Platform Fundamentals

Hierarchy, Account Types, and Deployment Planning

- Hierarchy
- Account Types
- Deployment Planning

Hierarchy

The Frame platform uses a hierarchical approach to organizing administration and access to accounts. In this section, we'll define each tier and the intended configuration strategy at each level.

Customers

The Customer tier is the highest tier within the Frame platform. This is the tenant with an attached subscription for a single business entity. Customers can attach their identity provider(s) and infrastructure at the Customer level.

> As a general rule, we advise you register your identity provider and infrastructure at the Customer level so all Organizations and Accounts can use those resources, unless you have a need to restrict use of identity providers and infrastructures to specific Organizations and Accounts.

Organizations

The Organization tier is the middle tier within the Frame platform, residing between Customers and Accounts. There can be many organizations listed under one Customer depending on the use case. A business may use organizations to set up unique environments for different departments within their company.

Customers can attach their identity provider(s) and infrastructure at the Organization level. If they do, then the identity provider and infrastructure integrations can only be used at that Organization and Accounts under the Organization.

Accounts

This is where an admin will install and configure their applications and configure their production VMs. This is also where admins will create Launchpads for their end users. When an end user logs into Frame, they are accessing one of the accounts listed under an Organization and any of

the workload VMs configured for it.

Roles

The table below describes every available type of user and administrator role, including where they fall in the Frame entity hierarchy and their permissions.

Launchpad Users

- Users with the **Customer Administrator** role can access all Launchpads for all Accounts on their Frame Platform.
- Users with **Organization Administrator** role can access all Launchpads within the Accounts owned by the Organizations that they have administrator rights to.
- Users with **Account Administrator** role can access all of the Launchpads within the Accounts that they have administrator rights to.
- Users with only **Launchpad User** permissions access Launchpads that are configured by the administrators. A user can access multiple Launchpads from multiple accounts if configured this way by the administrators. When logging into an account, the user will see their assigned Launchpads configured by their administrator and access their applications from there. Users can be given access to one or more accounts within multiple organizations as set by the admins of those respective levels.

Account Types

Frame can provide a very customized experience to the end user depending on the unique needs of your organization. This section of the documentation reviews all available Frame account types and their benefits.

Non-persistent (Default) vs. Persistent Desktop Accounts

Non-persistent Accounts Overview

A non-persistent Frame account is used when a Frame administrator wants their user sessions to be “stateless.” When sessions are stateless, any changes made to an instance are completely erased once the session is closed. The instance is then returned to a pool where it waits to be served to the next user, starting from a clean slate.

Non-persistent accounts can be created and configured with the following:

- AHV, AWS, Azure, and Google Cloud Platform
- Domain Joined Instances

Applicability

Non-persistent Frame accounts were designed for organizations who wish to:

- Deliver virtualized applications (rather than desktops),
- Provide a consistent end-user experience between user sessions,
- Simplify image management by updating a single image when desired and easily making it available to a group of users, and
- Provide groups of users access to different combinations of compute, memory, and GPU resources (e.g., instance types) based on user profiles.

Requirements

- Users must be able to authenticate to the platform using either:
  - an identity provider integration
  - Frame Basic Authentication, **or**

    - Frame Secure Anonymous Tokens Feature

Setup

Non-persistent Frame accounts are a selectable option during the "Create Accounts" process.

Persistent Desktop Accounts Overview

In a typical Frame account, sessions are “stateless.” This means that all changes made to an instance are wiped from the instance after the session is closed. The instance is then returned to a pool where it waits to be served to the next user. The Frame platform also offers an alternative option called “Persistent Desktops.”

Persistent Desktops are stateful, desktop-only instances which are individually assigned to users. Users are given administrative control over their own desktop – they can install and manage their own unique application sets and settings in their own persistent environment. Account administrators can still monitor usage and basic session activity through the account Dashboard.

Persistent Desktop accounts can be created and configured with the following:

- AHV, AWS, Azure, and Google Cloud Platform
- Domain Joined Instances

Applicability

Persistent Desktops were designed for organizations who prefer to give their users more control over their own environments. Frame Account administrators still configure the Sandbox image to be used as a base for all instances in the pool, but end users manage their own instance once assigned. If required, Persistent Desktops can be domain joined, in order for enterprises to manage these persistent desktops through a Windows domain.

