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.

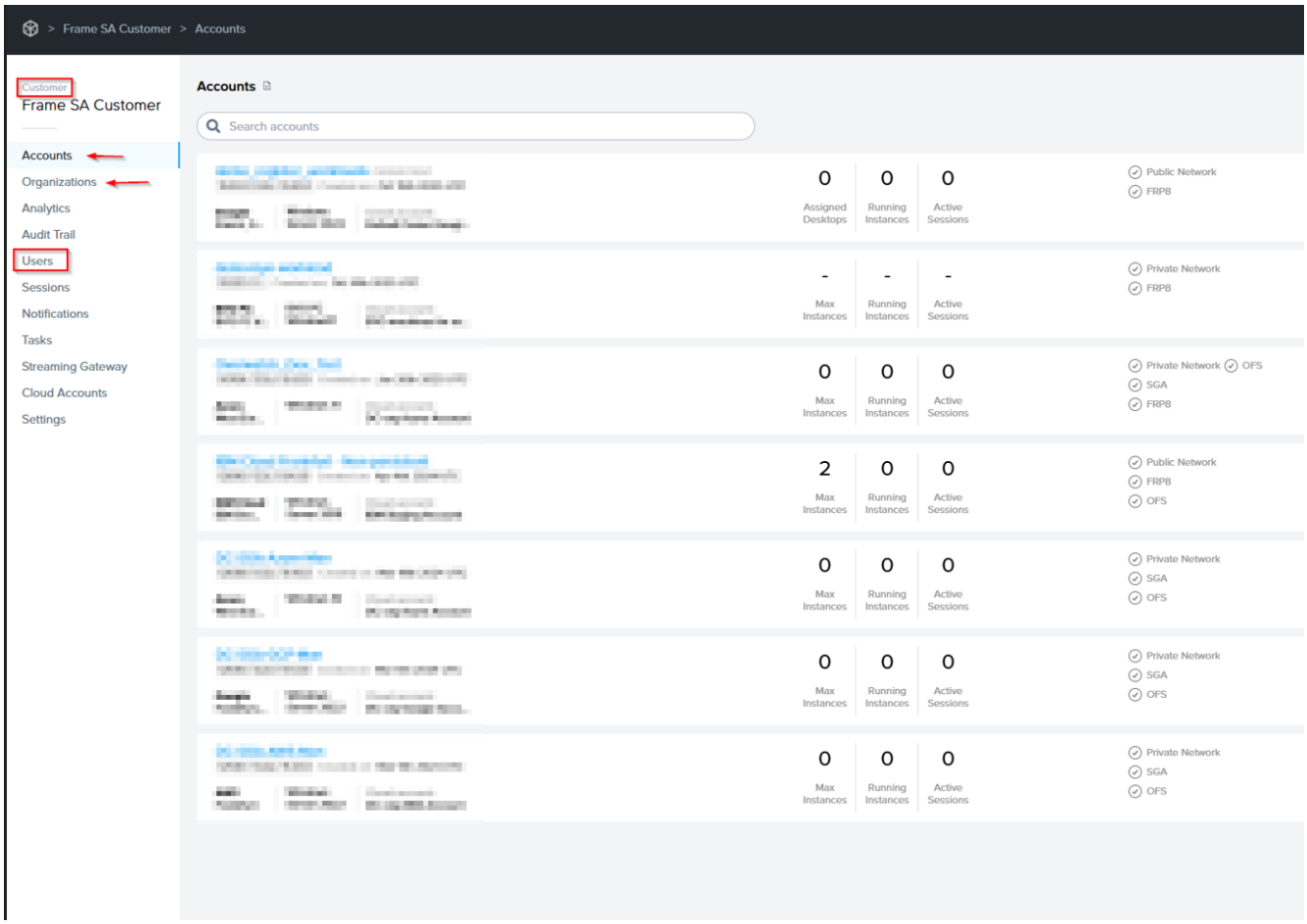
You can read more about Frame account hierarchy in the Platform Hierarchy section. Administrators must assign roles when inviting users. They may also modify roles for existing users at any time. If you have not yet invited any users, please refer to the Basic Authentication or third-party Identity Provider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

