

# Web-Activity-Failure-when-using-expired-SSL-TLS-certificates

Last updated by | Veena Pachauri | Mar 16, 2023 at 1:49 AM PDT

## Web Activity Failure when using expired SSL/TLS certificates

### Contents

- [Issue](#)
- [Troubleshooting](#)
- [Cause](#)
- [Resolution \(Recommended\)](#)
- [Workaround \(Non-recommended\)](#)

## Issue

Web Activity Failure when using expired SSL/TLS certificates.

This issue is observed when the WEB Activity keeps on failing either intermittently or consistently with the below error.

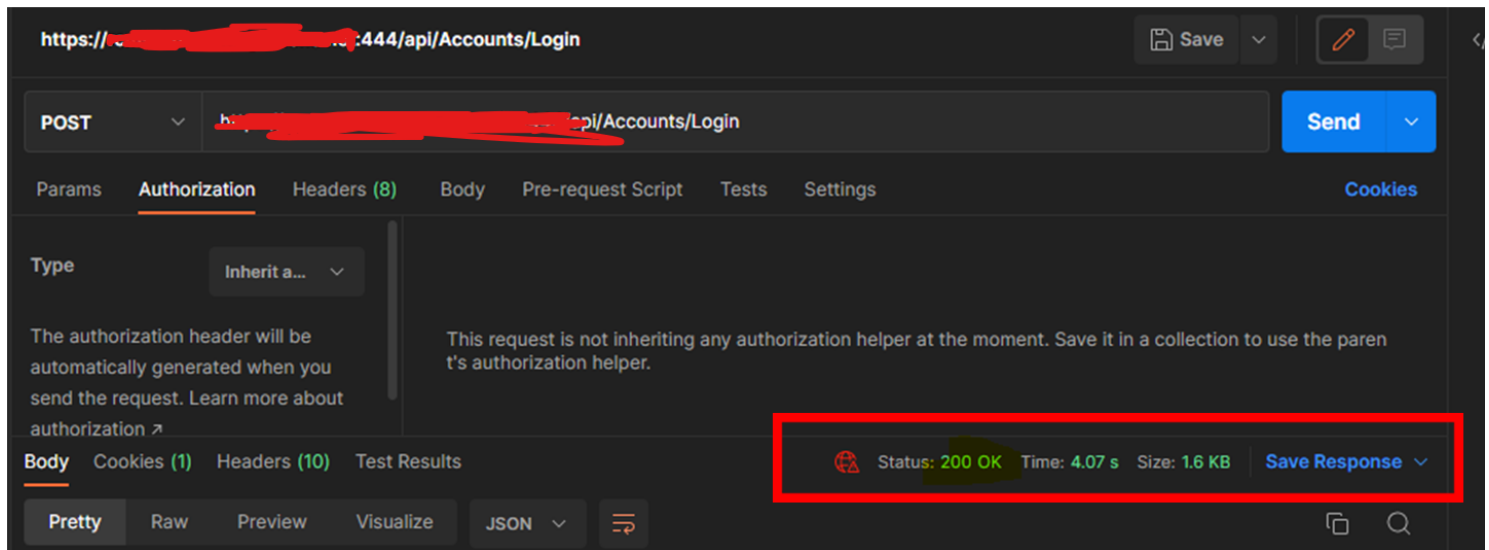
Response status code: 'NA - Unknown'. More details: Exception message: 'NA - Unknown [ClientSideException] An error occurred while sending the request.'. **The request didn't reach the server from client. This could happen because of an underlying issue such as network connectivity, a DNS failure, a server certificate validation, or a timeout.**

