

GSD. MFA for VPN - common issues

Article ID: KB0039788

Created: 2024-12-19 14:03:35

Updated: 2024-12-19 14:03:36

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:

VPN common issues

Alternative names of the system:

N/A

IMPORTANT NOTICE:

N/A

Solution:

Prerequisites to access MFA secured central VPN gateway "vpn.fresenius.com" :

AnyConnect at least 4.7 – make sure that all users received required version – 4.10 is recommended. If not, deploy AnyConnect client via SCCM.Certificate CA09 installed. MFA activated by user.

MFA guide for IT managers: \\fnc.ads.fresenius.com\DEEK1\Dat\netzwerk\projekte\VPN-MFA\Share

Most common issues based on Splunk data:

AnyConnect version

CA09 satus

MFA Status

Suggested actions

< 4.7

Applicable for all

Applicable for all

The lowest version that supports MFA is 4.7. 4.10 should be deployed to user device.

>= 4.7

Installed

Active

User meets all the prerequisites to use MFA VPN gateway. They should also have MFA profile installed. Action needed by user:

Choose vpn.fresenius.com from the AnyConnect dropdown list and try to connect. In case of any issues, they should raise incident or contact local support. In rare cases profile package might have not been installed properly. User can obtain it by manually entering "vpn.fresenius.com" in the AnyConnect VPN address. Profile file can also be installed from local SCCM.

>=4.7

No certificate/non CA09 certificate

Applicable for all

CA09 certificate is missing:

Double check if users is added to the right group and GPO is linked properly. If 1) is met, please check common certificate issues: <https://confluence.intra.fresenius.de/display/FNCAD/Troubleshoot+user+certificate+%28auto%29enrollment>

>= 4.7

Installed

MFA option if required

Action by users needed to activate MFA: https://fnc.service-now.com/sp?id=kb_article_view&sysparm_article=KB0010350&sys_kb_id=aa60ead4dba23814aefb64d60596191a

Once activated users should follow the general guide to start using MFA.

Assignment Group:

Int_WW_Collaboration_WPaaS_SLS_FDT

Ticket Creation:

Template: N/A Categorization:

Configuration Item: N/A Category: N/A Subcategory: N/A

Important Links:

N/A: