IPM service privilege customizing

Detailed procedure for customizing service privilege for Eaton Intelligent Power Manager on Windows systems.

Document revision : 1.0

Document date: May 22, 2018

Document state : validated

REVISION HISTORY

Revision	Date	Authors	Notes
1.0	2018/05/22	Emilien Kia	First version

Table of contents

1 Introduction

The present document summarizes procedures to modify level of privilege used to run Eaton Intelligent Power Manager on Microsoft Windows operating systems.

By default, as many other services, IPM is installed as local administrator (*LOCAL\Administrators* account, LOCAL has to be replaced by the name of the machine). This user is the owner of the directory where IPM is installed and of all of its files.

Please note that, for confidentiality reasons, some files, including the database, are protected from users access. Their permissions explicitly prevent LOCAL\Users to have any access, read-access included.

By default, the two IPM services (Eaton Intelligent Power Manager & Eaton EMC4J) are started as local system (LOCAL\SYSTEM). This level of privilege is quite high and make IPM able to access to many privilege files and execute actions like scripts with many high level privilege.

The present document aims to describe how an end-user can tune privileges used to run Eaton Intelligent Power Manager.

For more advanced Windows configuration, please refer to your IT department.

This document assumes Eaton Intelligent Power Manager is correctly installed and running.

This document assumes all licenses conditions are met and approved for all software.

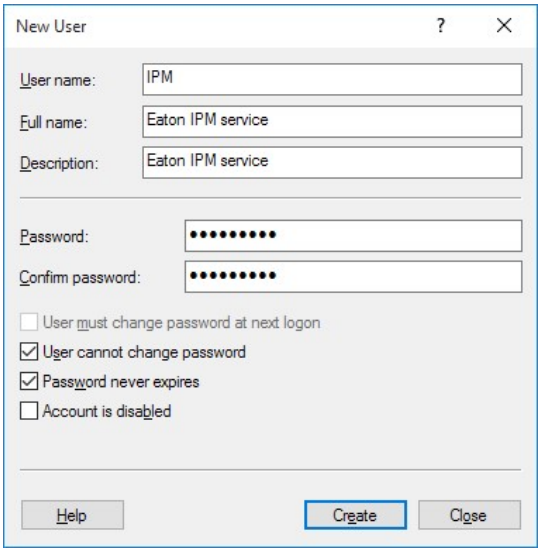
2 Make IPM running with a specific user

The easiest, and only described, method to run Eaton Intelligent Power Manager with lower privileges is to make it running with a specific user account. This account can be tune as the end-user want. This section will present how to create such account with low privileges.

2.1 Creating a new user

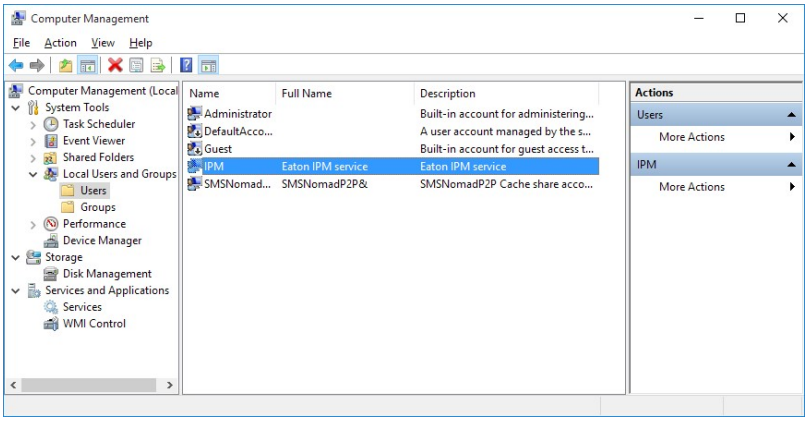
This section explains how to create a new local user. This user will be used to run Eaton Intelligent Power Manager.

1. In the “Computer Management” center, go to the “Local Users and Groups/Users” section and create a new user.
2. Set the new user’s properties like a comprehensive name, full name and description. Set it a strong password and set options as follow:



As it is not a human user, no need to change the password at next logon, it cannot change the password, and the password should not expires.

