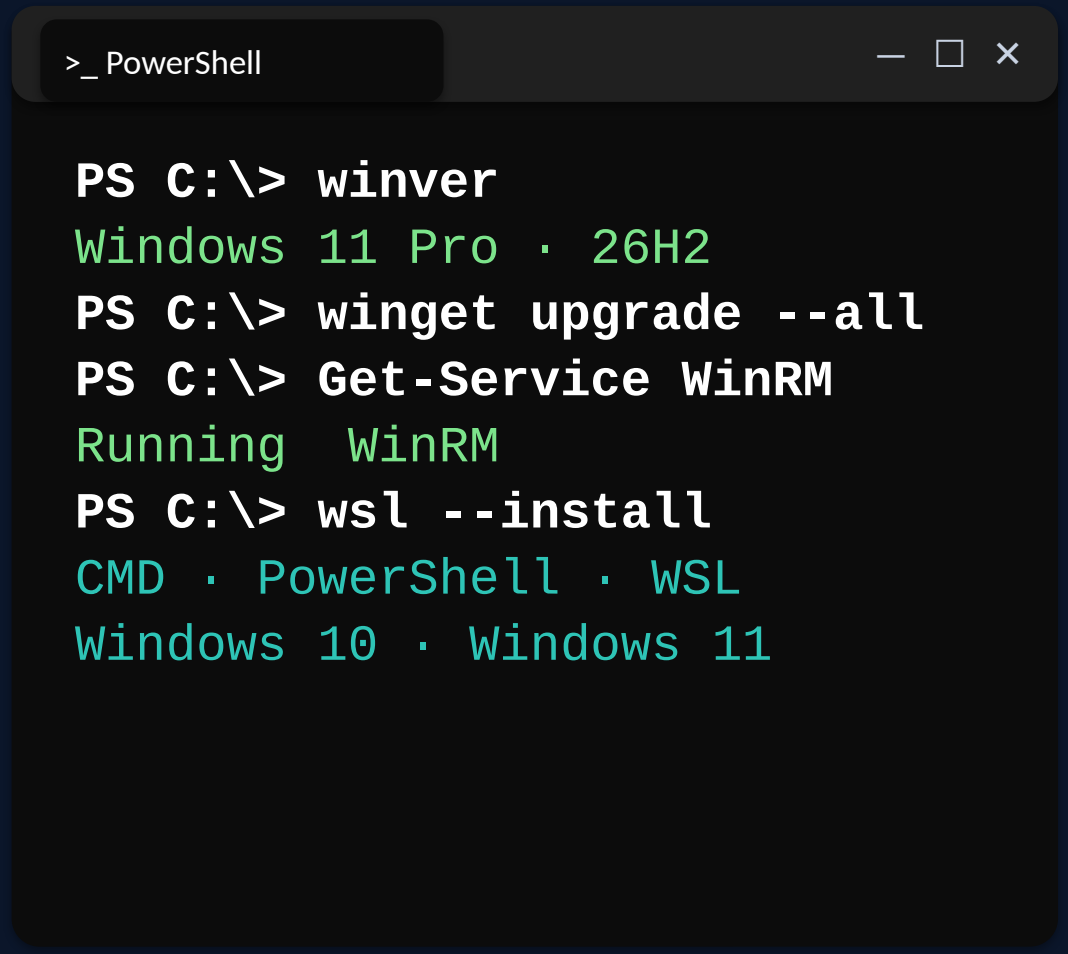


LESSON 8 OF 12

Windows 10 & 11

Desktop · Workstation · Laptop

Account Management: Users, Groups, UAC & Sign-in

Full Course · Windows 11 26H2 · Windows 10 22H2

What You Will Learn in Lesson 8

- Account types: Microsoft, local, work or school, domain
- Standard users vs administrators, and how UAC protects you
- Managing users with Settings, lusrmgr.msc, net user and PowerShell
- Built-in groups and what they allow
- Sign-in options: Windows Hello, PIN, passkeys and passwords
- User profiles, runas and password policies
- Best practices for families, schools and offices

Types of Accounts

Account	Signs in with	Typical use
Microsoft account	Email + Windows Hello / password	Home PCs; OneDrive, Store, BitLocker key backup
Local account	User name + password, this PC only	Labs, shared or offline PCs
Work or school	Microsoft Entra ID account	Organizations using Microsoft 365 and Intune
Domain account	Active Directory (DOMAIN\user)	Companies with on-premises servers
Built-in Administrator	Disabled by default	Recovery only — leave it disabled
Family (child) account	Microsoft Family Safety	Screen time and content limits for kids

