

1. Depending on your assigned administrator role, go to the **Users** left-hand menu on the Customer or Organization page in your Admin Console or on the Account Dashboard.
2. Click on the **Basic (username/password)** tab.
3. Click on the ellipsis next to the user you wish to remove from the account and select **Revoke Invitation**.

   Basic Authentication Tab - Revoke an invitation

4. A confirmation prompt will appear. Click **Revoke** in the bottom right corner of the dialog box.

   Basic Authentication Tab - Revoke confirmation

Logging in

Once users have accepted their Basic Authentication invitation, they can sign in using email address and password on our Frame Basic IdP Login page as pictured below. Most Frame Basic IdP users can login at ; however, you can direct your users to go to a specific Launchpad or Account Dashboard URL.

Require Frame Basic IdP

If you require users to always authenticate using Frame Basic IdP (especially if you have more than one IdP configured for your Customer, Organization, and/or Account(s)), direct your users to a specific Launchpad or Account Dashboard URL appended to the URL.

Authorization

The Frame Platform provides administrators with a role-based access control (RBAC) capability to manage user and administrative access to their accounts. Through the Frame Admin user interface, administrators are able to assign roles which grant varying levels of access to their users. These same granular controls are available for all authentication types.

> Customer and Organization administrators can manage users from the Admin page by clicking on the ellipsis next to the desired entity, selecting “Edit,” and clicking on the “Security” tab. Account administrators manage their users from the “Users” section of their Dashboard.

Roles

Roles allow administrators to easily manage the permissions and access levels of their users. Regardless of the authentication type, administrators must specify the role they wish to grant to their users before those users can be authorized to access Frame resources.

Role Permissions

Hierarchy	Role	Permissions
Customer	Customer Administrator	Highest level of access. Customer administrators are able to create and manage multiple organizations and accounts. Customer administrators can also modify permissions for any of the user roles listed below.
Customer	Customer Analytics	Customer Analytics users can only access the Analytics graphs at the customer level.

Hierarchy	Role	Permissions
Customer	Customer Auditor	Customer Auditor users have read only access to functionality at the customer, organizations, and account levels.
Customer	Customer Security Administrator	Customer Security Administrator users can only access Audit Trail and Users functions at the customer level to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and manages users (if Frame IdP is enabled) for all organizations and accounts.
Customer	Customer Support	Customer Support users can only access the Summary, Analytics, Audit Trail, and Status pages for Accounts under the customer level to review activity and research user sessions. They can reboot, terminate VMs, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.
Customer	Limited Customer Administrator	Limited Customer administrators possess the same permissions as Customer administrators for managing organizations and accounts. However, they do not have the ability to create organizations or accounts, manage users, or start sessions.
Organization	Organization Administrator	Organization administrators can manage any organizations assigned to them by the Customer or Limited Customer administrator and those organizations' accounts. Organization administrators can only be created by Customer or Limited Customer administrators.

Hierarchy	Role	Permissions
Organization	Limited Organization Administrator	Limited Organization administrators can manage organizations assigned to them by Customer or Organization administrators and those organizations' accounts. However, they do not have the ability to create accounts, manage users, or start sessions.
Organization	Organization Analytics	Organization Analytics users can only access the Analytics graphs at the specified organization level.
Organization	Organization Auditor	Organization Auditor users have read only access to the organization and accounts under the organization.
Organization	Organization Security Administrator	Organization Security Administrator users can only access Audit Trail and Users functions at the specified organization level to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and add users (if Frame IdP is enabled) for all accounts under the specified organization.
Organization	Organization Support	Organization Support users can only access the Summary, Analytics, Audit Trail, and Status pages for Accounts under the specified organization level to review activity and research user sessions. They can reboot, terminate VMs, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.

Hierarchy	Role	Permissions
Account	Account Administrator	Account administrators can access and manage any accounts assigned to them by the Organization, Limited Organization, Customer, or Limited Customer administrators.
Account	Limited Account Administrator	Limited Account administrators possess the same permissions as Account administrators for managing accounts. However, they do not have the ability to manage users or start sessions.
Account	Account Analytics	Account Analytics users can only access the Analytics page in the account Dashboard.
Account	Account Auditor	Account Auditor users have read only access to the account Dashboard.
Account	Account Security Administrator	Account Security Administrator users can only access the Users and Audit Trail pages in the account Dashboard to manage all auth providers (Basic (username/password), Google, SAML2, API, SAT), configures SAML2 providers, manage SAML2 permissions, and manage users (if Frame IdP is enabled) for the specified account. They are also able to access Audit Trail and Session Trail for the specified account.
Account	Account Support	Account Support users can only access, at the Account level, the Summary, Analytics, Audit Trail, and Status pages to review activity and research user sessions. They can reboot, terminate VMs, shadow sessions, and close sessions. They can detach personal drives and enterprise profile disks (if the disks do not detach after session closing) and backup, restore, and delete personal drive and profile disk volumes.