User Permissions

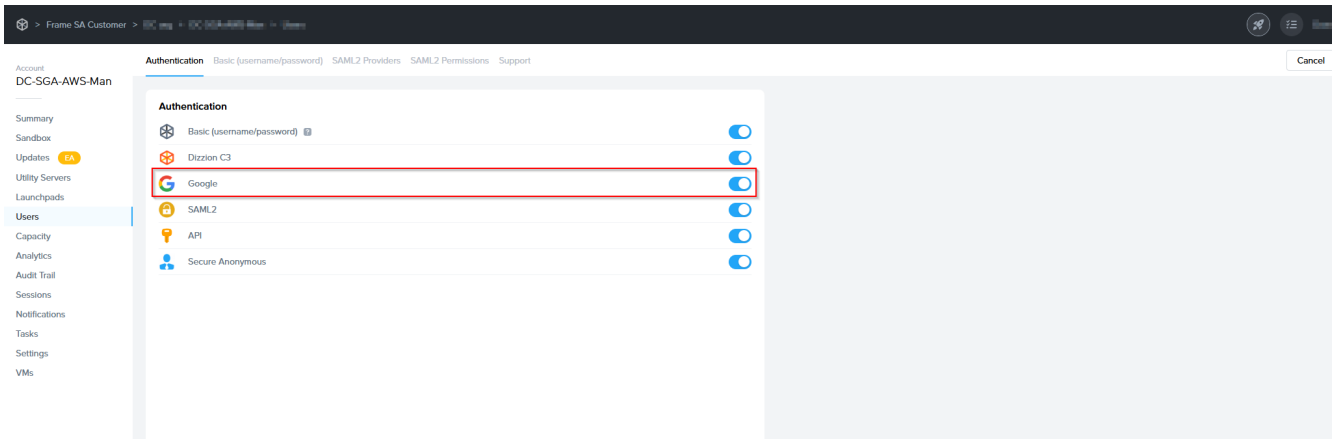
Google (OAuth2) IdP

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

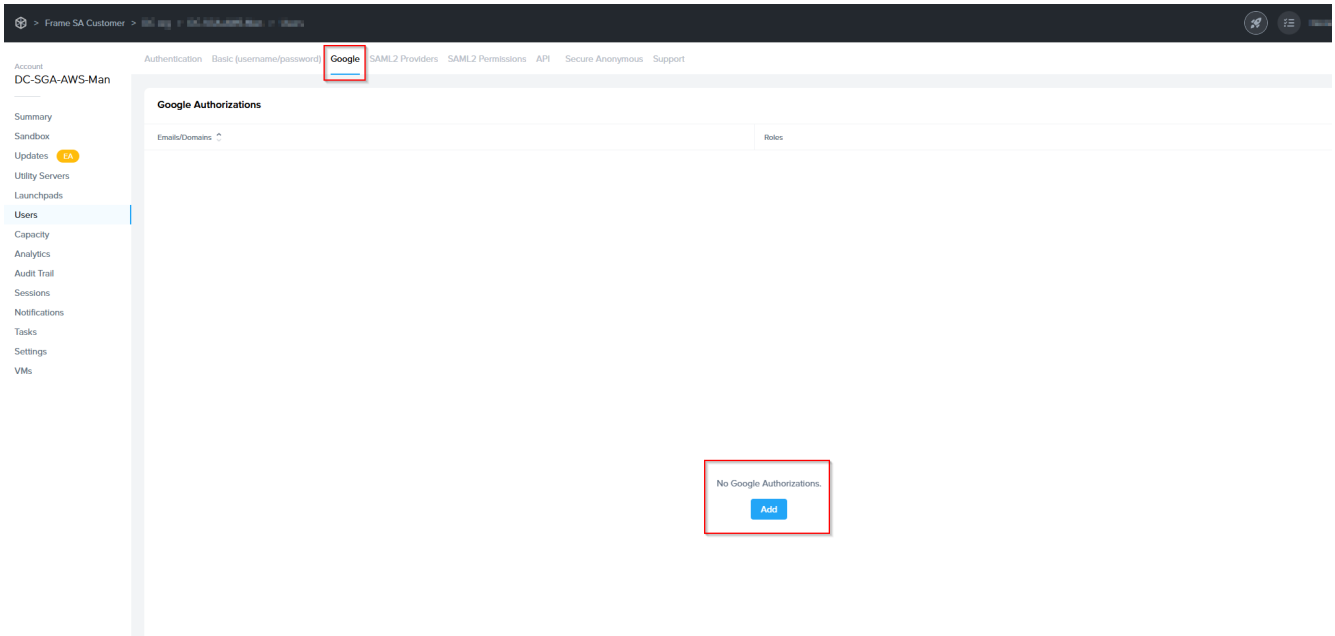
From the Frame Console, navigate to your desired entity where you wish to set up your permissions integration (Customer/Organization/Account), and select **Users**.