## Troubleshooting

1] Look into the CustomLogEvent and it would show a web activity failure with status NA – unknown:

```
#2023-01-05 08:01:02.8942276 <LogProperties><Text>ExecuteWebActivityAsync: invoking POST on https://rcm-zones-integrations.net:444/api/Accounts/Login, in datafactory zones-datafactoryV2-uat, region eu</Text></LogProperties>
#2023-01-05 08:01:02.8942606 <LogProperties><Text>WriteAsync: start</Text></LogProperties>
#2023-01-05 08:01:02.8942902 <LogProperties><Text>WriteAsync: Generating body for method POST</Text></LogProperties>
#2023-01-05 08:01:02.8943340 <LogProperties><Text>WriteAsync: Invoking endpoint - https://rcm-zones-integrations.net:444/api/Accounts/Login</Text></LogProperties>
#2023-01-05 08:01:02.9146228 <LogProperties><Text>GetStateFromExceptionType: Processing exception of type ClientSideException with status NA - Unknown</Text></LogProperties>
#2023-01-05 08:01:02.9146708 <LogProperties><Text>StartAsync failed. Extracting internal message. An error occurred while sending the request.</Text></FunctionName></FunctionName></FunctionParameter></FunctionParameter></LogProperties>
```

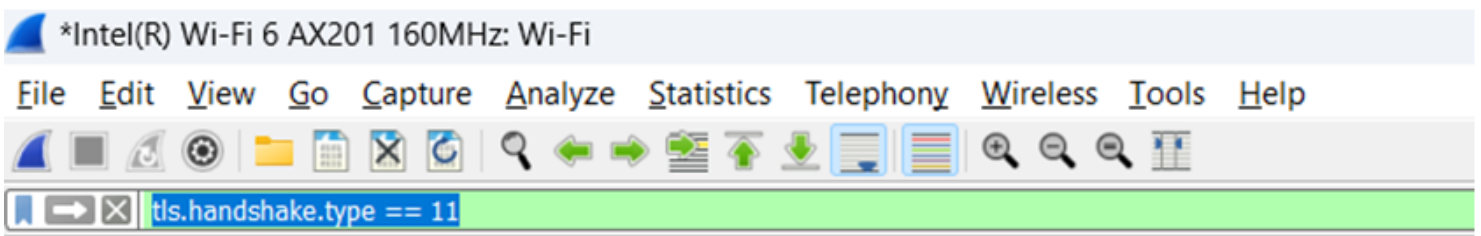
2] Check if we are able to reach the server endpoint through the POSTMAN, It should show the **status: 200 OK** means we are able to reach the endpoint from the POSTMAN. See below snippet



3] Take a network trace with Wireshark while replicating the issue using POSTMAN (if we are able to reach the server through POSTMAN) from endpoint while Wireshark was running:

4] Filter network trace using the below command :

`tls.handshake.type == 11`



Example as below :

No.	Time	Source	Destination	Src Port	Dst Port	TTL	Protocol	SNI (TLS) - Server Name	Info
219	2023-01-06 12:06:20.189952	192.168.1.3	13.82.173.85	61370	444	128	TCP		61370 → 444 [59K] Seq=2495134283 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
219	2023-01-06 12:06:20.234255	192.168.1.3	13.82.173.85	61370	444	128	TCP		444 → 61370 [15K] Seq=855097720 Win=65536 Len=0 MSS=1460 WS=256 SACK_PERM=1
220	2023-01-06 12:06:20.236360	192.168.1.3	13.82.173.85	61370	444	128	TLSv1.2		61370 → 444 [ACK] Seq=2495134284 Ack=855097720 Win=132352 Len=0 Client Hello
222	2023-01-06 12:06:20.368660	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
223	2023-01-06 12:06:20.368671	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
224	2023-01-06 12:06:20.368674	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
225	2023-01-06 12:06:20.368676	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
226	2023-01-06 12:06:20.368687	13.82.173.85	192.168.1.3	444	61370	111	TLSv1.2		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
227	2023-01-06 12:06:20.369347	192.168.1.3	13.82.173.85	61370	444	128	TCP		61370 → 444 [ACK] Seq=2495134801 Ack=855097720 Win=132352 Len=0
228	2023-01-06 12:06:20.377927	192.168.1.3	13.82.173.85	61370	444	128	TLSv1.2		61370 → 444 [ACK] Seq=2495134801 Ack=855097720 Win=132352 Len=0
230	2023-01-06 12:06:20.505057	13.82.173.85	192.168.1.3	444	61370	111	TLSv1.2		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
231	2023-01-06 12:06:20.505104	192.168.1.3	13.82.173.85	61370	444	128	TLSv1.2		61370 → 444 [ACK] Seq=2495134801 Ack=855097720 Win=132352 Len=0
237	2023-01-06 12:06:20.620946	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
238	2023-01-06 12:06:20.665763	13.82.173.85	192.168.1.3	444	61370	111	TCP		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
239	2023-01-06 12:06:20.665763	13.82.173.85	192.168.1.3	444	61370	111	TLSv1.2		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
240	2023-01-06 12:06:20.665765	13.82.173.85	192.168.1.3	444	61370	111	TLSv1.2		444 → 61370 [ACK] Seq=855097720 Ack=2495134801 Win=525856 Len=0
241	2023-01-06 12:06:20.666058	192.168.1.3	13.82.173.85	61370	444	128	TCP		61370 → 444 [ACK] Seq=2495136653 Ack=855099128 Win=132352 Len=0

