Workaround for problems with local permission groups and cached Entra ID users

Problem description

Microsoft has a bug with local permission groups (e.g. Administrators & Remote Desktop Users) on Windows 10 & 11. If you use Microsoft Entra ID user objects to grant permissions onto Microsoft Entra ID joined devices you can do this either directly (as described here: Quick commands (Windows) | LNC DOCS (lucanoahcaprez.ch)) or using Microsoft Entra ID groups.

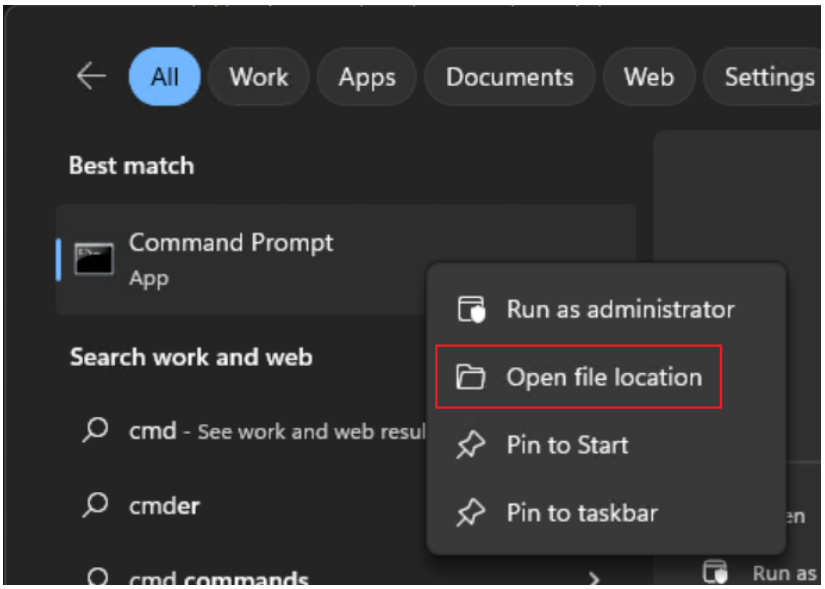
When using these groups you only see the SID of the group and their users are cached locally at the moment the group is added to the device. If you subsequently fill Microsoft Entra ID users into the Microsoft Entra ID groups, exactly this bug will occur. Then the new user entity will have no permissions. There is this workaround for this.

Force user object sync

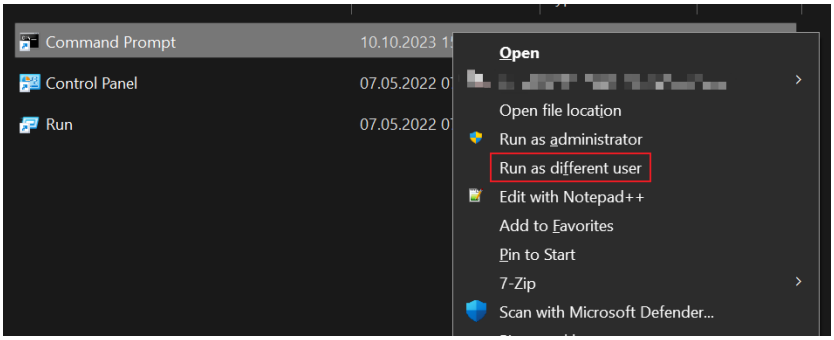
The basic idea is that the user logs in once with normal authorizations and thus triggers user synchronization on the device. One solution is for the user to log in to the device normally.

If this is not possible, for example because you are connected to a customer or the permissions are used for support purposes, the following can be done:

1. Open the file location of any program:



2. Run executable using the credential of the Microsoft Entra ID user account with the problems. Select "Run as different user".



3. Enter the UPN and password from the affected user account.

4. Check if the program is in the context of the appropriate user. For the example of "cmd" enter this and confirm the correct username:

```
whoami
```

5. Close window and now the permissions are synced correctly. You can now continue with the work that caused the problem in the first place.

Revision #1
Created 19 October 2023 11:22:37 by Luca Noah Caprez
Updated 19 October 2023 18:44:30 by Luca Noah Caprez