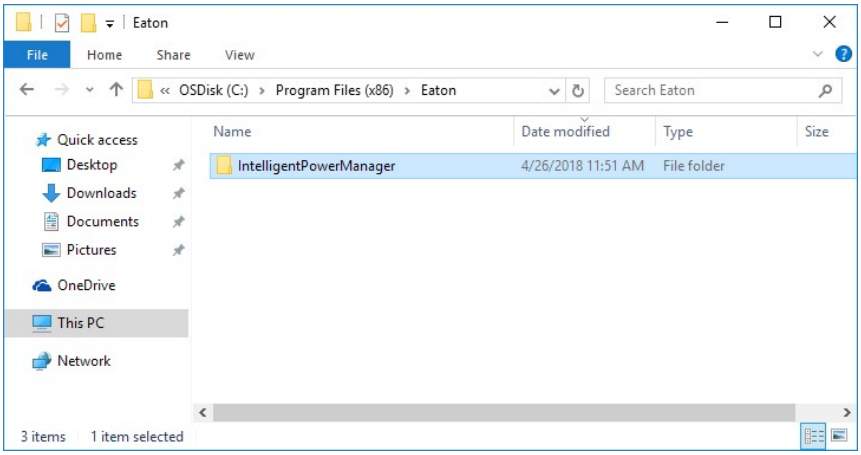
3. Once created, the new user should be visible in the list of users:



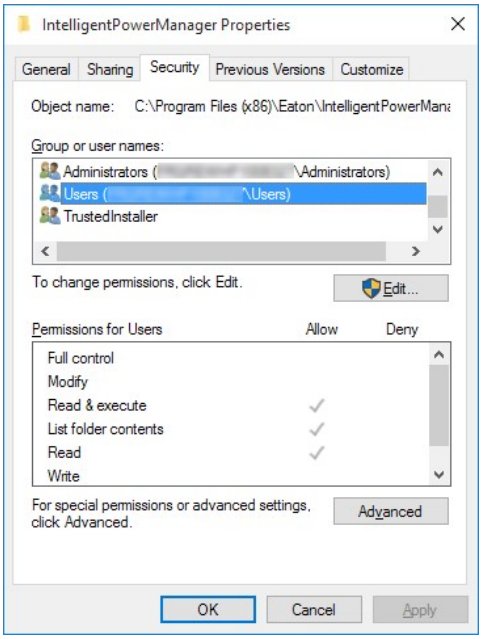
2.2 Adding user permissions to IPM files

This section describes how to add permission rules to IPM files and directories for a user.

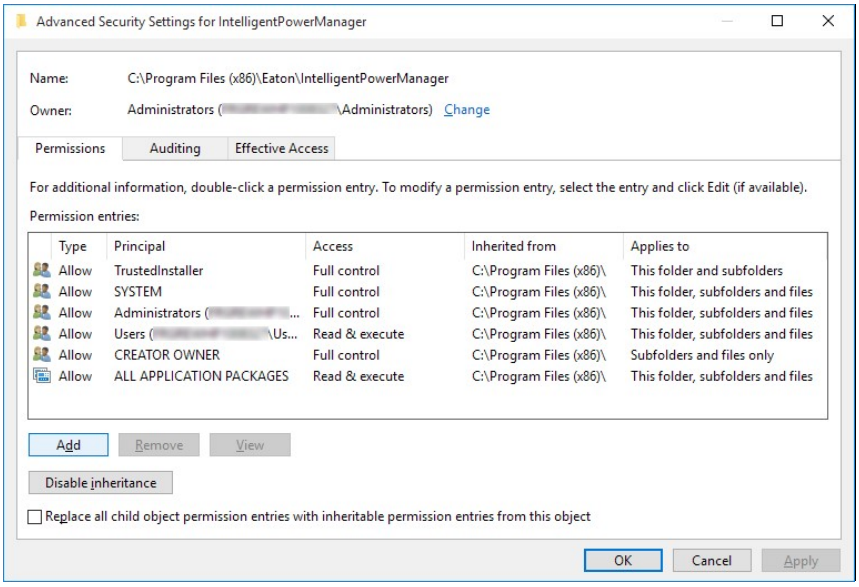
1. With the file explorer, go to the directory where IPM is installed, typically in "C:\Program Files(x86)\Eaton\IntelligentPowerManager".