Standard User vs Administrator

	Standard user	Administrator
Run apps, browse, documents	Yes	Yes
Install software for everyone	No (asks for admin credentials)	Yes, after a UAC prompt
Change system settings, drivers	No	Yes, after a UAC prompt
Manage other users	No	Yes
Risk if malware runs	Limited to the user's files	Can change the whole system

How UAC Protects You

- Admins run with a standard token until a task needs more
- Consent prompt (admins): 'Do you want to allow this app…?' — Yes/No
- Credential prompt (standard users): type an admin name and password
- Prompts appear on the Secure Desktop, which malware cannot click
- Check the publisher name before you click Yes
- Never turn UAC off: UserAccountControlSettings.exe

Users and Groups with CMD (net)

```
C:\> whoami /groups | findstr /i "Administrators"      # am I an admin?
C:\> net user                                          # list local users
C:\> net user student * /add                           # * = prompt for the password
C:\> net user student                                  # details, last logon, groups
C:\> net localgroup Administrators                     # who are the admins?
C:\> net localgroup "Remote Desktop Users" student /add
C:\> net user student /active:no                       # disable the account
C:\> net user student /delete
```

Users and Groups with PowerShell

```
PS C:\> Get-LocalUser | Select-Object Name, Enabled, LastLogon
PS C:\> $pw = Read-Host -AsSecureString 'Password'
PS C:\> New-LocalUser -Name student -Password $pw -FullName 'Lab Student'
PS C:\> Add-LocalGroupMember -Group Users -Member student
PS C:\> Get-LocalGroupMember -Group Administrators
PS C:\> Disable-LocalUser -Name student
PS C:\> Remove-LocalUser -Name student -WhatIf

# GUI: Settings > Accounts > Other users   |   lusrmgr.msc (Pro and higher)
```

Important Built-in Groups

Group	Members can
Administrators	Do anything on this computer
Users	Run apps and use their own files (standard users)
Remote Desktop Users	Sign in through Remote Desktop (Lesson 10)
Backup Operators	Back up and restore files, even without file permissions
Hyper-V Administrators	Manage virtual machines without being full admins
Event Log Readers / Performance Log Users	Read logs / collect performance data

Sign-in Options

Option	Notes
Windows Hello PIN	Tied to this device and its TPM — safer than a reused password
Face / fingerprint	Windows Hello biometrics on supported cameras and readers
Passkeys	Phishing-resistant sign-in to websites, stored by Windows Hello
Security key	A USB or NFC FIDO2 key
Password	Still needed for some cases; use long passphrases
Dynamic lock	Locks the PC when your paired phone walks away

Profiles, runas and Password Policy

```
PS C:\> Get-CimInstance Win32_UserProfile | Select-Object LocalPath, LastUseTime
# Delete old profiles: sysdm.cpl > Advanced > User Profiles > Settings

C:\> runas /user:%COMPUTERNAME%\admin2 "mmc compmgmt.msc"   # run as another user

C:\> net accounts                          # password and lockout policy
C:\> net accounts /minpwlen:12 /lockoutthreshold:10
C:\> secpol.msc                            # Local Security Policy (Pro and higher)
```

Best Practices

- Use a standard account every day; keep a separate admin account
- Every person gets their own account — never share one
- Long, unique passphrases plus Windows Hello; save recovery codes
- Remove or disable accounts that are no longer used
- Families: child accounts with Microsoft Family Safety
- Organizations: Windows LAPS rotates local admin passwords

Lab: Least Privilege in Action

```
PS C:\> $pw = Read-Host -AsSecureString
PS C:\> New-LocalUser labuser -Password $pw ; Add-LocalGroupMember Users labuser
# Sign out, sign in as labuser, then try:
#   - install an app for all users  -> UAC credential prompt
#   - open C:\Windows\System32 and create a file -> Access denied
C:\> whoami /groups
C:\> whoami /priv
# Back as admin: add labuser to 'Remote Desktop Users', then disable the account
PS C:\> Disable-LocalUser labuser
```

Summary & Homework

- Microsoft, local, work/school and domain accounts serve different needs
- Standard user daily + UAC = far less damage from mistakes and malware
- net user / net localgroup and *-LocalUser / *-LocalGroupMember cmdlets
- Windows Hello PIN and passkeys beat reused passwords
- Homework: audit your PC — list users and the Administrators group
- Homework: move your daily work to a standard account

Thank You! 🙏

Free videos & PDFs: www.MyWebUniversity.com

Slides for this lesson: MyWebUniversity.com/presentations

YouTube: @MyWebUniversity · @MyWebUniversity-Dari

Wahidullah Lutfy — Founder and Director of IT of MyWebUniversity, and CS teacher

Book: The Direct Path to Linux Ubuntu (Amazon · Barnes & Noble)

Learn it, then pass it on.