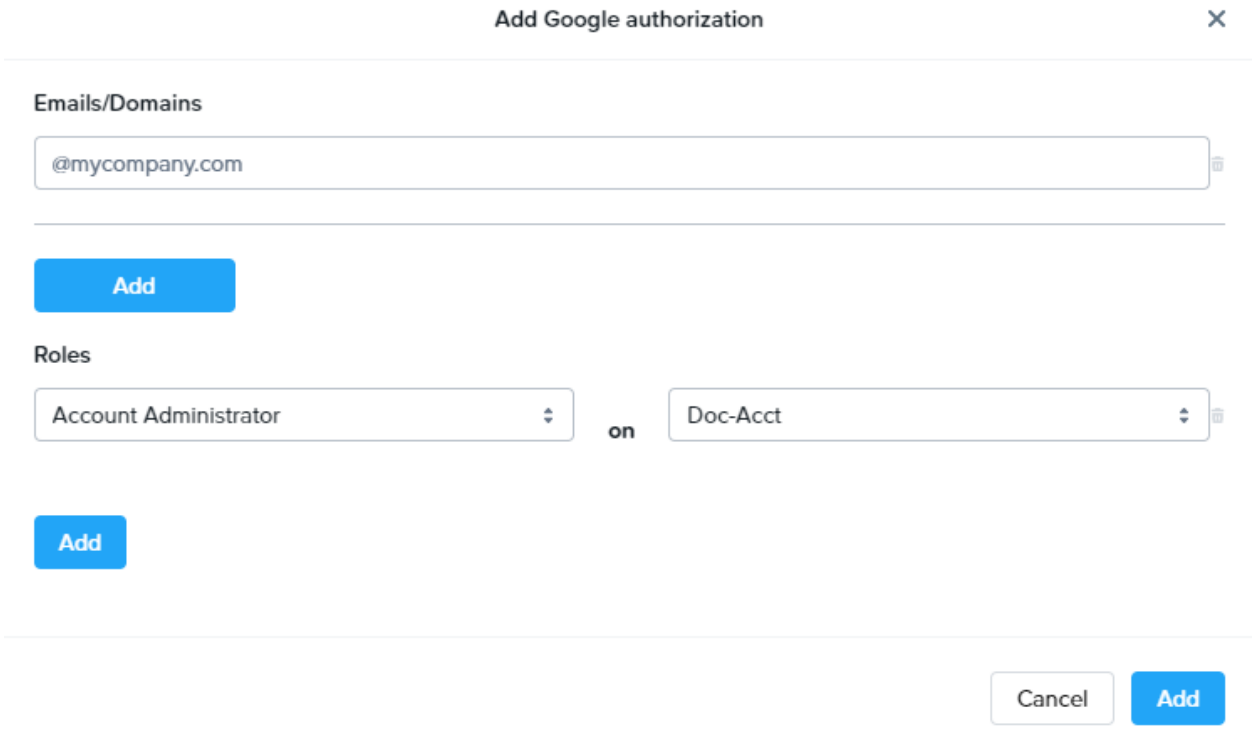
Enable the **Google** toggle from the Authentication tab and then click **Save** in the upper right corner of the console.



