

Reissue KDC Authentication certificate for domain controllers

- Parallels Secure Workspace

Symptoms

Authentication issues when using single sign-on (SSO).

Cause

Expired Kerberos Domain Controller certificate (intended purpose: KDC Authentication).

Resolution

1. On **each** Microsoft Windows Kerberos Domain Controller, press **[Win] + R**.
2. Enter **certlm.msc** and press [OK] to launch the management console showing the certificates of the local computer.
3. Navigate to **Personal > Certificates**.
4. Check that you have a valid **KDC Authentication Certificate** for each Domain Controller (it should be listed under the "Intended purposes" column).
Make sure the certificate exists and that it has not expired. If it is expired or missing, the Domain Controller needs to be issued a new certificate for **KDC Authentication**.

?

Note: if there were other certificates being used by the KDCs, it may be necessary to restart the "Kerberos Key Distribution Center" service on the Microsoft Windows Server to make sure the Kerberos service uses the new certificate.

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.