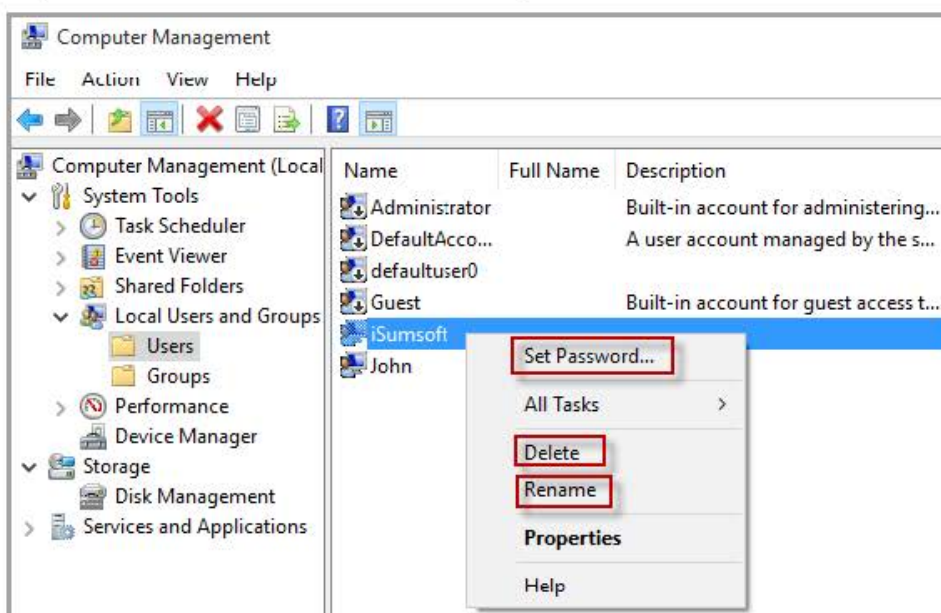


## 17. Създаване на потребители и групи

Третият начин за управление на локалните акаунти е от **Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups -> Users**. От меню „Action“ се избира „New User“ и от новопоявилния се прозорец се въвеждат данните на потребителя, като се избира, дали той да променя самостоятелно паролата си при първоначално вписване в системата, или да не му се дава такава възможност, включително и валидността на паролата да не изтича никога.



След натискане на бутона „Create“ акаунтът се създава и се появява в списъка „Users“. От свойствата му (зареждат се от десен бутон -> Properties или с двойно щракване върху името му) могат да се променят основни настройки (таб „General“ - настройки по името, описанието, валидността на паролата, дали акаунтът да се забрани или не); групите, в които членува (таб „Member Of“), и допълнителни настройки на профила, като скрипт за зареждане при вписване в ОС и местоположение на личната директория (таб „Profile“).

**Потребителският профил (user profile)** е съвкупност от данни, които съхраняват текуща среда на работа, настройки на приложенията и лични данни. Също така всички мрежови връзки, които биват установени, когато се работи на компютъра. Скриптът за влизане е файл, който може да бъде създаден и зададен на потребителски акаунт с цел конфигуриране на работната среда на потребителя. Например може да се използва скрипт за влизане, за установяване на мрежови връзки или за

стартиране на приложения. Всеки път, когато потребителят влиза в системата, зададеният скрипт се изпълнява.

**Потребителските групи** представляват колекция от множество потребителски акаунти, управлявани от общ набор от привилегии и настройки за защита. Основната цел при създаването на потребителски групи в Windows е да се опрости процесът по управление на множество потребители в голяма и сложна компютърна среда. Членовете получават позволенията, дадени на групата, и могат да членуват в множество групи.

Основните типове акаунти (потребителски групи) са:

- **Администратори** - членовете на групата Administrators. Съществува вграден и деактивиран по подразбиране администраторски акаунт Administrator.
- **Стандартни потребители** - членове на Users. Всеки нов акаунт става член на тази група по подразбиране, освен ако при създаването му не се причисли към друга.
- **Гости** - членове на групата Guests. Съществува вграден и деактивиран по подразбиране акаунт Guest. Потребителите от тази група имат повече ограничения от стандартните потребители, например не могат да създават парола.

За да се добави нова група с асоциирани потребители към нея, е необходимо да се избере от **Control Panel -> Administrative Tools -> Computer Management -> Local Users and Groups -> Groups** меню **Action -> New Group**.





