Frame Single Sign-On

Introduction

Frame Single Sign-On (SSO) allows users to access a domain-joined VM without requiring users to enter their domain user credentials every time they enter into a Frame session. This patented feature (US Patent #11,483,305) provides a more streamlined end-user experience in terms of Windows domain user authentication.

The first time a user starts a session to a domain-joined workload VM, Frame Terminal (running within the user's browser or Frame App) prompts the user to enter their Active Directory domain user credentials. Frame Terminal encrypts the user credentials using a user-specific public key certificate generated by Frame Platform. The encrypted domain user credentials are stored locally within the user's browser or Frame App cache, linked to the user's identity within Frame (as provided by the identity provider) and specific Frame Account, and sent to the workload VM via Datagram Transport Layer Security (DTLS).

Requirements

- A Frame account configured under Settings > Domain Settings so that test and production workload VMs are joined to Active Directory.
- The Sandbox has been published at least once with at least one domain-joined test/production workload VM for users.
- Frame Guest Agent 1.9.4.0 and higher
- Frame Server 8.6.8.0 and higher
- Frame Remoting Protocol 8

Limitations

- If a user wishes to log in using a different domain user account to workloads in the same Frame account, they must clear their encrypted user credentials from the browser cache or completely clear the Frame App cache.

- Frame SSO is dependent on the cache file persisting across device power cycles. Currently, Frame SSO will not work with thin clients that do not have a persistent store to save the user’s encrypted domain user credentials.

Enable Frame SSO

You enable Frame SSO, as an Admin, by going to **Settings > Domain Settings** in the Frame Account Dashboard and toggling on Frame SSO.

image.png

Disable Frame SSO

To disable Frame SSO, turn off the Frame SSO feature in Domain Settings. Users will be required to authenticate to the Windows domain each time they start a Frame session, regardless of whether they used the Frame SSO feature in the past.

> Disabling Frame SSO does not clear the users' encrypted domain user credentials in their browser or Frame App cache.
> Users will need to individually clear their browser/Frame App cache (see below).

User Experience

This section discusses what your users will experience when Frame SSO is enabled on a domain-joined Frame account.

First login

When Frame SSO is enabled and the user's browser (or Frame App) does not have the user's encrypted domain credentials in its cache, the user will be asked to enter their domain credentials.

image.png

>

> The user must specify their username as UPN: username@domain.com or domain\username

Subsequent logins

Once the user's domain credentials are encrypted and stored in their browser or Frame App cache on the device, the user will see the following screen in subsequent logins when they start their sessions.

image.png

Encrypted User Credential Storage

Once a user successfully logs into a domain-joined Frame session, the encrypted domain user credentials are saved in the browser or Frame App cache. If more than one domain user is using the browser, there will be more than one encrypted domain user credential record.

Clearing User Credentials

Web browser

To clear the encrypted domain user credentials, the browser user must perform one of two operations:

1. The user can go to **Clear Browsing Data** in their Chrome browser and only clear **Cookies and Other Site Data**.
2. Alternatively, the user can go to the **Developer Console** and follow the path below to delete the user credential entry:
   `dev.console > Application > Storage > IndexedDB > frame-player-user-preferences > keyvaluepairs > [user creds entry]`

image.png

Frame App

For Frame App, users must delete the cache folder by clearing the **User Cache** in Preferences.

Troubleshooting

Errors

Incorrect Username or Password

If the user attempts to register a username or password that cannot be validated by their domain controller, Frame Terminal will display:

image.png

The user will need to ensure they are entering the correct domain credentials.

Maximum number of login attempts exceeded

If the user exceeds the maximum number of login attempts as defined by their administrator's domain policies, then Frame Terminal will return an error.

image.png

The user should revalidate their domain user credentials outside of Frame and may need to contact their Windows administrator to reset their domain password.

Revision #13
Created 1 October 2025 04:51:45
Updated 17 December 2025 16:31:19 by Dominik Conrad