



Known Issues for Hybrid Data Security

- If you shut down your Hybrid Data Security cluster (by deleting it in Cisco Webex Control Hub or by shutting down all nodes), lose your configuration ISO file, or lose access to the keystore database, your Cisco Webex Teams users can no longer use spaces under their People list that were created with keys from your KMS. This applies to both trial and production deployments. We do not currently have a workaround or fix for this issue and urge you not to shut down your HDS services once they are handling active user accounts.
- A client which has an existing ECDH connection to a KMS maintains that connection for a period of time (likely one hour). When a user becomes a member of a Hybrid Data Security trial, the user's client continues to use the existing ECDH connection until it times out. Alternatively, the user can sign out and back in to the Cisco Webex Teams app to update the location that the app contacts for encryption keys.

The same behavior occurs when you move a trial to production for the organization. All non-trial users with existing ECDH connections to the previous data security services will continue to use those services until the ECDH connection is renegotiated (through timeout or by signing out and back in).

