



Preauth module pkinit (17) (real) returned: -1765328313/Failed to verify received certificate (depth 0): certificate has expired

- Parallels Secure Workspace

Symptoms

First see [How to analyze the log files to identify single-sign on \(SSO\) issues](#) .

Single sign-on fails. In **awingu-worker-smc.service.log**, a similar error can be seen:

```
2022-11-05 18:15:28.770421 somehost
awingu-worker-smc.service[manage.py:16089]: Processed
[sad-south-stairway-magnesium]
2022-11-05 18:16:17.285456 somehost
awingu-worker-smc.service[manage.py:5655]: Process-1:34 processing
cdsessions.tasks.refresh_sso_certificate [fourteen-lithium-east-bakerloo]
2022-11-05 18:16:17.350102 somehost awingu-worker-smc.service[python:15376]:
Generating a RSA private key
2022-11-05 18:16:17.481250 somehost awingu-worker-smc.service[python:15376]:
.....+++++
2022-11-05 18:16:17.654401 somehost awingu-worker-smc.service[python:15376]:
.....+++++
2022-11-05 18:16:17.654690 somehost awingu-worker-smc.service[python:15376]:
writing new private key to 'private_key.pem'
2022-11-05 18:16:17.654865 somehost awingu-worker-smc.service[python:15376]:
-----
2022-11-05 18:16:17.770724 somehost awingu-worker-smc.service[python:15376]:
writing RSA key
2022-11-05 18:16:17.965336 somehost
awingu-worker-smc.service[manage.py:5655]: Password for
someuser\@somewindowsdomain.com@SOMEWINDOWSDOMAIN.COM:

2022-11-05 18:16:17.965771 somehost
awingu-worker-smc.service[manage.py:5655]: Using specified cache:
/etc/awingu/domains/SOMEAWINGUDOMAIN/8cle5c53-7f4c-4a8d-acb9-2003659eafa9/kerberos/k
Using principal: someuser\@somewindowsdomain.com@SOMEWINDOWSDOMAIN.COM
PA Option X509_user_identity =
FILE:/etc/awingu/domains/SOMEAWINGUDOMAIN/8cle5c53-7f4c-4a8d-acb9-2003659eafa9/certi
[17101] 1667672177.784037: Getting initial credentials for
someuser\@somewindowsdomain.com@SOMEWINDOWSDOMAIN.COM
[17101] 1667672177.784039: Sending unauthenticated request
[17101] 1667672177.784040: Sending request (200 bytes) to
SOMEWINDOWSDOMAIN.COM
[17101] 1667672177.784041: Resolving hostname somedc.somewindowsdomain.com
[17101] 1667672177.784042: Sending initial UDP request to dgram 10.1.2.3:88
[17101] 1667672177.784043: Received answer (189 bytes) from dgram 10.1.2.3:88
[17101] 1667672177.784044: Sending DNS URI query for
_kerberos.SOMEWINDOWSDOMAIN.COM.
[17101] 1667672177.784045: No URI records found
[17101] 1667672177.784046: Sending DNS SRV query for
```

```
_kerberos-master._udp.SOMEWINDOWSDOMAIN.COM.  
[17101] 1667672177.784047: Sending DNS SRV query for  
_kerberos-master._tcp.SOMEWINDOWSDOMAIN.COM.  
[17101] 1667672177.784048: No SRV records found  
[17101] 1667672177.784049: Response was not from master KDC  
[17101] 1667672177.784050: Received error from KDC: -1765328359/Additional  
pre-authentication required  
[17101] 1667672177.784053: Preauthenticating using KDC method data  
[17101] 1667672177.784054: Processing preauth types: PA-PK-AS-REQ (16),  
PA-PK-AS-REP_OLD (15), PA-ETYPE-INFO2 (19), PA-ENC-TIMESTAMP (2)  
[17101] 1667672177.784055: Selected etype info: etype aes256-cts, salt  
"SOMEWINDOWSDOMAIN.COMsomeuser", params ""  
[17101] 1667672177.784056: PKINIT loading CA certs and CRLs from FILE  
[17101] 1667672177.784057: PKINIT client computed kdc-req-body checksum  
9/D137800B66AECBEEA5B4A5E7A1B12F0F122A1367  
[17101] 1667672177.784059: PKINIT client making DH request  
[17101] 1667672177.784060: Preauth module pkinit (16) (real) returned:  
0/Success  
[17101] 1667672177.784061: Produced preauth for next request: PA-PK-AS-REQ  
(16)  
[17101] 1667672177.784062: Sending request (4918 bytes) to  
SOMEWINDOWSDOMAIN.COM  
[17101] 1667672177.784063: Resolving hostname somedc.somewindowsdomain.com  
[17101] 1667672177.784064: Initiating TCP connection to stream 10.1.2.3:88  
[17101] 1667672177.784065: Sending TCP request to stream 10.1.2.3:88  
[17101] 1667672177.784066: Received answer (4311 bytes) from stream  
10.1.2.3:88  
[17101] 1667672177.784067: Terminating TCP connection to stream 10.1.2.3:88  
[17101] 1667672177.784068: Sending DNS URI query for  
_kerberos.SOMEWINDOWSDOMAIN.COM.  
[17101] 1667672177.784069: No URI records found  
[17101] 1667672177.784070: Sending DNS SRV query for  
_kerberos-master._udp.SOMEWINDOWSDOMAIN.COM.  
[17101] 1667672177.784071: Sending DNS SRV query for  
_kerberos-master._tcp.SOMEWINDOWSDOMAIN.COM.  
[17101] 1667672177.784072: No SRV records found  
[17101] 1667672177.784073: Response was not from master KDC  
[17101] 1667672177.784074: Processing preauth types: PA-PK-AS-REP (17)  
[17101] 1667672177.784075: PKINIT OpenSSL error: Failed to verify received  
certificate (depth 0): certificate has expired  
[17101] 1667672177.784076: PKINIT client could not verify DH reply  
[17101] 1667672177.784077: Preauth module pkinit (17) (real) returned:  
-1765328313/Failed to verify received certificate (depth 0): certificate has  
expired  
[17101] 1667672177.784078: Produced preauth for next request: (empty)  
[17101] 1667672177.784079: Getting AS key, salt  
"SOMEWINDOWSDOMAIN.COMsomeuser", params ""  
kinit: Cannot read password while getting initial credentials
```

Cause

The Parallels Secure Workspace appliance does not trust the certificate presented by the Kerberos Domain Controller.

Resolution

- Validate the "trusted roots" file that is uploaded in **System Settings > Configure > User Connector:**

© 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.