GSD. Network – VPN – Cisco AnyConnect Connection Issue

Article ID: KB0039762
Created: 2024-12-19 14:03:33
Updated: 2024-12-19 14:03:33
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/b513d404c3ca1a100acd3300150131fb', 'value': 'b513d404c3ca1a100acd3300150131fb'}

General Information:

Possible symptoms/errors:

User has VPN Certificate Validation Failure when connecting to VPNUser has Cisco AnyConnect Connection IssueCisco AnyConnect prompt for credentials

Alternative names of the system:

VPN Cisco

IMPORTANT NOTICE:

If Cisco AnyConnect prompt for credentials, there is the issue with VPN Certificate. Follow standard troubleshooting for VPN Certificate issue.

Solution:

The reason why this error occurs when connecting to VPN might be a combination of certificate and connection entry or certificate has expired or is invalid. User should try to connect by changing the connection entry first.

Details:

Advise user to open Cisco AnyConnect Secure Mobility Client application from the system tray if already running. Otherwise, user must start it first.

The only supported gateway is vpn.fresenius.com If a user connects to vpn-access.fresenius.com or vpn-gw.fresenius.de he/she should be migrated to vpn.fresenius.com asap(It requires a new CA09 user certificate and a MultiFactor enabled Azure AD User) If the connection entry says vpn-access.fresenius.com, inform user to replace it with any of the following:

vpn.fresenius.com

If the connection entry is vpn-gw.fresenius.de, user must replace it with:

vpn.fresenius.com

User should now be able to connect to VPN successfully.If the issue persists, check expiration date of Certificate by advising user to:

Open Internet OptionsGo to ContentGo to Certificates

Advise user to reconnect VPN if certificates are not expired. If a pop up window for logon and password is shown while connecting to VPN, it means that wrong domain has been selected (or there any other

fault).   If issue still persists, perform Cisco AnyConnect Profile Cleanup

Cisco AnyConnect Profile cleanup:

In case the user cannot connect to the VPN service and the app (AnyConnect) states there is no certificate file, even though it is imported (as can be checked in certmgr.msc => personal => certificates), the solution is reinstallation of the AnyConnect app or the profile cleanup.

Cisco AnyConnect profile is located in:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\

NOTE: Visibility of hidden folders needs to be enabled.

Folder profile needs to be deleted (or renamed for backup).

A. In case the laptop is connected to the internal network (is present at the office):

Advise user to log on to the laptop as an admin,User must shut down AnyConnect app,Guide user to delete\change name of the profile folder:

C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\ ,

Inform them to run Cisco AnyConnect and to enter the proper gateway,It will ask to select the certificate – advise user to select the proper one (usually there's only one to select).

NOTE: Admin rights needed to perform those steps.

B. In case the user is outside the office, it could be difficult as the needed action requires admin rights. It is possible only if the site and computer has been prepared for LAPS.

The LAPS password will change automatically in the AD after it was retrieved by someone. It can also be reset manually after retrieval via ServiceNow

Please refer to the following knowledge article about LAPS: KB0013973- How to request and use the LAPS feature in ServiceNow

Remote to the laptop with GoToRescueRun CMD as different user (shift+right RMB),Log on as local admin via .\admin and use the latest LAPS password In the Command Line enter the following commands: Cd\ Cd C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ Rename profile to profile_bak Run Cisco AnyConnect,Go to Options,In options\preferences check the box next to the option to accept the certificate file automatically - depending on AnyConnect version – it might not be there. If option do not appear make sure that the user knows that they need to accept the certificate file, as the app will ask them to do so. Enter the proper gateway and click connect. At this point you will lose the GoToRescue connection,It will ask to select the certificate – user needs to select the proper one (usually there's only one to select)

If there is an issue with certificates, create a ticket, and pass it to the 2nd level support:

Ext_WW_OCC-User-Administration_SLS_Capgemini

If other problem than certificates issue, create a ticket and pass it to the 2nd level support:

Int_WW_Network-Operations_SLS_FDT

Assignment Group:

Int_WW_Network-Operations_SLS_FDT

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/ASubcategory: N/A

Important Links:

N/A