2. Open the folder properties dialog box by right-click on it and select “Properties” on the context menu, and go to the “Security” tab. You can see local administrators and users have some rights on it.

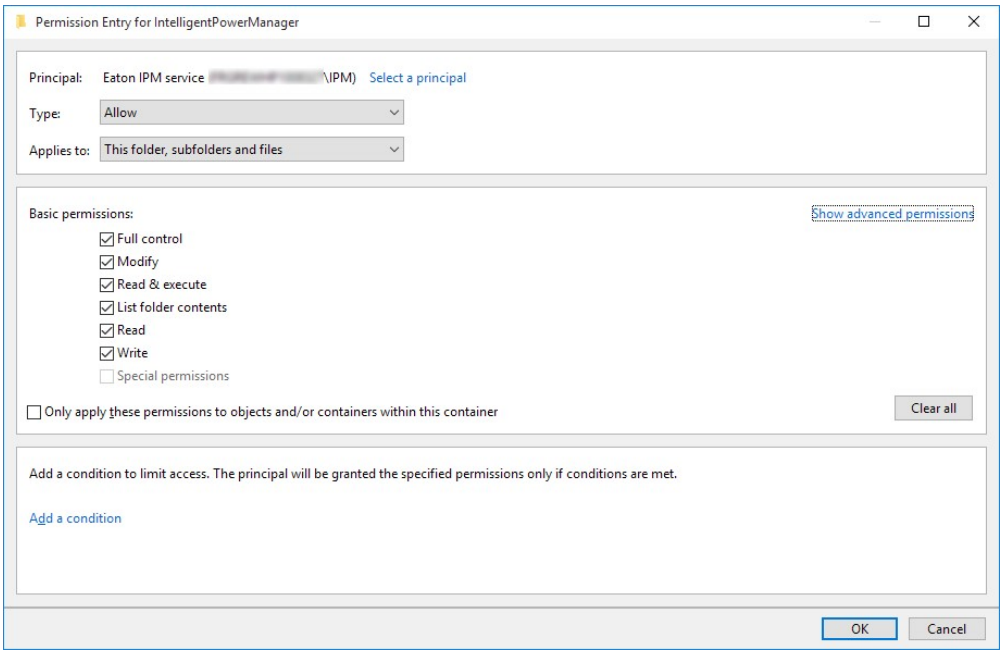


3. Open the “Advanced Security Settings” dialog box by clicking on the “Advanced” button. You can see a detailed list of access rights to the directory and its owner.



4. We will add permissions for a user by clicking on the “Add” button. The following dialog box appears. You can select the new user by clicking on the “Select a principal” link. This user should be the one created by the previous section.
   Choose:

- the type of permission “Type” (“Allow” is required)
- the level of application “Applies to” (“This folder, subfolders and files” is required)
- and the details of permissions “Basic permissions” (“Full control”, implying “Modify”, “Read & execute”, “List folder contents”, “Read” and “Write”)

