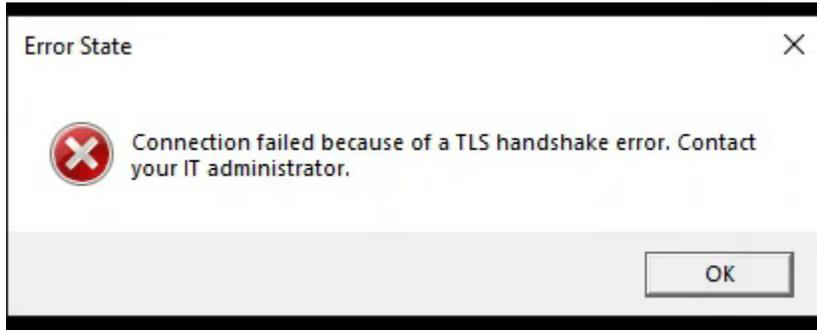


Accessing FINI Testing Environment – VPN Connection Certificate Refresh

This document provide a step-by-step guide to renew the VPN configuration file in case the Client-To-Site VPN users encounter the TLS connection problem as shown in the diagram below.

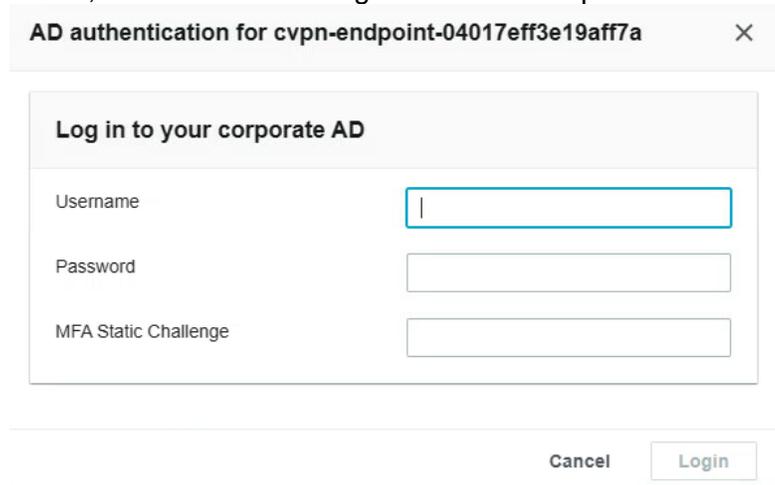


Steps 1

Go to: <https://self-service.clientvpn.amazonaws.com/endpoints/cvpn-endpoint-04017eff3e19aff7a>

Steps 2

Input Username, Password & Existing MFA Static Response

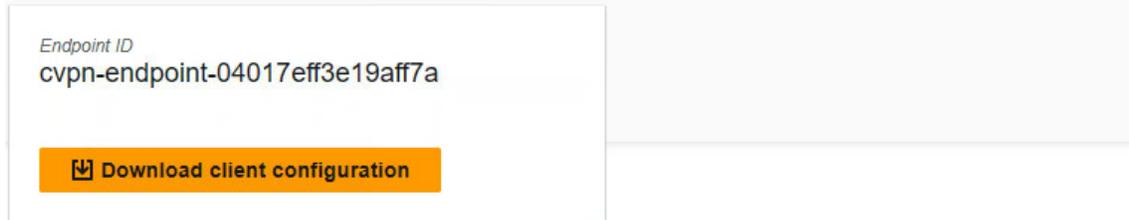


An authentication form titled "AD authentication for cvpn-endpoint-04017eff3e19aff7a" with a close button (X) in the top right corner. The form has a header "Log in to your corporate AD". Below the header, there are three input fields: "Username" (with a cursor), "Password", and "MFA Static Challenge". At the bottom of the form, there are two buttons: "Cancel" and "Login".

Steps 3

Download Client Configuration

Download the VPN client configuration file for the endpoint



Step 4

Re-import the new VPN Client Configuration file

- File -> Manage Profiles ->
- Enter Display Name (free text)
- Select the newly download configuration profile
- Press Add Profile
- Select new profile and re-establish the connection