Hierarchy	Role	Permissions
Account	Sandbox Administrator	Sandbox Administrator can only access the Sandbox page in the account Dashboard to manage the Sandbox (e.g., schedule a publish, power on/off VM, install and update applications, update the OS, backup Sandbox, restore from backup, change instance type, and clone to another Sandbox, if authorized).
Account	Utility Server Administrator	Utility Server Administrator can only access the Utility Server page in the account Dashboard to add, manage, and terminate utility servers.
Account	Launchpad Administrator	This account-level role can only add, delete, and change Launchpad definitions.
End User	Launchpad User	End users or "Launchpad users" can only access Launchpads that are configured by the administrators. A Launchpad user can access multiple Launchpads from multiple accounts if configured this way by administrators.
API	API - Generate Anonymous Customer Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in all Frame accounts under the specified Customer entity.
API	API - Generate Anonymous Organization Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in all Frame accounts under the specified Organization entity.
API	API - Generate Anonymous Account Token	Authorizes the API requestor to obtain Secure Anonymous Tokens from Frame Admin API for starting Frame sessions in the specified Frame account.

Administrators are able to grant permissions based on their own level of access. For instance, while a Customer admin can assign any role to any user, an Organization admin can only grant the Organization Admin role or below to another user.

You can read more about Frame account hierarchy in the Platform Hierarchy section. Administrators must assign roles when inviting users. They may also modify roles for existing users at any time. If you have not yet invited any users, please refer to the Basic Authentication or third-party Identity Provider Integrations sections of our documentation, depending on which platform you wish to use to add your users.

User Permissions

Google (OAuth2) IdP

If you have decided to use the Google OAuth integration through Frame, it's easy to manage users by domain/email.

From the Frame Console, navigate to your desired entity where you wish to set up your permissions integration (Customer/Organization/Account), and select **Users**.

image.png

Enable the **Google** toggle from the Authentication tab and then click **Save** in the upper right corner of the console.

image.png

Click the new *Google* tab. Click **Add** at the top-right.

image.png

A new window will appear prompting you to enter either an email address or a domain. For this example, we will add a domain and give anyone associated with that domain an *Account Administrator* role on the “Doc-Acct” Account.

When specifying a Google Workspace domain, you must prefix the domain with the symbol, as shown above.

Admins can also add multiple domains and email addresses under the same role set. For example, using the **Add** button, we have added a single email address along with our domain. The user associated with that email address will be given the same role on the “Doc-Acct” Account.

image.png

To add another level of granularity, our domain and single email address can be given additional roles by clicking **Add** below the *Roles* section.

image.png

Now, once we click **Add** at the bottom of the window, the domain and single email address will be given *Launchpad User* access on the "Applications 2” Launchpad, and *Account Administrator* access on the “Persistent Desktops” account. Administrators can add many Google authorization role sets for multiple domains/email addresses.

User Permissions with a SAML2 IdP

Once you have set up your SAML2 provider integration with Frame, you will need to designate permissions for your users. Navigate to the **SAML2 Permissions** tab to the right of the **SAML2 Providers** tab from the **Users** page of the desired entity. Click **Add Permission**.

image.png

- **For provider**: Select the SAML2 Provider you are designating permissions for.
- Allow access:
- **Always**: Once the user is authenticated, they have access to the role you specify below – no conditions required.
- **When all conditions are satisfied**: The user must meet all conditions specified by the Admin to be granted access to the role specified.
- **When any condition is satisfied**: The user can meet any conditions specified by the Admin to be granted access to the role specified.
- **Conditions**: Specify your assertion claims and their values which will correspond with the roles you wish to grant. Reference the table below for our accepted assertion claims.
- **Grant roles**: Select the desired roles you wish to grant to your users. You can add multiple role sets by using the **Add** button. Reference the roles section above for more information.

Assertion Claim	Claim Value	Example
em	Email	johnsmith@mycompany.com

Assertion Claim	Claim Value	Example
givenName	First Name	John
sn	Surname	Smith

When qualifying users by domain, it is best practice to use “em ends with @yourcompany.com.”

During the IdP setup, you may have used to define the email attribute. While this is fine for the IdP, you must use to reference the email attribute when configuring SAML2 permissions on Frame.

