

16. Създаване на потребители и групи

Процесът по създаване на потребителски акаунти трябва да се планира и организира внимателно, като за тази цел е необходимо да се спазят **две основни правила**. На първо място, да се спазват **конвенции за именуване (*naming convention*)** - полезна практика и задължителна в случаите, при които потребителите са много и структурата на организацията е сложна. Тя представлява единен стандарт за идентификация на потребителите. Спазването на единна конвенция за именуване помага на администраторите и потребителите да запомнят имената за влизане, а също така улеснява намирането на определени потребителски акаунти при добавянето им към групи. На второ място, да се зададат **изисквания за паролите**, за да се защити достъпът до компютърната система. Всеки потребителски акаунт трябва да има парола, препоръчително е тя да отговаря на някои правила:

- Винаги трябва да се задава парола на акаунт от групата Administrators, за да се възпрепятства неоторизиран достъп до системата.

- Трябва да се определи дали паролите ще се контролират от администратор или от потребителите. Могат да се зададат уникални пароли на потребителите, като им бъде забранено да ги променят, или обратно - да се даде възможност на потребителите сами да въвеждат собствени пароли при първото им влизане в системата. В повечето случаи е добре потребителите да имат възможност да контролират своите пароли. Една от полезните възможности е тази, чрез която потребителите са задължени да сменят паролите си през определен интервал от време. Като част от защитата на акаунтите може да се използва т.нар. „диск за пароли“ (Password Reset Disk): за използването му е необходимо потребителят да разполага с USB устройство, на което да се запази криптирания файл с паролата.

- Трябва да се използват пароли, които трудно могат да бъдат компрометирани: с очевидни асоциации като име на член от семейството, рождена дата, ЕГН и т.н.

- Могат да съдържат до 128 знака. Препоръчва се минимална дължина от 8 знака.

- Добре е да отговарят на изискванията за сложност, които включват използване на главни и малки букви, цифри и валидни знаци (прави се разлика между малка и главна буква).

Създаване и управление на потребителски акаунти и групи

В Windows 10 могат да се създават два типа акаунти - **Microsoft акаунти** и **локални акаунти**. За първия вид се изисква валиден Microsoft имейл. Позволява се синхронизация с определени услуги на Microsoft между различни устройства. Тези акаунти имат достъп до файлове, които се намират онлайн, независимо от устройството, на което се използват. Локален акаунт може да се конвертира в Microsoft акаунт по всяко време. Обратният процес също е възможен.



Създаването им става от **Settings -> Accounts -> Family & Other Users -> Add someone else to this PC**. Първо се въвежда потребителското име. От следващия екран - паролата, а след това - имена, държава и дата на раждане.

Създаденият акаунт може да се добави към групата на стандартните потребители или администраторите.

За разлика от Microsoft акаунтите локалните акаунти се създават и управляват само на текущата компютърна система. Информацията за тях се съхранява в регистъра на ОС (управляващ ключ **HKEY_USERS**). Всеки локален акаунт има **уникален идентификатор (Security Identifier, SID)**. Дори акаунтът да бъде изтрил, неговият SID продължава да се съхранява и не може

да бъде създаден нов акаунт с този SID. Локалните акаунти имат конкретни права за достъп до системата и файловете, зависещи и от групата, в която е добавен съответният акаунт. При логването му се създава **секретен маркер (security access token)**, който включва потребителско име, SID и групи, в които членува даденият потребител. Всяка стартирана програма получава достъп до този маркер. При всеки достъп на потребител до обект (ресурс) на ОС от секретния маркер се извлича SID на потребителя и се прави проверка дали има отказ или позволение за достъп. Към всеки обект (ресурс) е **асоцииран списък за контрол на достъпа (ACL - Access Control List)**, в който са описани потребителите/групите чрез техния SID и какви са правата им върху дадения обект. Администраторските акаунти при логване получават два маркера - един със стандартни и един с администраторски привилегии.

