

# Addl Endpoints for AAD Auth & CRL Checks

Last updated by | Yao Siabi | Feb 22, 2023 at 11:44 AM PST

## Additional Endpoints Required for AAD Authentication and CRL Checks


### Contents

- [Additional Endpoints Required for AAD Authentication an...](#)
  - [Issue](#)
  - [Investigation/Analysis](#)
  - [Mitigation](#)
  - [Limitations](#)
  - [More Information](#)
  - [Publicly Accessible References](#)
  - [Internally Accessible References](#)
  - [Root Cause Classification](#)

### Issue

Attempts to connect with an Azure Active Directory account are failing with a timeout error, but SQL Authentication works as expected. Alternatively you could be encountering generic connection errors with the inner exception being 'Revocation of the SSL certificate failed'.

This is for situations in which the customer is not willing to accept either of these workarounds:

- Disabling the SSL Certificate Revocation Check
  - <https://techcommunity.microsoft.com/t5/azure-database-support-blog/revocation-of-the-ssl-certificate-failed-for-aad-authentication/ba-p/2278773> 
- Allowing all SSL traffic from that server on their firewall

The Kusto telemetry may reveal an Error 33155 State 1.

An example timeout error from the client application could be:

Cannot connect to your\_server\_name.database.windows.net.

Failed to authenticate the user [aad\\_user\\_name@yourcompany.onmicrosoft.com](#) in Active Directory (Authentication=ActiveDirectoryPassword).

Error code 0xCA82EE2; state 10

The request has timed out. (.Net SqlClient Data Provider)

An example of the 'Revocation of the SSL certificate failed' error in SSMS:  
One or more errors occurred. (mscorlib)

One or more errors occurred. (mscorlib)














Revocation of the SSL certificate failed. (System.Data)




## Investigation/Analysis

- Investigate Kusto Telemetry to determine if the traffic is reaching the service, and what the error is from our side if so
- ADFS is used to sync a customer's Active Directory environment to Azure Active Directory. If the customer has an Active Directory Federation Server (ADFS) setup to authenticate they will also need to whitelist their ADFS endpoint on port 443. To determine their ADFS endpoint, navigate to ASC and then to 'Tenant Explorer', then 'Domains', and finally 'Federations'. In addition a Fiddler trace would show it. Fiddler would also reveal how the client machine is resolving the ADFS endpoint URL via DNS which can be helpful if there are multiple Ips and a subsection of them are blocked.
- Test connectivity to the endpoints described below as necessary and whitelist them if blocked, for example use PowerShell to "tnc [login.windows.net](https://login.windows.net) -port 443". Work through the URLs without wildcards first.
- Take a Fiddler Trace to Determine where traffic is being blocked

## Mitigation

This is a non-exhaustive list of endpoints that may be required depending on the authentication type. This is compiled from several documents and there is no known exhaustive list of endpoints required, public or otherwise. Additional endpoints may be required to communicate with ADFS, or depending on the customer networking path, endpoints to reach who if they are using a public CA for ADFS (Godaddy, etc).

URL	Port	Description
<a href="https://mscrl.microsoft.com">mscrl.microsoft.com</a> 	HTTP/80	Used to download CRL lists.
*.verisign.com	HTTP/80	Used to download CRL lists.
*.entrust.net	HTTP/80	Used to download CRL lists for MFA.
*.management.core.windows.net (Azure Storage)	HTTPS/443	Used for the various Azure services
*.graph.windows.net (Azure AD Graph)	HTTPS/443	Used for various Azure Services
<a href="https://secure.aadcdn.microsoftonline-p.com">secure.aadcdn.microsoftonline-p.com</a> 	HTTPS/443	Used for MFA.
*.microsoftonline.com	HTTPS/443	Used to configure your Azure AD directory and import/export data.
login.microsoftonline.us	HTTPS/443	Used by US Gov for AD Login.
<a href="https://login.microsoftonline.com">login.microsoftonline.com</a> 	HTTPS/443	Used by Public cloud for AD login for MFA.
<a href="https://login.windows.net">login.windows.net</a> 	HTTPS/443	Used by Public cloud for AD login for Password and Integrated.
<a href="http://crl.microsoft.com">http://crl.microsoft.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://crl3.digicert.com">http://crl3.digicert.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://crl4.digicert.com">http://crl4.digicert.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://ocsp.digicert.com">http://ocsp.digicert.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://www.d-trust.net">http://www.d-trust.net</a> 	HTTP/80	Used to verify certificates.
<a href="http://root-c3-ca2-2009.ocsp.d-trust.net">http://root-c3-ca2-2009.ocsp.d-trust.net</a> 	HTTP/80	Used to verify certificates.
<a href="http://crl.microsoft.com">http://crl.microsoft.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://oneocsp.microsoft.com">http://oneocsp.microsoft.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://ocsp.msocsp.com">http://ocsp.msocsp.com</a> 	HTTP/80	Used to verify certificates.