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

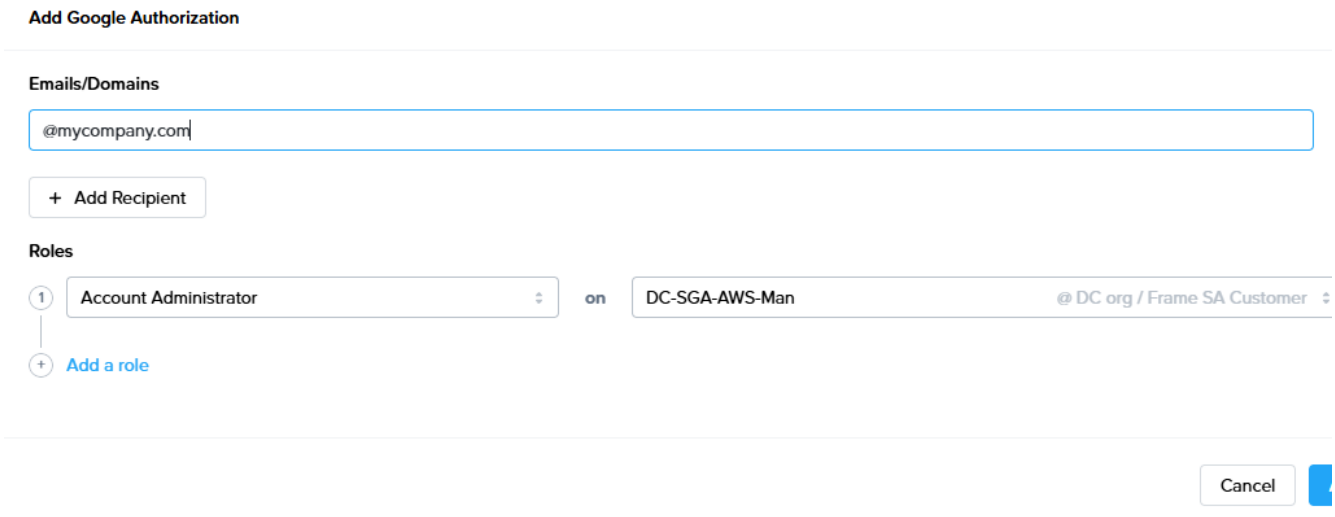


A new window will appear prompting you to enter either an email address or a domain. For this example, we will add a domain and give anyone associated with that domain an *Account Administrator* role on the “Doc-Acct” Account.



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.



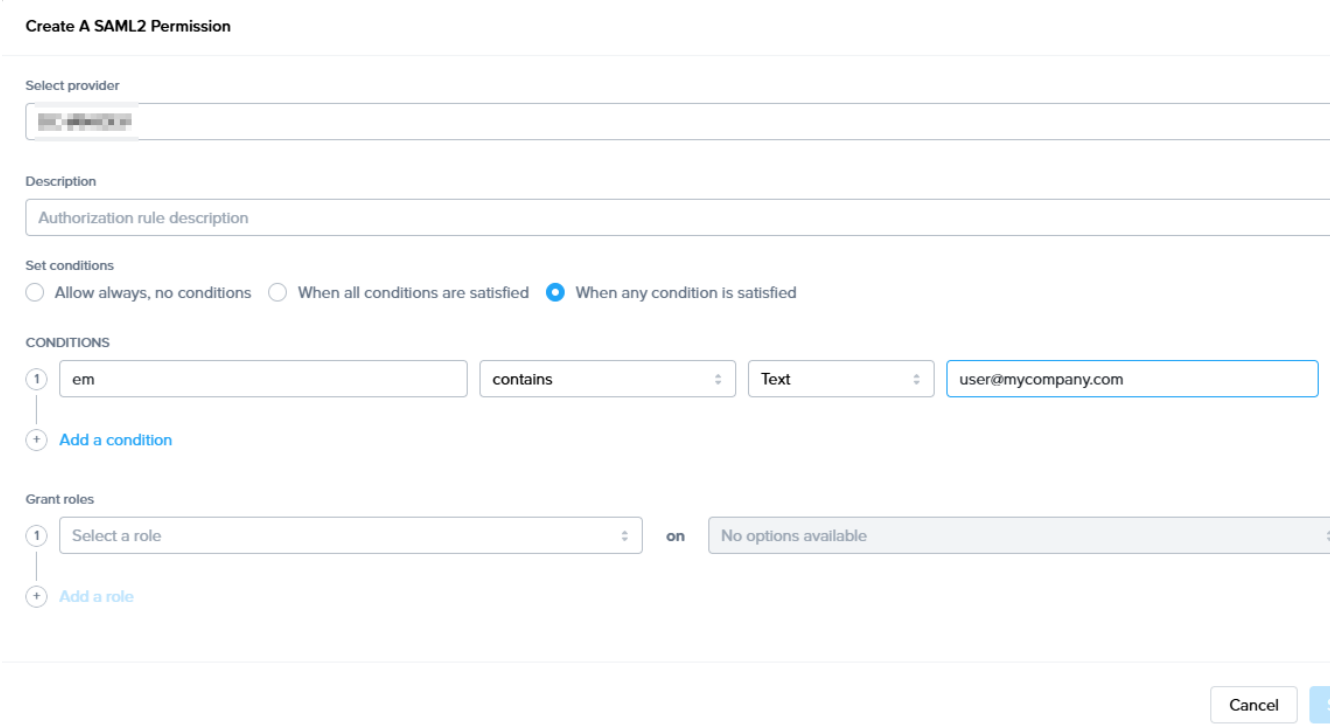
To add another level of granularity, our domain and single email address can be given additional roles by clicking **Add** below the *Roles* section.