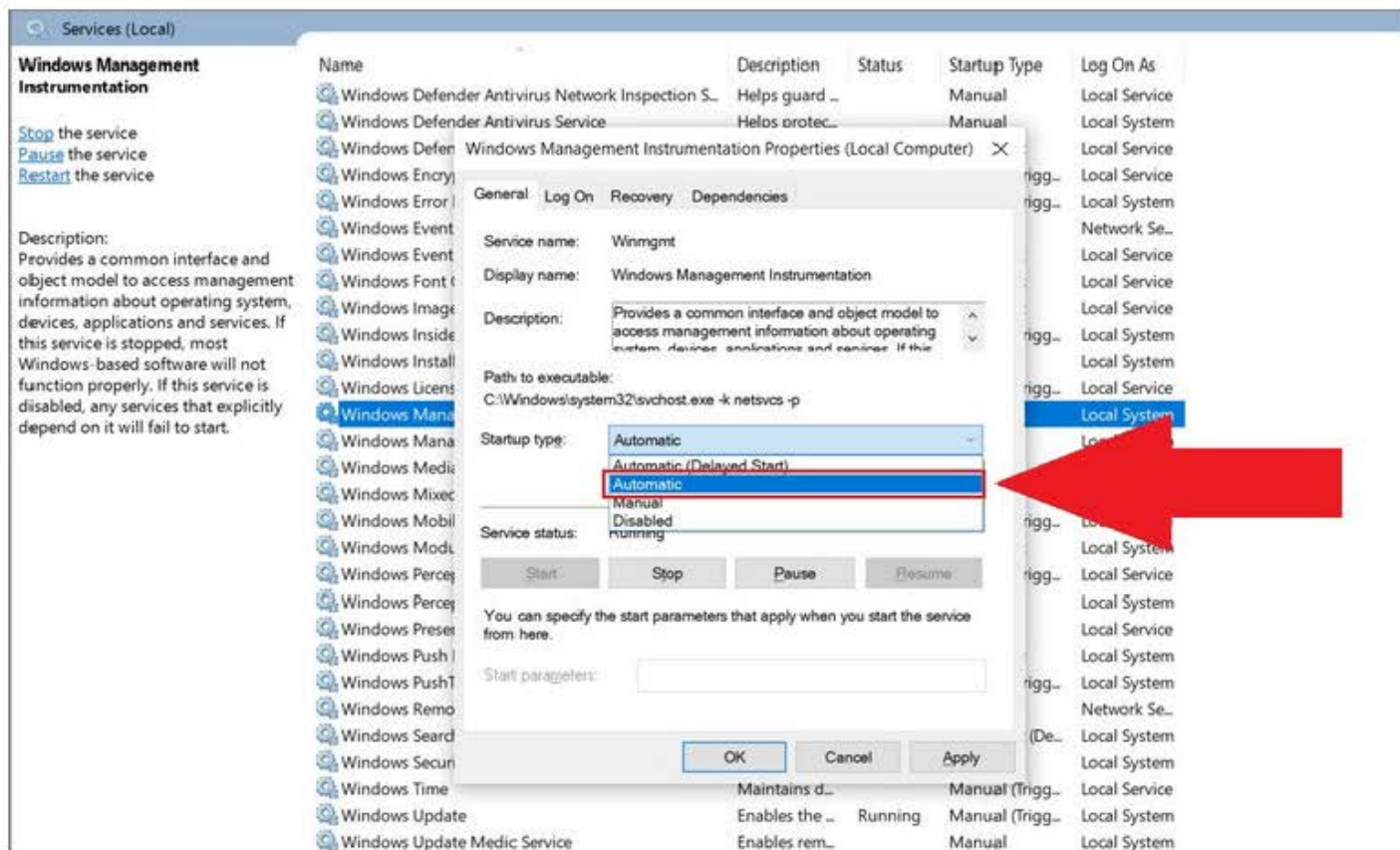
Подробности за акаунтите в команден ред могат да се получат чрез командите „**WhoAmI /user**“ и „**wmic useraccount get name,sid**“. Чрез първата се извеждат данни само за текущо вписания акаунт, а чрез втората - за всички съществуващи на ОС. Командите се изписват в **Command Prompt (CMD)**, стартиран с административни права (в търсачката на Windows се изписва CMD, след което върху иконата на командния интерпретатор се кликва с десен бутон и се избира „Run as administrator“).

В случай че се изведе грешка като „wmic is not recognized as an internal or external command, operable program or batch file“, от **Control Panel -> System -> Advanced system settings -> Environment variables** трябва да се редактира системната променлива Path, като се добави стойност **C:\Windows\System32\wbem**. Системната променлива Path задава списък от директории, които командният интерпретатор преглежда за изпълнението на команди.