Click **Save** when you are done. Administrators can add multiple permission sets under the *SAML2 Permissions* section.

SAML2 Attributes

When creating SAML2 permissions on Frame, admins may use custom attributes from their IdP by setting specific permissions settings. For this example, we will use a very common custom attribute – “groups.” Most IdPs provide ways to “group” users and these groups can be passed to Frame via custom attribute mappings. Using additional attribute maps, you can build conditions for varying roles and access privileges. When creating any rules for SAML2 claims/attributes, use “contains” in the comparison operator field as shown below.

Here is an example of where you would set group statements in Okta:

Here is an example of a list of groups in Okta:

This is how we would pass one of the groups (“Okta-Contractors”) over to Frame, allowing administrators to create rules and roles to meet their needs.

With the configuration above, any users from the “Okta-Contractors” group signing into Frame will be given Account Administrator access to the “Contractor Account.”

All identity providers use different methods to manage user groups, please consult your IdP's documentation for more information about groups and group management.

Troubleshooting

If users see the following Unauthorized page after successfully authenticating to their SAML2 identity provider, then there were no SAML2 Permission rules that were satisfied by the SAML2 attribute names and corresponding values provided by the identity provider.

To address this issue, the Frame Administrator must:

1. Confirm the correct SAML2 attribute names and values are being provided in the SAML2 Authentication Response message after the user has successfully authenticated to the SAML2 identity provider.
2. Review the list of SAML2 attribute names (under the Field column) and corresponding SAML2 attribute values (under the Value column) on the Unauthorized page and determine which SAML2 attribute name and corresponding SAML2 attribute value should be used to define a SAML2 Permission authorization rule.

Authorization rules are defined in the SAML2 Permissions tab on the appropriate Frame Customer, Organization, or Account. Once the Frame Administrator confirms the right SAML2 attributes and values are listed on the Unauthorized page, they can then create a SAML2 Permission rule for the user (or group of users).

As an example, based on the information provided in Unauthorized page image, the Frame Administrator could replace with and with in the SAML2 Permission page below to create a SAML2 Permission rule specific to one individual's email address.

tip for group assertions

In general, use the operator as SAML2 identity providers typically provide SAML2 attribute values as a list/array of values.

Dizzion C3

Dizzion Frame now supports Dizzion C3 as an authentication provider, allowing administrators to use the same credentials they already use for support.dizzion.com and c3.dizzion.com to access Frame. By enabling Dizzion C3 authentication, users can seamlessly log in without managing multiple credentials, improving security and streamlining access. This guide will walk you through the steps to enable Dizzion C3 as an authentication provider.

Prerequisites

Before enabling Dizzion C3 authentication for Frame, ensure the following:

- You have the **Frame Customer Admin role in Dizzion C3** (contact your Dizzion Customer Success Manager if needed)
- You have administrator access to the Frame Admin Console to configure authentication settings.
- Your Frame organization/account is set up and active.\n- Users have valid **Dizzion C3 credentials** to authenticate.\n\n

> By default, any user with the **Frame Customer Admin role** assigned within Dizzion C3 will automatically be assigned the **Customer Administrator role** within Frame.

Configuration

1. Log in to Frame and navigate to **Users > Authentication** from either the Organization or Account level of the Frame Console. (More details around authentication based on tenant hierarchy can be found here.
2. Enable **Dizzon C3** on this page (under the **Authentication** tab). Click **Save** in the upper right corner of the page.

   Enable Dizzion C3

3. Once enabled, **Dizzion C3** will appear as a sign-in option on the Frame login page.

4. Users can now simply click on the **Sign in with Dizzion C3** to be redirected to the Dizzion C3 authentication portal. If authentication is successful, you will be redirected back to Frame with access granted.

Users with the appropriate role can now log in using their Dizzion C3 credentials.

Accessing Frame from the Dizzion C3 Portal

Administrators with the **Frame Customer Admin role** can also log in to Frame directly from the Dizzion C3 portal by following the steps below:

1. Navigate to the Dizzion C3 Portal.
2. 2. Enter your email address and click **Next**.
3. 3. Enter your password and click **Sign In**.

4. Click on "Click here to launch Frame" to be redirected.

Launch Frame

5. A new browser tab will open, and you will be automatically redirected to Frame.

Additional Resources

Enabling this feature allows user access to be managed through Dizzion's C3 Platform. If you wish to modify user access to the platform, you must do so via C3. More detailed information around C3 user management can be found in our C3 Administration documentation.

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**.
   image.png

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.
   image.png
   - **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	