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**.



- **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
givenName	First Name	John
sn	Surname	Smith

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

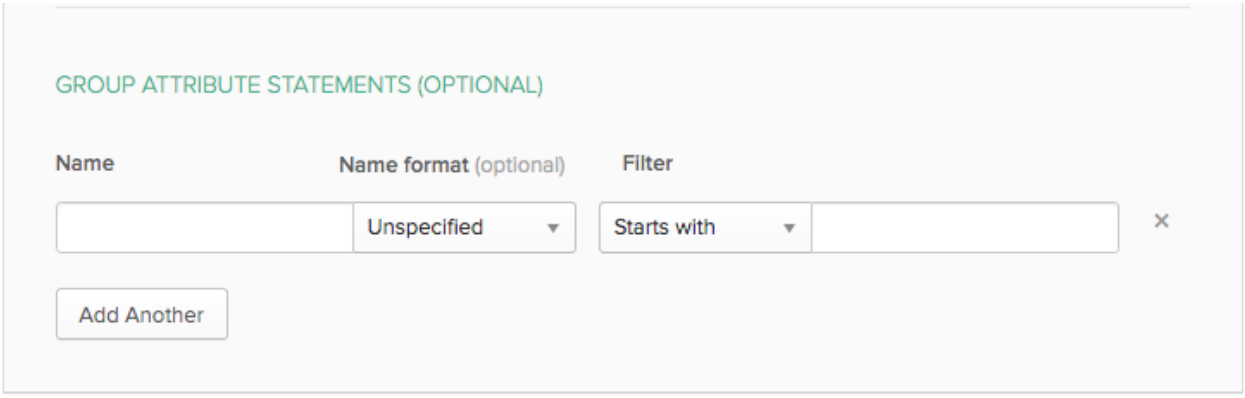
During the IdP setup, you may have used to define the email attribute. While this is fine for the IdP, you must use to reference the email attribute when configuring SAML2 permissions on Frame.

