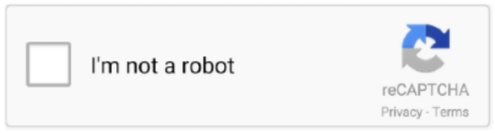

Continue

Configuring Active Directory To Support Kerberos For Mac

After the initial login, end users can access any Kerberos-enabled service in the network (such as webmail) without having to log in again until the SSO session expires (the SSO session duration is established by the Kerberos administrator).. If the portal or gateway is not running in FIPS or CC mode, you can also use des3-cbc-sha1 or arcfour-hmac.. If the GlobalProtect portal or gateway is running in FIPS or CC mode, the algorithm must be aes128-cts-hmac-sha1-96 or aes256-cts-hmac-sha1-96.. Networks that support Kerberos SSO require end users to log in only during initial network access.. This authentication method helps identify users for user and HIP policy enforcement.. (Optional) Authentication Message—Message that is displayed when end users log in to the portal.

The GlobalProtect™ app for Mac endpoints now supports (SSO) for GlobalProtect portal and gateway authentication.. The must match the algorithm in the service ticket issued by the TGS, which is determined by the Kerberos administrator.. • for Kerberos authentication • Import the Kerberos keytab file to an • Select Device Authentication Profile.. • Click OK to save your changes • Configure the GlobalProtect app behavior for Kerberos authentication failure.. The and are the principal name and password of the GlobalProtect portal or gateway.. The ultimate bug catcher on flowvella Kerberos SSO maintains a seamless logon experience by providing accurate User-ID™ information without user interaction.. Jsq client for mac • Select an existing authentication profile or Add a new one.