От Services трябва да се провери дали е стартирана услугата **Windows Management Instrumentation**.

Стартира се отново **Command Prompt (CMD)** като администратори и се въвежда командата „wmic“, описана по-горе.

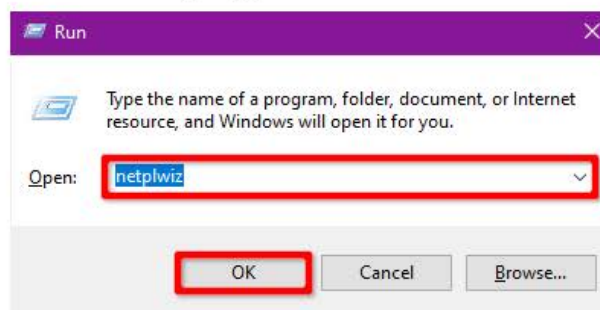
По-детайлна информация за групите, в които членуват акаунтите, може да се получи чрез командата „**gpresult/r**“. Тя работи при версии Pro и Enterprise на Windows 10. Потребителите на версия Home могат да използват **net user „User Name“**, за да изведат информация за акаунта и групите, към които принадлежи.



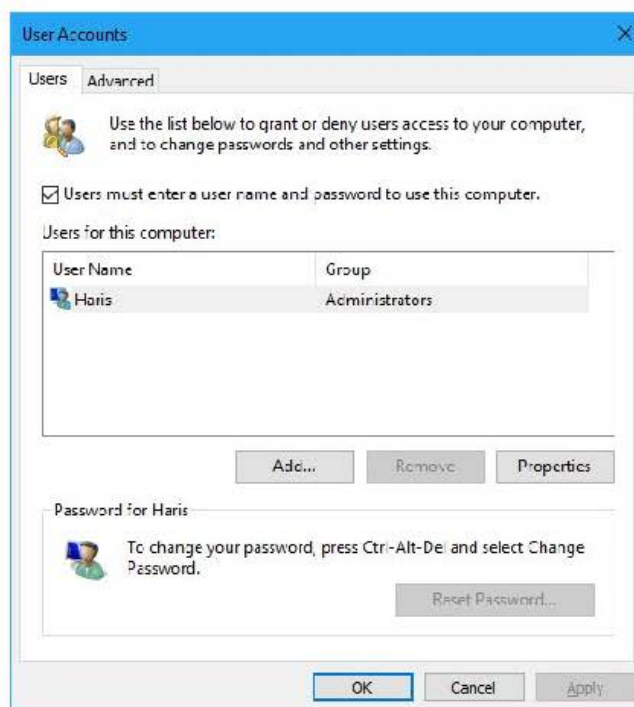
Създаването на локални акаунти в Windows 10 става по три начина: от **Settings** -> **Accounts** -> **Family and other users**, чрез приложението NetplWiz и от **Control Panel** -> **Administrative Tools** -> **Computer Management** -> **Local Users and Groups**.

Създаването на локален и Microsoft акаунт се осъществява от едно и също място от **Settings** -> **Accounts** -> **Family and other users** -> **Add someone else to this PC**. За да се създаде локален акаунт, е необходимо да се избере опцията „Add a user without a Microsoft account“. След това се определят потребителско име и парола, а в последствие може да се промени и неговият тип - администратор или стандартен потребител. По подразбиране новите акаунти са от групата на стандартните потребители.

Приложението NetplWiz се използва за управление на локални акаунти. Стартира се от netplwiz.exe или се изписва командата на фигурата:



Съдържа два таба - Users и Advanced. От първия се управляват потребителите, а от втория са достъпни разширени опции. Редактиране или изтриване на съществуващи потребители става, след като се маркира желаният от тях. След натискане на бутон „Properties“ се зареждат свойствата на акаунта, от които могат да се променят потребителското име и групите, в които членува. От бутон „Remove“ се изтрива съществуващ акаунт, а от бутон „Reset Password“ може да се промени паролата му.



С бутон „Add“ се добавя нов акаунт - Microsoft или локален. За създаване на втория тип се натиска „Sign in without a Microsoft account“, после се избира бутон „Local account“ и се въвеждат данните му.