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

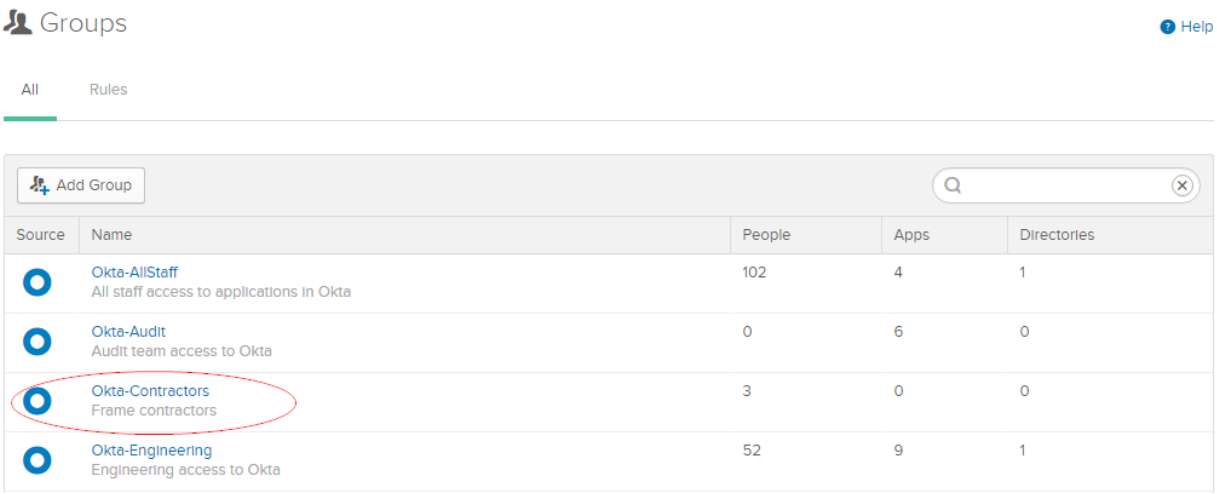
SAML2 Attributes

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.

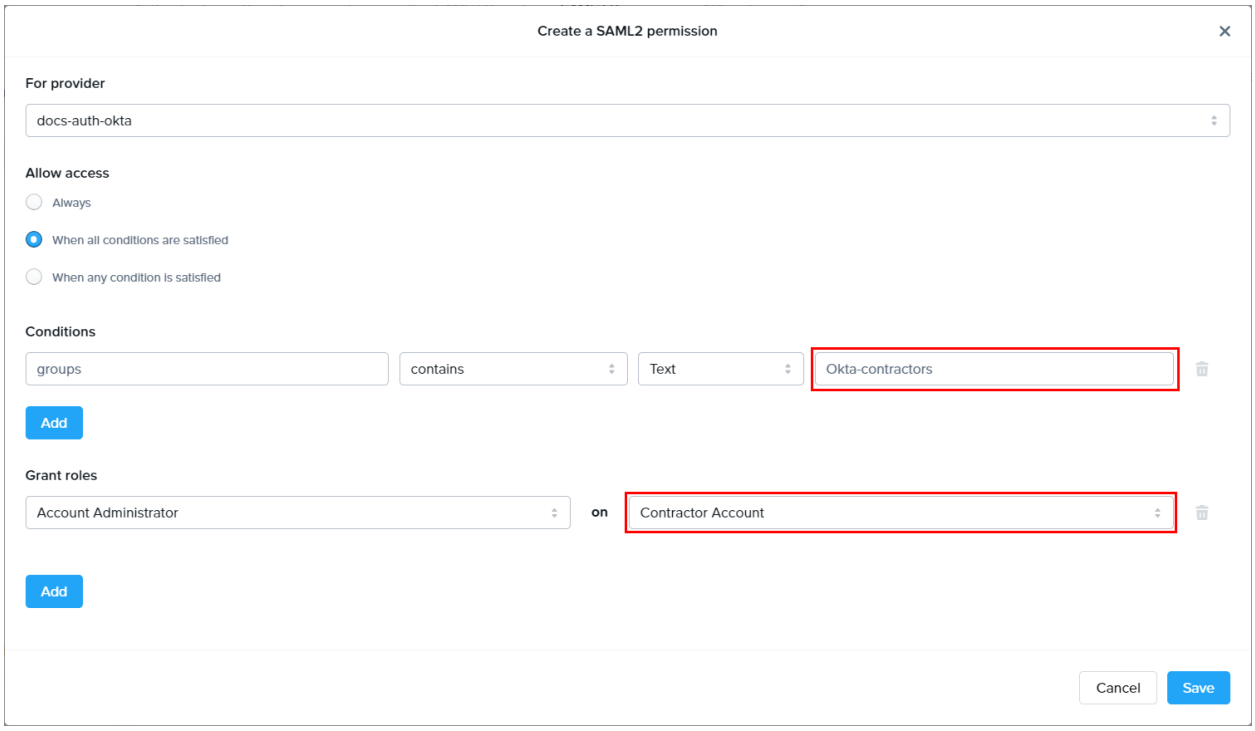
Here is an example of where you would set group statements in Okta:



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.

