AAD - Fiddler Trace for advanced Troubleshooting

Last updated by | Vitor Tomaz | Feb 18, 2021 at 2:30 AM PST

Contents

AAD - Fiddler Trace for advanced Troubleshooting

Using Fiddler Trace

On scenarios where TSG failed or do not help resolve the problem, please request customer to try logging in via Universal authentication and grab a Fiddler trace for further analysis.

DISCLAIMER: Please inform the customer that these two traces will capture the user password, so it is recommended they create a dummy user for capturing these traces.

Steps

How to Grab a Fiddler Trace?

1. Please download Fiddler from here https://www.telerik.com/download/fiddler
2. Install Fiddler and add root certificate.
3. Please get a "Fiddler Trace" with "Decrypt HTTPS Traffic" option checked in

[Tools->Options->HTTPS] .

4. Launch SSMS
5. Try to login with AAD
6. Stop capture in Fiddler
7. Save and send trace.

How to Debug Fiddler Trace?

1. Open the Fiddler trace.
2. Look for a call to Host "login.windows.net ⤤" or "login.microsoftonline.com ⤤" in the left pane.
3. Select the frame, and look to the right. The upper panel contains the request. You can expand the request by clicking on "Raw" and view the request packet being sent to AAD.

4. Look for the corresponding response value. The responses from AAD are usually very specific and will help guide the customer on what is missing in the authentication request.

{"**error":"interaction_required","error_description"**:"AADSTS50079: The user is required to use multi-factor authentication......"

5. If the Fiddler trace contains a "seemingly legitimate" access token, you can grab the token from the trace and debug the token. (Again, a valid token is a potential privacy issue. The customer can either wait for the token to be expired or work closely with CSS on this such that the token does not leave customer environment)

How to Debug the AAD Token?

1. Grab the AAD issued accesstoken.
2. Open a browser of your choice and go to https://jwt.io/ ⧉
3. Paste the token in the following box:

Encoded PASTE A TOKEN HERE

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzd
WIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IkpvaG4gRG9
lIiwiYWRtaW4iOnRydWV9.TJVA95OrM7E2cBab30RM
HrHDcEfxjoYZgeFONFh7HgQ
```

4. Once you paste the token, the right side automatically parses the token. Validate the properties of the token (like expiration time, tenantId, person who this token was issued to). To get precise information on what could potentially be wrong with the token, look for the information in Kusto table **MonFedAuthTicketService** (details mentioned above)

How good have you found this content?

🙂 🙁