Requirements

- Users must be able to authenticate to the platform using either:
    - an identity provider integration
    - Frame Basic Authentication, **or**
    - Frame Secure Anonymous Tokens Feature
- If the persistent desktop Frame account is configured to join the persistent desktop VMs to a Windows domain, the users can be required to authenticate to their Windows domain before accessing their assigned Windows desktop.

Setup

The Persistent Desktops feature is enabled upon account creation. It cannot be enabled on accounts that have already been created, since provisioning and infrastructure management of a Persistent Desktop account is handled differently than on a non-persistent Frame account.

Administration

See the Persistent Desktops Administration guide for more details.

Deployment Planning

Customers who wish to deliver virtualized applications and/or desktops to their end users should carefully consider the topics discussed below when planning the implementation of a Frame solution. The design and implementation of their unique Frame Platform solution will vary depending on the customer's use case requirements. The required roles and skill sets for the design, implementation, and operation of their solution are dictated by the customer's business, technical, and operational requirements. Additionally, customers will need to decide on how they will provide end user training, ensure end user adoption (based on what their end users are familiar with), and transition end users from their current environment to the Frame Platform.

This document outlines the key topics that should be considered during the **planning phase** before designing, implementing, and rolling out a Frame solution. The Deployment Planning document is intended to provide a *basis for planning your Frame implementation*. It does not provide every design consideration and tradeoff. Should you have questions, please contact your Dizzion account manager or customer success manager for additional assistance.

NOTE

Frame Discovery Workbook

Download and complete our Frame Discovery Workbook to summarize the high-level requirements for your use case(s). This workbook helps customers summarize their answers to the questions below and prepare for design and deployment activities.

https://files.difr.com/#resources

End User Experience

As a best practice, customers planning their Frame implementation should start by clearly establishing their **desired end user experience**. End user experience is defined by:

- How users will reach their virtualized applications and/or desktops through Frame
- What the users will be able to do while in the Frame session

Clearly defining your end user experience goals before getting started helps to ensure successful implementation and adoption of Frame.

Accessing Frame

Part of defining the end user experience is determining how your users will access their virtual applications or desktop in Frame. The following table identifies the key questions you will want to answer.

Topic	Question	References
Authentication	Will your users need to authenticate to an Identity Provider (IdP) before reaching Frame?	Authentication
Authorization	How will you manage entitlements (e.g., role-based access control)?	Authorization
Integration	Will the users be accessing Frame from a web page you manage or will you simply give them a URL?	
Integration	Will the users access a Launchpad URL, a PWA, a Launch Link, or a custom JavaScript-based web integration?	Launchpad, PWA, Launch Link, Frame Session API

Frame Session Experience

Next, use the questions below to determine what you would like your users to be able to do during and after their Frame session.

Topic	Question	References
Authentication	Will you require your users to authenticate to a Windows domain controller once they reach a Windows OS VM?	Domain
Application Access	Are you providing your users with desktop environments or limiting their access to only specific applications?	Install and Onboard Apps, Launchpad
Persistence	Will users need non-persistent VMs or persistent desktop environments?	Account Types

Topic	Question	References
Profiles	Would you like your users to be able to persist their application profiles across sessions while using non-persistent VMs?	Profiles
Data Storage	Will users need to be able to access/save their files with cloud storage providers or need a personal drive within the Frame account?	Personal Drives, Cloud Integrations
Applications	What specific applications will your users need access to within their Frame session? Do any of these applications require a GPU?	
Features	Will users be able to copy/paste between their device and the Frame session? What features will you allow them to have?	Clipboard Integration, Session Features
Session Lifecycle	How long can the users stay in their Frame session?	Time Limits
Session Lifecycle	Once the user's Frame session ends, what is the user allowed to do? Start a new session? Forced to re-authenticate to your identity provider? Redirected to a web page?	

End User Devices

A consistent user experience requires an understanding of what user devices are to be used to access a Frame session and the peripherals your users need.

Topic	Question	References
Configuration	What devices are your users expected to use with Frame and what are the minimum requirements?	System Requirements
Configuration	Will your users be expecting to use more than one monitor?	Multiple Monitors

Topic	Question	References
Peripherals	What peripherals (besides keyboard and mouse) will your users need?	USB Human Interface Device
Management	Do you manage your user's devices or are they allowed to bring their own devices?	

Infrastructure

You will need to determine what infrastructure(s) you will be using to host your workload VMs and where these workload VMs are geographically, in relation to your end users.