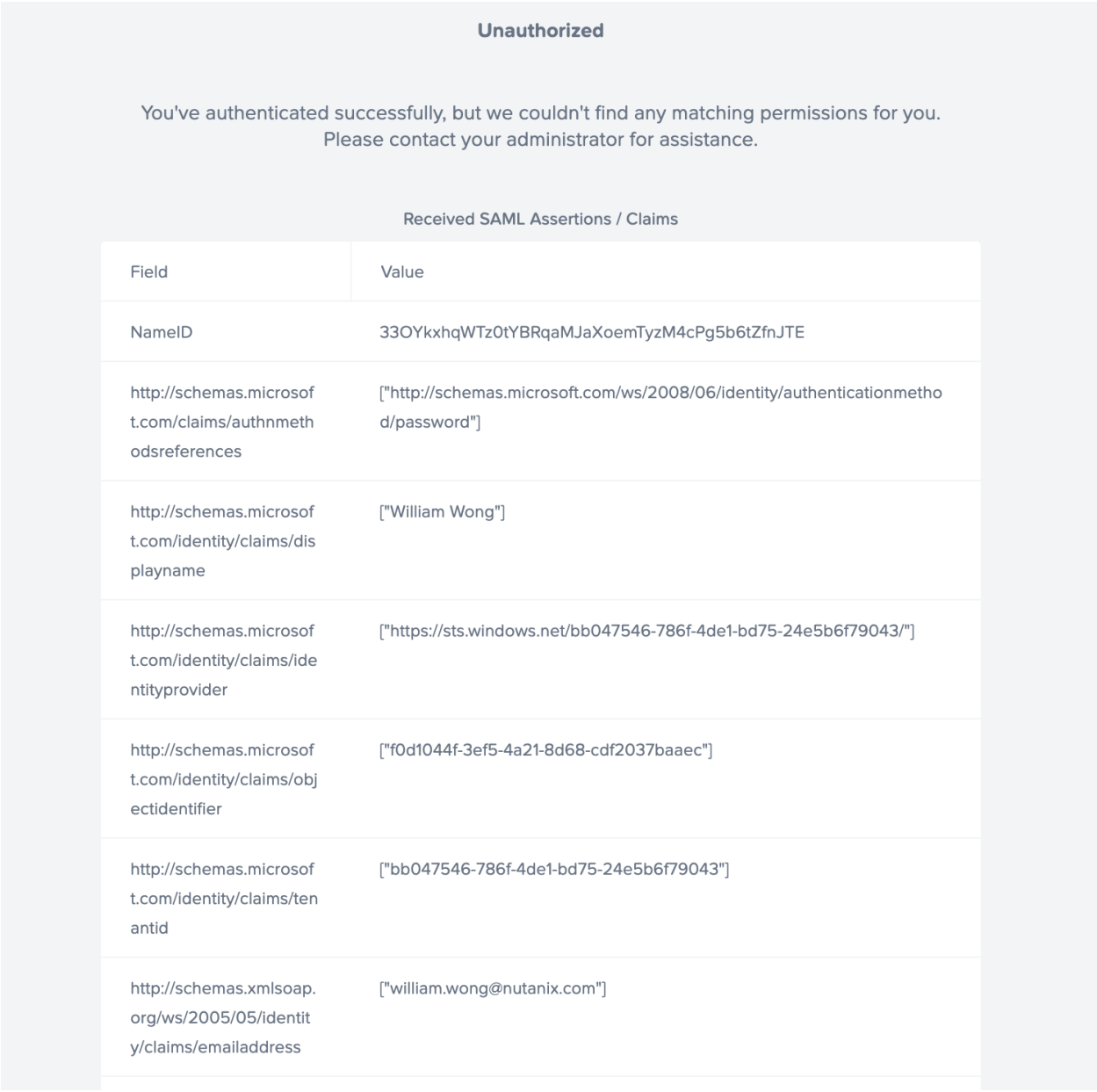


With the configuration above, any users from the “Okta-Contractors” group signing into Frame will be given Account Administrator access to the “Contractor Account.”

