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.

Revision #3
Created 16 October 2025 18:52:30 by Chris Tusa
Updated 16 October 2025 18:54:14 by Chris Tusa