Topic	Question	References
Infrastructure	What infrastructure(s) have you selected to host your workload VMs and where are they geographically located?	Infrastructure

Networking

To ensure the best user experience, users must have the best network possible between their device and the workload VM selected for their application usage needs. Additionally, customer administrators must decide, from a networking standpoint, how their users will reach the workload VMs and what resources are available to the users from their workload VMs.

Topic	Question	References
Network Architecture	How do you want the users reach your workload VMs?	Networking
Network Architecture	Once the users are in their Frame sessions, what can the workload VMs access on the network? What are users not allowed to reach from the workload VMs?	Networking

Topic	Question	References
Network Quality	What is the maximum latency, minimum bandwidth, and maximum packet loss between the end user devices and the workload VMs?	Network Requirements
Network Management	Are you able to apply QoS or prioritize Frame session traffic higher than other forms of traffic on your network?	
Data Center Network Quality	If you are using Nutanix AHV clusters on-premises and your users are accessing the workload VMs from the Internet, what is the network bandwidth between the Internet and your data center? Do you have sufficient bandwidth for the expected number of concurrent Frame sessions?	

Operating System

Your choice of infrastructure and required applications will determine what operating system(s) you will use.

Topic	Question	References
BYO or Frame-provided	If you are using public cloud infrastructure, will you bring your own operating system images or start with Frame-provided images?	Operating System
Windows Domain	If you require your users to use Windows domain-joined workload VMs, what computer/user GPOs do you require?	Domain

Security

Infrastructure, network, operating system, and Frame configuration must be evaluated based on your use case requirements. The following key questions are important for ensuring a secure

design, implementation, and operation of a Frame solution.

Topic	Question	References
Anti-malware	What anti-virus/anti-malware solutions do you require in the workload VMs?	Security Basics
Anti-malware	What anti-virus/anti-malware solutions do you require on end user devices?	
Firewall	Do you restrict outbound access from your private network to the Internet?	Network Requirements
Firewall	Do you restrict inbound and outbound UDP traffic in your network or between end users and the workload VMs?	Network Requirements
Firewall	Do you implement any SSL "break and inspect" solutions for inbound or outbound connections to your private network?	SSL Break and Inspect
Proxy Server	Do you require traffic from the network to the Internet where the workload VMs reside to go through an outbound proxy server? For what protocols?	Proxy Server

Recommended Resources

The following table outlines the key roles and associated responsibilities needed for a successful design and implementation of a typical Frame solution. Additional roles are needed to leverage Frame Admin API endpoints for automation and create custom Frame integrations with existing websites.

Role	Responsibilities
Business Sponsor	Defines business requirements, including business success criteria, and provides budget for the project.
End User / Use Case Owner	Expert on the desired end user experience(s) / use case(s). Defines the end user success criteria, requirements, and end user test plan. Serves as the “voice of the end user experience”.

Role	Responsibilities
Project Manager	Organizes and coordinates customer resources, tasks, reports on progress, and identifies / mitigate execution risks.
Solution Architect or Cloud Architect	Defines the technical requirements based on the business requirements, including technical success criteria, and responsible for overall solution design.
Network Engineer	Manages the customer’s network. Assigns CIDR block for the network containing Frame-managed workloads, manages routing between private network and Internet and from workloads to company’s network-accessible resources.
Information Security	Manages company firewalls and endpoint protection solutions (anti-virus/anti-malware) that will be used within the Frame-managed workloads.
Identity Provider Administrator	Manages and configures the customer’s SAML2 identity provider. Registers Frame Platform as a SAML2 Service Provider for federated authentication and configures their identity provider to generate SAML2 assertions to enforce role-based access control within Frame.
Windows Domain Administrator	Manages the customer’s Windows domain infrastructure and creates the domain service account for use in the Frame-managed workloads.
Application Administrator	Installs and configures customer’s applications for use by end users. Typically, this person is the first Frame “Customer Administrator”. For some organizations, this role maintains the template image(s) with the OS and applications. Understands application requirements, configuration, and dependencies (e.g., required file servers, data storage services, licensing servers, etc.).
Endpoint Administrator	Deploys and manages the end user endpoints (e.g., desktops, laptops, thin clients, mobile devices) to be used to access Frame-managed workloads.
End User Application/Desktop Tester	Verifies, from an end user's perspective, that the solution meets the needs of the end users.