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.



Unauthorized

You've authenticated successfully, but we couldn't find any matching permissions for you.
Please contact your administrator for assistance.

Received SAML Assertions / Claims

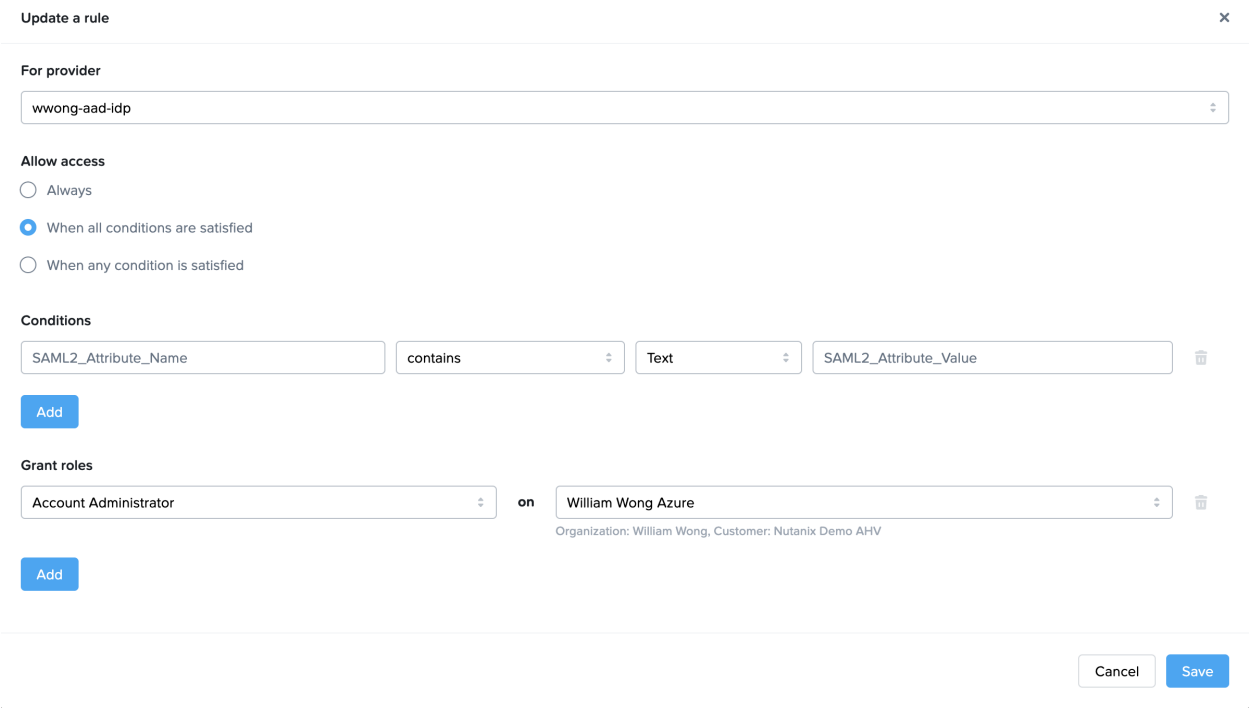
Field	Value
NameID	33OYkxhqWTz0tYBRqaMJaXoemTyzM4cPg5b6tZfnJTE
http://schemas.microsoft.com/claims/authnmethodsreferences	["http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/password"]
http://schemas.microsoft.com/identity/claims/displayname	["William Wong"]
http://schemas.microsoft.com/identity/claims/identityprovider	["https://sts.windows.net/bb047546-786f-4de1-bd75-24e5b6f79043/"]
http://schemas.microsoft.com/identity/claims/objectidentifier	["f0d1044f-3ef5-4a21-8d68-cdf2037baaec"]
http://schemas.microsoft.com/identity/claims/tenantid	["bb047546-786f-4de1-bd75-24e5b6f79043"]
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	["william.wong@nutanix.com"]

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.

Revision #16
Created 1 October 2025 04:49:22
Updated 13 May 2026 08:24:41 by Dragan Mladenovic