IT Pro related questions – IdP, SSO

- What identity providers can be used with Dizzion DaaS and Cloud PC?
- Can Active Directory be used to log in to Virtual Desktop or Application?
- Can EntraID be used to log in to Virtual Desktop or Application?
- Can I enforce MFA and conditional access policies for logins?
- Does Dizzion DaaS and Cloud PC support passkeys (KeyPass)?

What identity providers can be used with Dizzion DaaS and Cloud PC?

Dizzion supports SAML2 and OAuth-based identity providers for accessing customer, organization, and admin interfaces. For end-user access—including LaunchPad, Launch Link, the Progressive Web App (PWA), and the Session API—authentication can be done using SAML2, OAuth, or SAT (Secure Anonymous Tokens).

Can Active Directory be used to log in to Virtual Desktop or Application?

Yes, each Frame account can be integrated with Microsoft Active Directory, allowing end users to log in to their virtual desktop or application using their AD credentials. However, access to the LaunchPad, Launch Link, or PWA still uses SAML, OAuth, or SAT. For a seamless experience, Frame SSO (Single Login) can be enabled to streamline authentication across both layers.

Can EntraID be used to log in to Virtual Desktop or Application?

Yes, each Frame account can be integrated with Microsoft EntraID, allowing end users to log in to their virtual desktop or application using their EntraID credentials. However, access to the LaunchPad, Launch Link, or PWA still uses SAML, OAuth, or SAT. For a seamless experience, Frame SSO (Single Login) can be enabled to streamline authentication across both layers.

Can I enforce MFA and conditional access policies for logins?

Yes, the configured SAML2 or OAuth IdP enforces MFA and Conditional Access rules.

Does Dizzion DaaS and Cloud PC support passkeys (KeyPass)?

Yes – Dizzion DaaS and Cloud PC fully support passkeys, assuming your Identity Provider and Windows environment support them.
If your IdP allows passkey authentication, customers may use it to access both the Dizzion Console and Windows virtual desktops within Dizzion sessions.

Dizzion does not block the use of passkeys (sometimes referred to as KeyPass).
If your Identity Provider (IdP) supports passkeys (FIDO2 / WebAuthn), then Dizzion supports them as well.
Customers can use passkeys to sign in to the Dizzion Console and into Windows VMs / Cloud PCs as well as withing the sessions, provided that the required IdP and OS configurations are in place.

What is supported ?

- If your IdP (Microsoft Entra ID, Okta, Duo, etc.) allows FIDO2 passkeys, users can authenticate to the Dizzion Console using a passkey.
- If your Windows VM or Cloud PC is Entra ID–joined (or in a hybrid identity setup that supports FIDO2), users can also use passkeys to log into the VM session.
- Dizzion does not restrict or block any passkey method; all authentication policies come from your IdP.

Requirements

To use passkeys with Dizzion:

1. Your IdP must support WebAuthn/FIDO2/passkeys.
2. Passkeys must be enabled as an authentication method in the IdP.

3. The user’s device and browser must support passkeys (Edge, Chrome, Safari, Windows Hello, FIDO2 hardware keys, Android/iOS passkeys).

4. The VM or Cloud PC must be joined to the identity system in a supported configuration (typically Microsoft Entra ID join) and initial login (first login to VM) needs to be done with the password due Microsoft requirements, meaning that passkey can only be used with Cloud PC and Persistent VMs in Dizzion DaaS Frame scenario (non-persistent VMs are not supported).

Example: Using Passkeys with Microsoft Entra ID

If customers want to enable passkeys via Microsoft Entra ID, here are the official setup guides:

Microsoft Documentation:

- Overview of passkeys (FIDO2) in Entra ID
  https://learn.microsoft.com/en-us/entra/identity/authentication/concept-authentication-passkeys-fido2

- Enable passkeys (FIDO2 security keys) in Entra ID
  https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-passkey-fido2

- Registering a passkey for a user
  https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-register-passkey

- Sign in to Windows with a passkey (FIDO2)
  https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-sign-in-passkey

- Passkeys using Microsoft Authenticator (optional)
  https://learn.microsoft.com/en-us/entra/identity/authentication/how-to-enable-authenticator-passkey