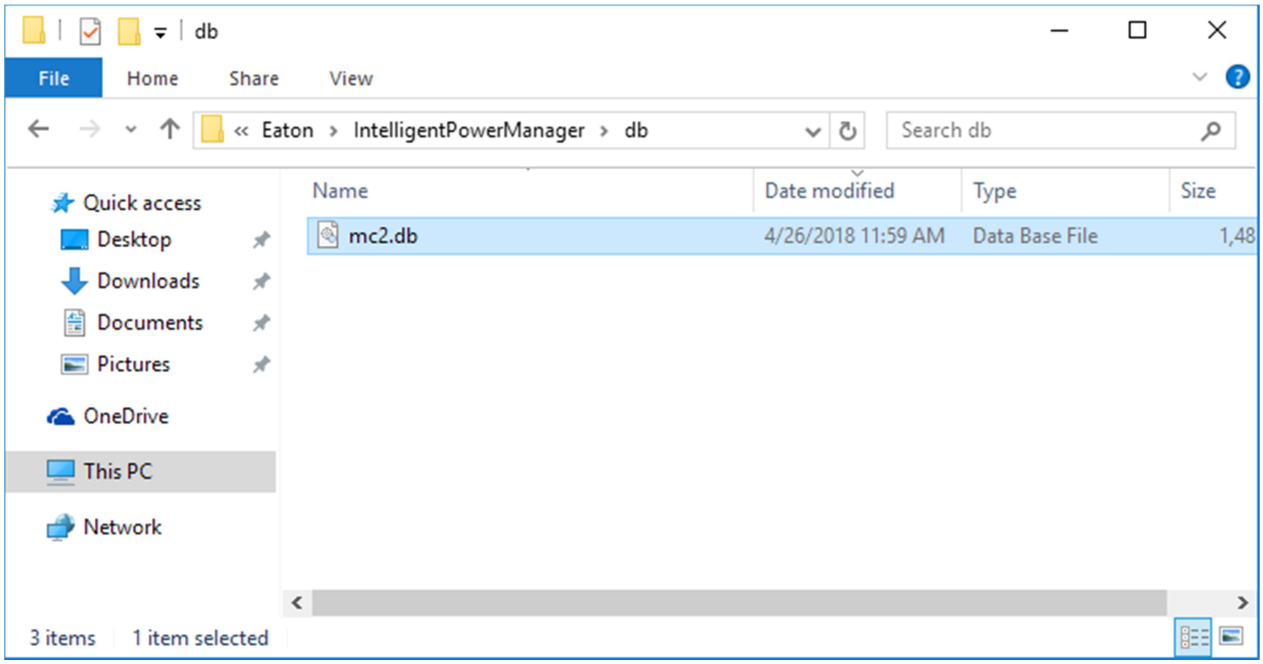


5. Then apply these permissions by pressing “Ok”.

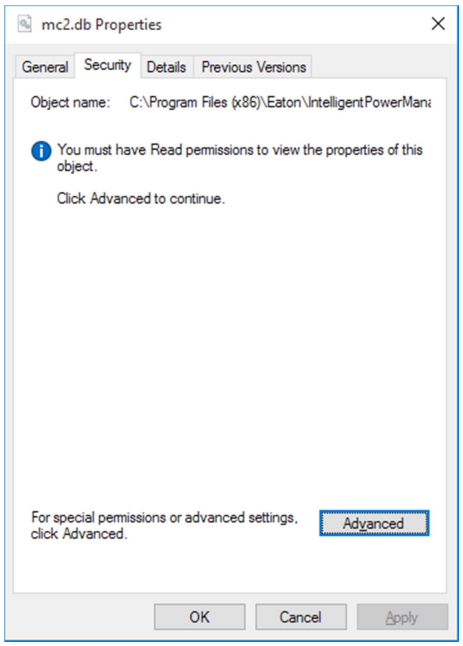
2.3 Remove user restrictions

By default, the IPM database is created with an explicit Access Control List (ACL) rule to prevent simple users (members of LOCAL/Users group) to read this file. This section will describe how to allow a user to be able to access to this file.

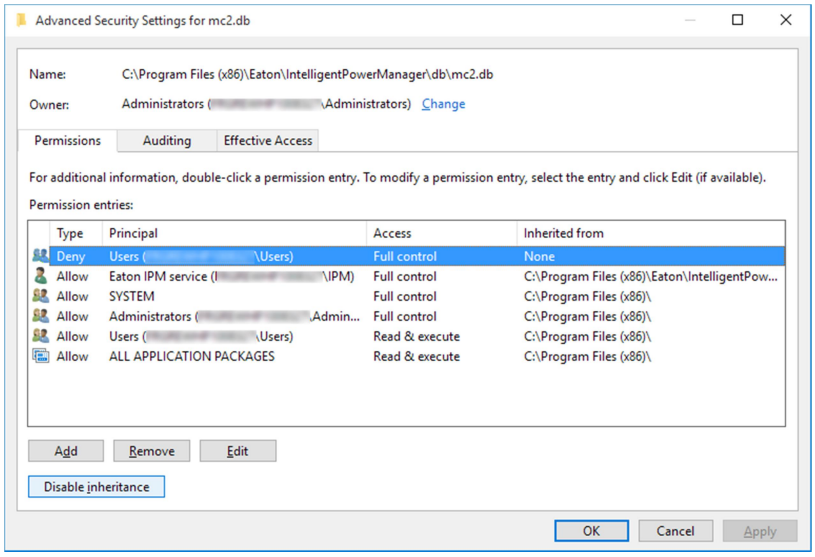
1. With the file explorer, go to the file location, typically “C:\Program Files (x86)\Eaton\IntelligentPowerManager\db”.