Друг инструмент за управление на потребителските акаунти е „Управление на потребителските акаунти“ (User Account Control - UAC), който е въведен в Windows Vista. Предимството му е, че предупреждава потребителите при възникване на опасност от инсталиране на зловреден софтуер, който може да прави системни промени без разрешение.

Акаунтът Administrator не е подчинен на UAC. По подразбиране нивото на сигурност е 2 - Notify me only when apps try to make changes to my computer, при което се извеждат съобщения, подтикващи потребителите да вземат решения за даване или отнемане на права на приложенията при извършване на промени в компютъра. Ниво 0 не е препоръчително, тъй като при него сигурността е много ниска и приложенията могат да правят промени без разрешение на потребителите.

Друга специфика по управлението на потребителски акаунти е включването на известия при извършване на определени действия (UAC Prompt) като:

- ✓ инсталиране и деинсталиране на програми;
- ✓ инсталиране на драйвери, които не са получени чрез Windows;
- ✓ промяна на настройките на Windows Firewall;
- ✓ променяне на UAC настройките;
- ✓ конфигуриране на Windows Update;
- ✓ добавяне/премахване на потребителски акаунти;
- ✓ промяна на типа на акаунт;
- ✓ конфигуриране на родителски контрол;
- ✓ извикване на Task Scheduler;
- ✓ възстановяване на системни файлове от архивно копие;
- ✓ промяна на папките на други потребители и др.

Управлението на потребителските акаунти е свързано с т.нар. „UAC щитове“, които са обобщени в таблицата:

Икона	Тип	Описание
	Административно приложение, част от Windows	Приложението има валиден цифров подпис, който удостоверява, че Microsoft е негов издател. Работата с приложението е безопасна
	Приложение, което не е част от Windows, изискващо разрешение за стартиране	Тази програма има валиден цифров подпис, чрез който се гарантира самоличността на издателя на програмата
	Приложение от непознат производител	Тази програма няма валиден цифров подпис от нейния издател. Това не е непременно знак за опасност, тъй като много от старите легитимни програми нямат подписи. Въпреки това приложението трябва да се използва с повишено внимание. Може да се позволи изпълнението му, ако е инсталирано от надежден източник
	Приложение от блокиран производител	Тази програма е блокирана, защото е известно, че е ненадеждна

Необходимо е да се уточни, че ако потребителят не е сигурен за надеждността на стартираното от него приложение, трябва да провери името на програмата в интернет, за да се увери, че не е злонамерен софтуер.

### **Управление на права за достъп**

NTFS правата за достъп (NTFS permissions) задават сигурност на достъпа (локален или отдалечен) за потребител или потребителска група до даден файл или директория на устройства, формирани във файловата система NTFS.

При създаване на нова директория, тя наследява разрешенията от родителската. Когато се създава файл, той наследява разрешенията, зададени за основната папка. Всеки файл има собственик, разполагащ с всички права за достъп до него. По подразбиране това е неговият създател.

За да се контролират правата за достъп на потребители или потребителски групи, трябва да се избере от контекстното меню на файла/папката Properties -> таб „Security“.

От свойствата на файла или папката могат да се задават допълнителни права за одит: контекстно меню на файл или папка -> Properties -> таб „Security“ -> бутон „Advanced“ -> таб „Auditing“ -> бутон „Continue“. За активиране на опцията се изискват администраторски права. Одитът на файлове или папки позволява да се тестват наложените политики за сигурност и да се определи дали неупълномощени потребители се опитват да използват ресурса.

За да се приложи опцията коректно, първо е необходимо да се активират съответните политики за одит от **Control Panel -> Administrative Tools -> Local Security Policy -> Local Policies -> Audit Policy**.

Активирането на всички опции не е задължително и дори препоръчително, поради няколко причини:

- В процеса на одит се създават логфайлове. Всяко вписване в дневника заема малко количество от свободното дисково пространство. Ако се появят твърде много одитирани събития (понякога стотици в минута), може да се изчерпи свободното дисково пространство.
- При всеки одит се заемат системни ресурси, което може да се отрази негативно на производителността на ОС.

- От свойствата на всеки един от видовете одит може да се избере дали да се записват успешните или неуспешните изпълнения на съответните действия.