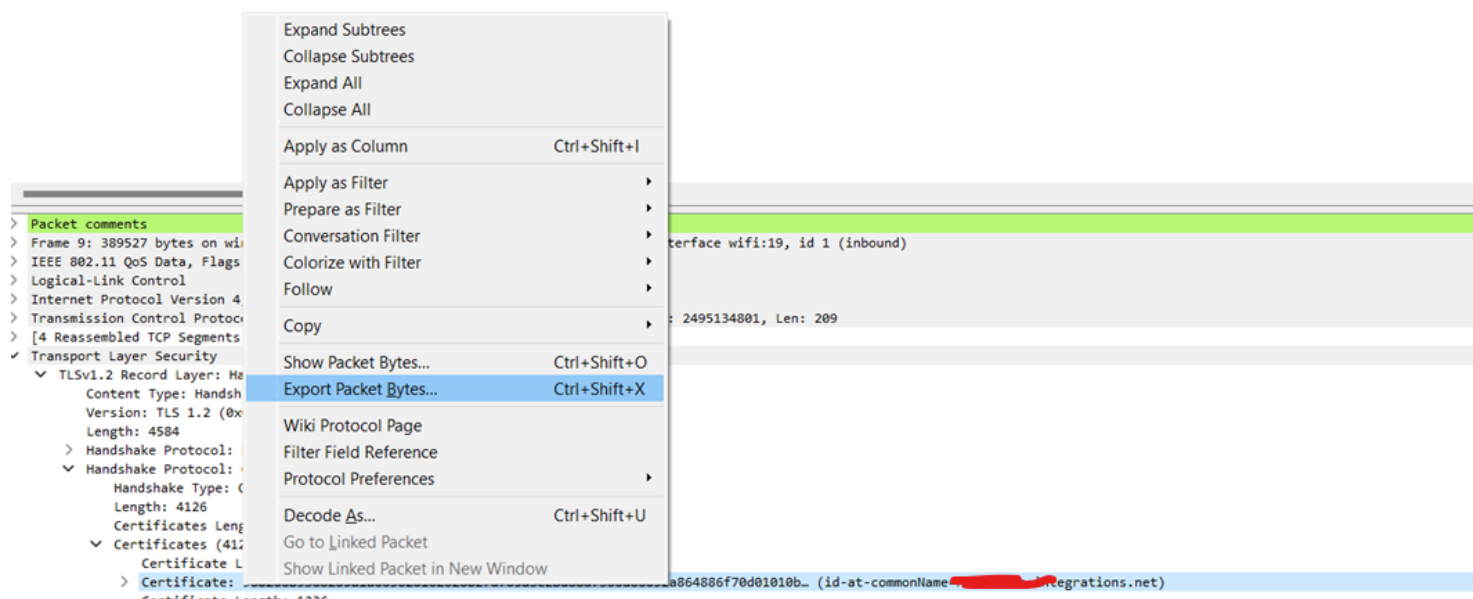
This will show all server certificates in the network trace. Then, you should select the correct SNI used by the https endpoint. See for the Server Name (SNI). Then, in the packet details pane, Server Hello, we can find the certificate validity:

```

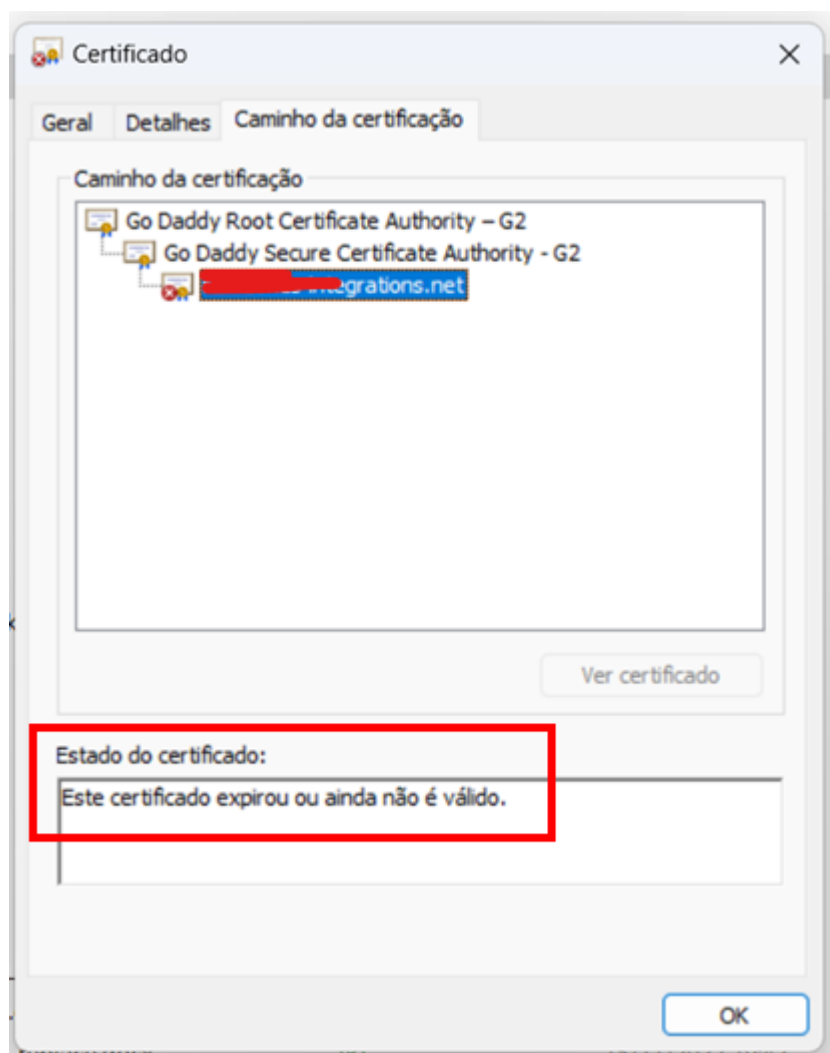
Certificate: 308206b9308205a1a003020102020827d705a3c2bd88d7300d06092a864886f70d01010b... (id-at-commonName=rcm-zones-integrations.net)
  signedCertificate
    version: v3 (2)
    serialNumber: 0x27d705a3c2bd88d7
    signature (sha256WithRSAEncryption)
    issuer: rdnSequence (0)
  validity
    notBefore: utcTime (0)
      utcTime: 2021-12-02 19:52:18 (UTC)
    notAfter: utcTime (0)
      utcTime: 2023-01-03 19:52:18 (UTC)