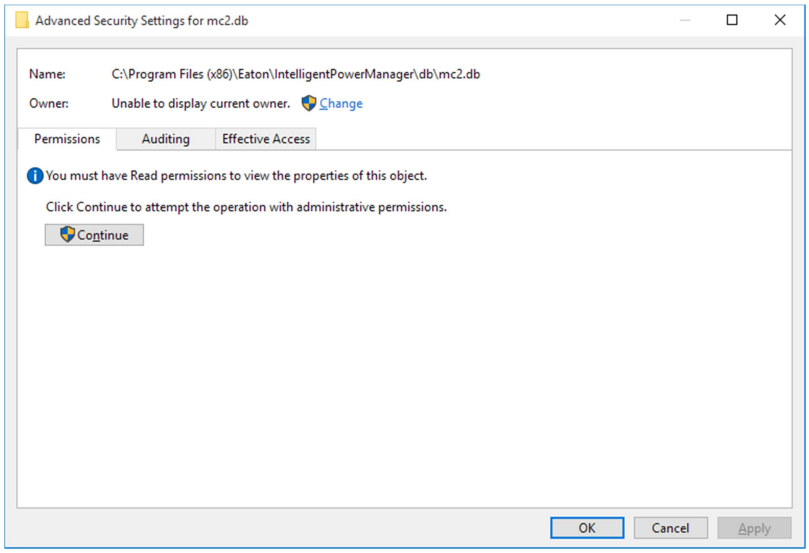
2. Open the “Property” dialog box for the file db/mc2.db then go to the “Security” tab.



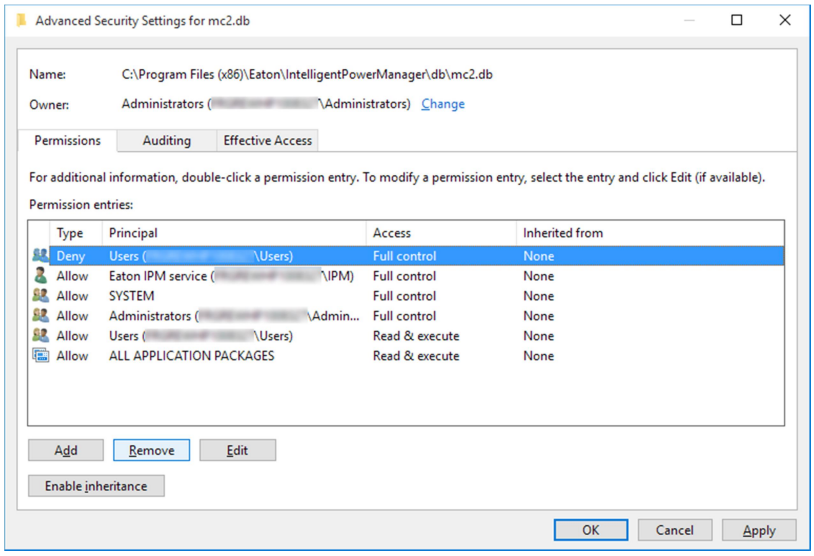
3. Open the “Advanced Security Settings” dialog box by clicking on “Advanced” button.



4. If the permission entry list is not displayed and a message “You must have Read permissions to view the properties of the object.” Is displayed instead, click on the “Continue” security button.



5. You have to manually and explicitly disable the permission inheritance by clicking on the “Disable inheritance” button. All the permission entries should not inherit anymore from anything, like below:

