GSD. Network - VPN User Certificate Enrollment for External User

Article ID: KB0039800
Created: 2024-12-19 14:03:37
Updated: 2024-12-19 14:03:37
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/75145c00c30e1a100acd33001501318e', 'value': '75145c00c30e1a100acd33001501318e'}

General Information:

Possible symptoms/errors:

VPN User Certificate Enrollment for External User

Alternative names of the system:

N/A

IMPORTANT NOTICE:

N/A

Solution:

Please note that the user account must be enabled for the target service, e.g. VPN access, before executing the steps in this guide or enrollment will fail. Additionally, the target service may require configuration on the end user client before the certificate can be used, e.g. the VPN client must be installed and properly configured to work with the Fresenius infrastructure.

If an external consultant or contractor is required to use a Fresenius ADS CA user certificate (e.g. for VPN) the standard autoenrollment mechanism provided by the Microsoft Certification Services will not work as their clients are not a member of the Fresenius Active Directory or client management, and often they are based remotely and cannot connect to the Fresenius Global Network. To enable user certificate enrollment for these users we provide an alternative enrollment path via the Microsoft Certificate Web Services that are available via the Internet. As the clients are not managed by Fresenius there is no way to automatically set up the required configuration for these users, so this guide explains in detail the necessary steps to use this service.

Please be advised that to use this service the AD user account of the user must have been enabled and authorized for certificate enrollment. For example, if the user needs the certificate for VPN, the VPN service has to be ordered via the Service Portal for the AD account and the request must be completed before certificate enrollment will work.

This guide describes the manual steps to configure a Windows based client device to receive a user certificate. If the user uses a different type of client device (e.g. MacOS or Linux) then this process will not work. Currently there is no option to enroll for a user certificate from these devices.

Manual configuration of the client1) Adding the Fresenius ADS RootCA2 certificates to your computers certificate store2) Configure Fresenius enrollment settings3) Enroll for user certificateAutomatic setup

script

Manual configuration of the client

1) Adding the Fresenius ADS RootCA2 certificates to your computers certificate store

Open the Fresenius PKI website with any browser of your choice. Click on the "Fresenius RootCA2 PKI" link to jump to the corresponding section

Download the following certificates

Fresenius ADS RootCA2

Fresenius ADS CA04

Fresenius ADS CA06

Fresenius ADS CA09

These are the minimum required to enable certificate enrollment from Fresenius. Download these files to a folder on your local hard drive

Click on start and type "certlm.msc" to search and open the Microsoft Computer Certificate Management Console. It may prompt you for administrative access to run this console.

Open the "Trusted Root Certification Authorities" folder and right-click on the "Certificates" folder. This will open a context menu. Choose the "Import..." option from the "All Tasks" section.

This will open the Certificate Import Wizard. On the first page click "Next" to continue

On the "File to import" click on "Browse.." and open the folder with the certificates that you downloaded before.

At this point, you MUST select the "Fresenius ADS RootCA2.crt" certificate for import. Verify that it is correctly selected before clicking the "Next" button

On the "Certificate Store" page please make sure that the "Trusted Root Certification Authorities" is selected as the target Certificate store.

Verify that all settings are correct, then click on "Finish"

This concludes the import of the root ca certificate

Now open the "Intermediate Certification Authorities" folder and right click on the "Certificates" folder. This will open a context menu. Choose the "Import..." option from the "All Tasks" section.

This will open the the Certificate Import Wizard as shown above. On the "File to Import", now choose the "Fresenius ADS CA04.crt" from your folder

Continue through the wizard and verify that "Intermediate Certification Authorities" is selected as the target Certificate store

Continue through the wizard and verify that all settings are correct. Click on "Finish" to complete the import

Repeat these steps to import the remaining "Fresenius ADS CA06.crt" and "Fresenius ADS CA09.crt" into the "Intermediate Certification Authorities" store.

After this, you will find three Fresenius ADS CA certificates in the "Intermediate Certification Authorities" folder and one Fresenius ADS RootCA certificate in the "Trusted Root Certification Authorities" store

This completes the import of the Fresenius PKI

2) Configure Fresenius enrollment settings

Click on start and type "certmgr.msc" to find and open the Microsoft User Certificate Management console

Right click on the "Personal" folder and select "Manage Enrollment Policies" from the "Advanced Operations" in the "All Tasks" option

On the "Manage Enrollment Policies" dialog click on "Add"

On the "Certificate Enrolment Policy Server " dialog enter the following URL into the "Enrolment Policy Server URI" field

https://enroll2.fresenius.com/ADPolicyProvider_CEP_UsernamePassword/service.svc/CEP

Change the "Authentication Type" selection to "Username/password". Click on "Validate Server". This will prompt you for your Fresenius credentials. Please enter your Fresenius Email address and password

If everything was configured correctly and your client was able to contact the Fresenius enrollment service you will see a success message in the "properties" field. Click on "Add" to complete the process.

Back on the "Manage enrollment policies" dialog, select the new "enroll2.fresenius.com" entry and click on "Properties".

Delesect the "Enable for automatic enrolment and renewal" option, then click "Ok" to close the dialog

The "Automatic Enrollment" option is now disabled. Click on "Ok" to finish the configuration

3) Enroll for user certificate

Click on start and type "certmgr.msc" to find and open the Microsoft User Certificate Management console

Right click on the "Personal" folder and choose the "Request new Certificate..." option from "All Tasks"