URL	Port	Description
<a href="http://www.microsoft.com/pkiops">http://www.microsoft.com/pkiops</a> 	HTTP/80	Used to verify certificates.
<a href="http://cacerts.digicert.com">cacerts.digicert.com</a> 	HTTP/80	Used to verify certificates.
<a href="http://ctldl.windowsupdate.com">ctldl.windowsupdate.com</a> 	HTTP/80	Used to verify certificates.

## Limitations


Please be aware this may introduce the Fiddler ESTS issue if Fiddler is used for troubleshooting.

- [https://supportability.visualstudio.com/AzureSQLDB/\\_wiki/wikis/AzureSQLDB.wiki/841937/Windows-Authentication-Fiddler-ESTS-Issue](https://supportability.visualstudio.com/AzureSQLDB/_wiki/wikis/AzureSQLDB.wiki/841937/Windows-Authentication-Fiddler-ESTS-Issue)

## More Information

Taking a Fiddler trace should also reveal the endpoint being blocked, or show the certificate (which will have the CRL endpoints listed) as long as you have HTTPS Decryption enabled. If possible, having a TEAMS meeting with the customer when they have the ability to reproduce and view the blocked traffic on their firewall may lead to expedited troubleshooting if they have multiple ports blocked, as Fiddler traces may only show one block at a time. Please note not all Firewalls can be configured to accept wildcards, while the above list has as many explicitly defined URLs as possible, you may need to see what traffic is being blocked on the Firewall to get definite URLs for those not fully defined here.

## Publicly Accessible References

- <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/certificate-authorities> 
- <https://docs.microsoft.com/en-us/azure/security/fundamentals/tls-certificate-changes> 
- <https://docs.microsoft.com/en-us/azure/active-directory/hybrid/tshoot-connect-connectivity#troubleshoot-connectivity-issues-in-the-installation-wizard> 
- <https://techcommunity.microsoft.com/t5/azure-database-support-blog/revocation-of-the-ssl-certificate-failed-for-aad-authentication/ba-p/2278773> 
- <https://docs.microsoft.com/en-us/microsoft-365/enterprise/microsoft-365-endpoints?view=o365-worldwide> 

## Internally Accessible References

- [https://supportability.visualstudio.com/AzureSQLDB/\\_wiki/wikis/AzureSQLDB.wiki/277597/Error-33155-State-1](https://supportability.visualstudio.com/AzureSQLDB/_wiki/wikis/AzureSQLDB.wiki/277597/Error-33155-State-1)
- [https://supportability.visualstudio.com/AzureSQLDB/\\_wiki/wikis/AzureSQLDB.wiki/286335/Error-33155](https://supportability.visualstudio.com/AzureSQLDB/_wiki/wikis/AzureSQLDB.wiki/286335/Error-33155)
- [https://supportability.visualstudio.com/AzureSQLDB/\\_wiki/wikis/AzureSQLDB.wiki/282783/AAD-Fiddler-Trace-for-advanced-Troubleshooting](https://supportability.visualstudio.com/AzureSQLDB/_wiki/wikis/AzureSQLDB.wiki/282783/AAD-Fiddler-Trace-for-advanced-Troubleshooting)

## Root Cause Classification

Azure SQL v3/Connectivity/Login Errors/Firewall errors and misconfigurations

**How good have you found this content?**