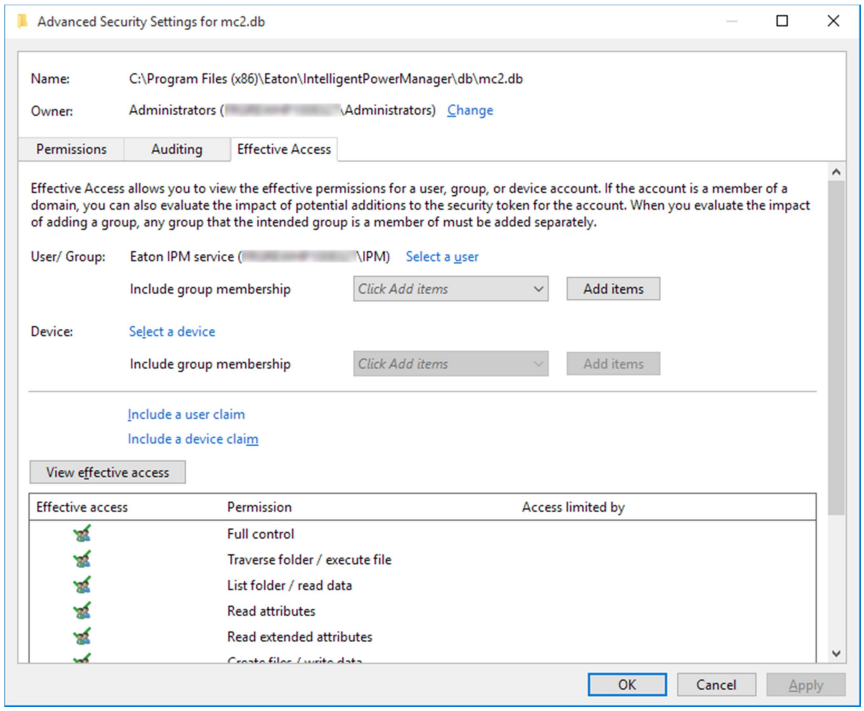


6. Remove the “Deny ”entry associated to the principal “Users” by selecting it and clicking on the “Remove” button. It shall not appear in the list anymore.

2.4 Test effective access permissions

In order to verify the permission configuration, this section test the permissions effective for a given user. Typically you should verify if a user account, and especially the user account created in 2.1, will effectively have permissions to access to files like the database.

1. Open the the “Property” dialog box for the tested file (db/mc2.db for example) then switch to its “Security” tab.
2. Open the “Advanced Security Settings” dialog box by clicking on “Advanced” button.
3. Enable reading permissions by clicking on “Continue” security button, if needed.
4. Switch to the “Effective Access” tab.
5. Choose a user (or a group) to test permissions by clicking on the “Select a user” link and selecting a user (or a group) in the dedicated dialog box.
6. Display effective access details by clicking on “View Effective access” button. Effective access shall have all green marks to be fully accessible and shall have all red marks to be fully inaccessible.

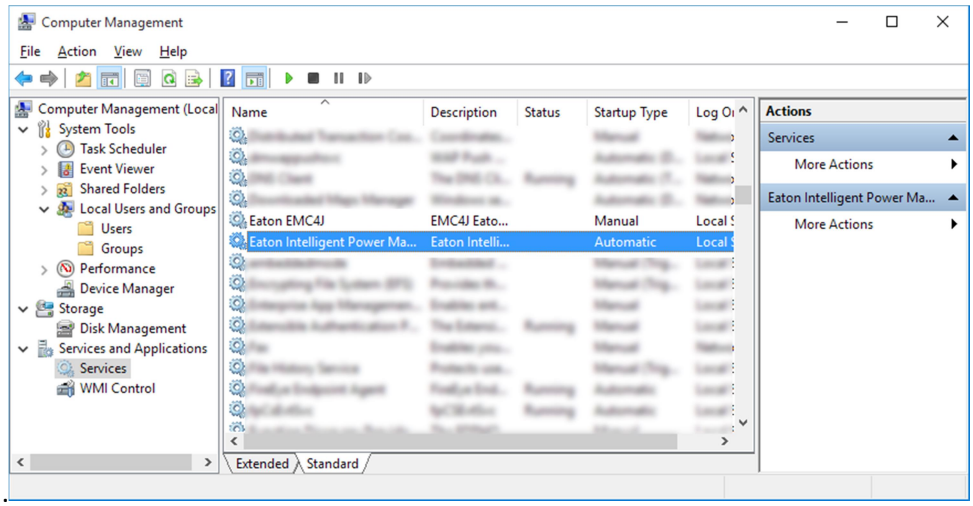


The db\mc2.db shall be completely accessible to the user running IPM and shall not be accessible to simple users.

