FME - SPLIT - Site and Device Migrations

Article ID: KB0039901
Created: 2024-12-19 14:03:45
Updated: 2024-12-19 14:03:45
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:

FME user reports their personal device (laptop or desktop computer) has been migrated but they are facing issuesFME users was not able to participate in the migration of their personal device (laptop or desktop computer)

Alternative names of the system:

N/A

IMPORTANT NOTICE:

Please note that this KB is only applicable for FME Carve Out migration site (migration of personal devices) related tickets. In case of any FME tickets for non-migrated issues or questions, please follow standard GSD Knowledge Articles.

Solution:

NOTE: Migration of personal devices (laptops or desktop computers) is a part of Fresenius Medical Carve Out project – FME sites are going to be migrated in waves.

NOTE: Migration of personal devices and all changes will be announced to FME Users in advance, so that they are informed about the all necessary steps. Instructions are given to FME Users before their site is migrated.

1. The following steps need to be performed by FME End User before and during migration:

User's device needs to stay at the office and has to be connected to the office network during the migration. That means user will need to leave the device at the office for the time of the migration. If they leave work on the day of/before the migration, they need to make sure their device is switched on and connected to the office network. Users can lock their device, but can't switch it off.If for any reason user is unable to come into the office and/or leave their computer in the office overnight, there will be manual steps necessary to update their computer to the new FME network. User will receive contact to their site SPOC to inform about their unavailability. Local administrators will invite them to a virtual meeting to guide them through the process.During the evening of migration, users will be not able to use the device. They should not attempt to log into their device or use any of the applications and data on it.Users should ensure OneDrive synchronization is enabled and all of their required data and files are uploaded to OneDrive. This is a safety measure to ensure that all files are available after migration. Users' files will be transferred with the migration but in case there are issues, they might not be able to access them. In this case, the files on OneDrive will still be available.Where permitted by local law and

company policy, if users have a company mobile phone, it is recommended to set up their email and Microsoft Teams access on the mobile device. This will ensure users can access the instructions needed during and after the migration and get help in case of any issues.

2. The following steps need to be performed by FME End User after migration:

User should start their device and enter their Bitlocker PIN as usual.User needs to log into their device. They will be prompted to enter their user credentials:

- Username: “globalfme\username” (inserting their username after the “\”)

- Password: The same password as before

NOTE: If user has recently changed your password and the new password does not work, they should try the old password.

User should connect to the office network, preferably via LAN cable but Wi-Fi works as well.Once user is connected to the office network, there will be a software update running in the background. User should ensure a stable connection to the network and let this update complete without interrupting (they should not move around or change the network). During the update, the Software Center will temporarily not be available.The update and migration will happen in the background. All other applications are available, and user can continue their daily work.After the update, user's device will reboot after 5 minutes. User should allow the device to automatically reboot on its own (they should not reboot the device manually). User needs to use the 5 minutes to close all their applications and files and let the timer run down without interfering.

NOTE: Users will not have access to these instructions when they first try to log into their device. They should prepare themselves for the migration by writing down what to do and keeping their Bitlocker PIN and login credentials at hand.

NOTE: Single sign-on will work for most of FME applications. That means that FME users will not have to re-enter their login credentials. If single sign-on does not work, FME user will be prompted to reenter their existing credentials.

NOTE: After the migration, whenever FME users connect to the VPN, they should select the new profile “FME-VPN” within Cisco AnyConnect.

Assignment Group:

N/A

Ticket Creation:

Template: N/ACategorization:

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

Important Links:

N/A