```

Or, if you select the same packet and perform an export packet Bytes in Wireshark

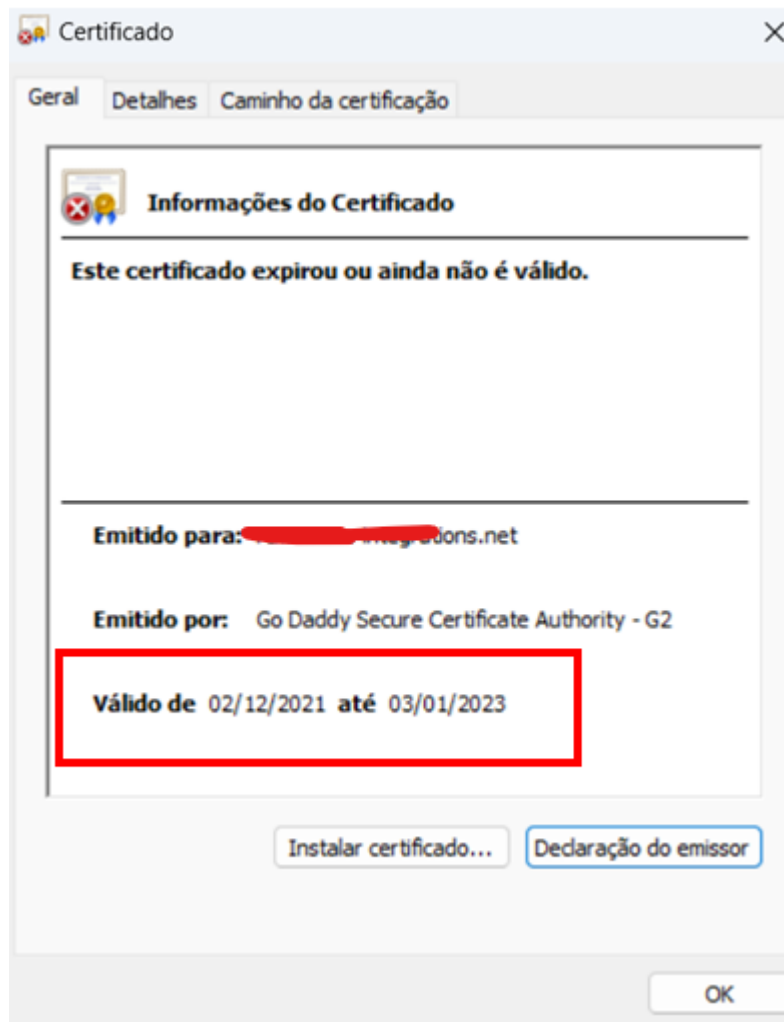


And save it as test.crt file type. You will be able to open the certificate:



On top, we have a message saying the certificate is not valid or the certificate is expired.

Then, you can see the certificate validation:



Which is not valid after 03-01-2023, 19:52:18 UTC. And in this example, the pipelines started to fail at: 3rd January 2023 at 08:00 PM UTC time.

## Cause

The validation from ADF to HTTP server was failing due to the expired certificates at the server end and leading to our WEB activity failure.

## Resolution (Recommended)

**Recommended** As we can confirm that the server-side certificate is expired, recommend customer to renew their certificates.

**\*\*NOTE: \*\*** Once, certificates are valid, the issue would be resolved.

## Workaround (Non-recommended)

We can disable certificate validation from the settings pane of the Web activity of the pipeline, but disabling the certificate validation means the data is not encrypted. This is something not recommended until you are connected to a trusted server that does not use a standard CA cert.

**NOTE:** Let the customer know about the risk of disabling the certificate validation if cx or SE is going forward with the workaround of disabling the cert validation.

Refer: <https://learn.microsoft.com/en-us/azure/data-factory/control-flow-web-activity#type-properties> 

<code>disableCertValidation</code>	Removes server side certificate validation (not recommended unless you are connecting to a trusted server that does not use a standard CA cert).	Allowed values are false (default) and true.	No
------------------------------------	--	--	----

- **Reviewer:** Veena Pachauri
- **Keywords:** Web Activity

How good have you found this content?