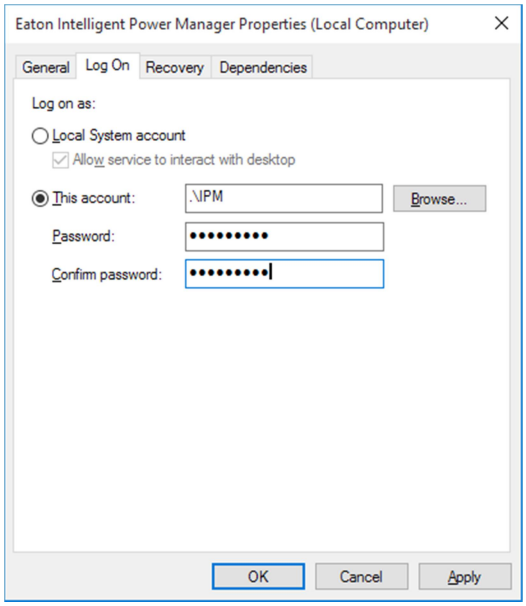
2.5 Set user running IPM services

This section present how to modify the user running IPM services.

1. Open “Computer Management” application and select “Services” section. Two Eaton services shall be available: “Eaton Intelligent Power Manager” and “Eaton EMC4J”. The procedure shall be applied with the same properties to both.



2. Select and edit one the two services. Switch to the “Log On” tab.
3. Select “Log on as:” to the option “This account:” and specify the user account to use. You can select it by browsing accounts with the button “Browse…”. Enter and confirm the password defined for this account in fields “Password:” and “Confirm password:”.

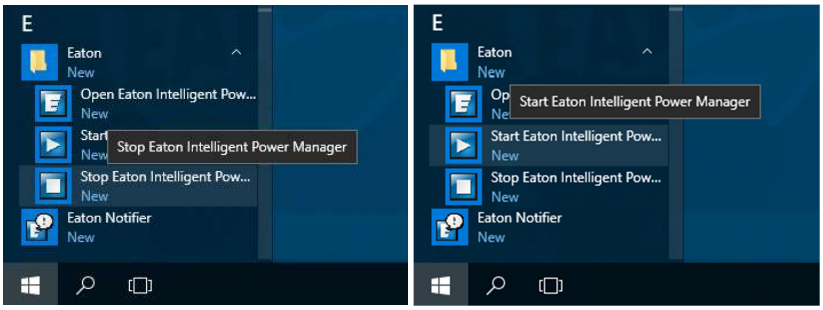


4. Apply the new configuration and close the dialog box.
5. Repeat the same operation with the other service with same account and password.

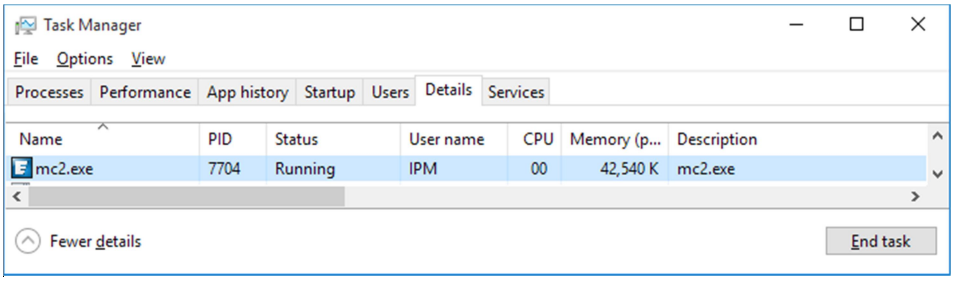
2.6 Restart IPM services

In order to apply the new service user configuration, you have to restart Eaton Intelligent Power Manager.

1. Stop the IPM service
2. Wait until it will be completely stopped
3. Start it



You can verify the user running IPM service in the Microsoft Windows “Task Manager”, in the “Details” tab. A process called “mc2.exe” shall be running and shall have the configured user name in the dedicated column.



Note that, some other “mc2.exe” process could be running, one per user session. They correspond to IPM Notifications application (systray icon and panel). Their user names should correspond to Windows desktop (human) users.

2.7 Using IPM

Once reconfigured, IPM can be used normally as described in the user manual.