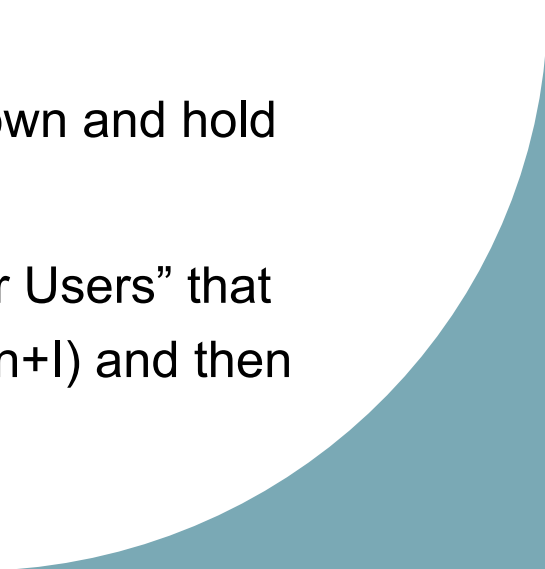


**Improving user
security and
Windows
performance**

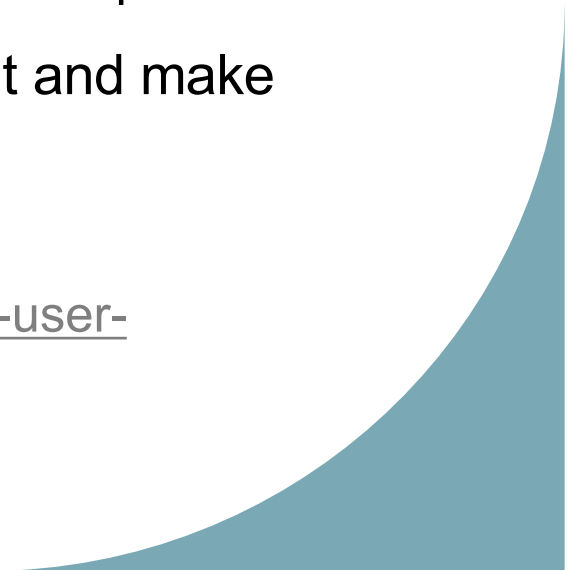


How to understand the notation used on the following slides

- When you see something like “Alt+F4” that means that you press the Alt key and the F4 key at the same time (i.e. press Alt, keep it down and press F4).
 - Similarly for 3 keys, e.g. Ctrl+Shift+Esc means press down and hold Ctrl, then press and hold Shift, then press Esc
 - When you see something like “Settings/Accounts/”Other Users” that means you launch Settings (from Start menu or with Win+I) and then choose “Accounts” and then choose “Other Users”
- 

Improving user security

- By default your Microsoft Windows user account has "Admin" privileges
 - This makes life very convenient for you, BUT
 - It also makes it easier for malware to install on your computer
- Better option is to create a separate Admin account and make your user account a normal user
 - How to do that (see the first option here <https://www.howtogeek.com/ways-to-create-a-local-user-account-on-windows-11/>)



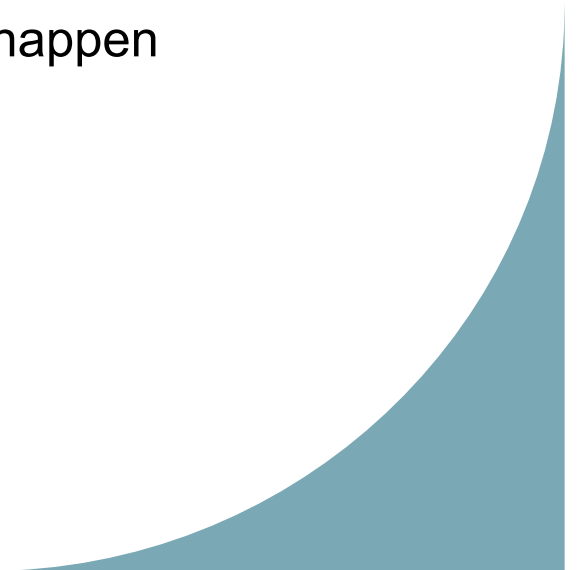
Improving user security (cont'd)

- After you have created the new Admin account, log out from your normal account and then make sure you can log in as your new Admin user by pressing Alt+F4 and choosing “Switch User” from the dropdown and clicking OK
- When you are logged in as the new Admin:
 1. go to **Settings/Accounts/”Other Users”**
 2. Click on your normal user
 3. Click on **“Change account type”**
 4. Choose **“Standard User”** from the dropdown
 5. Click OK



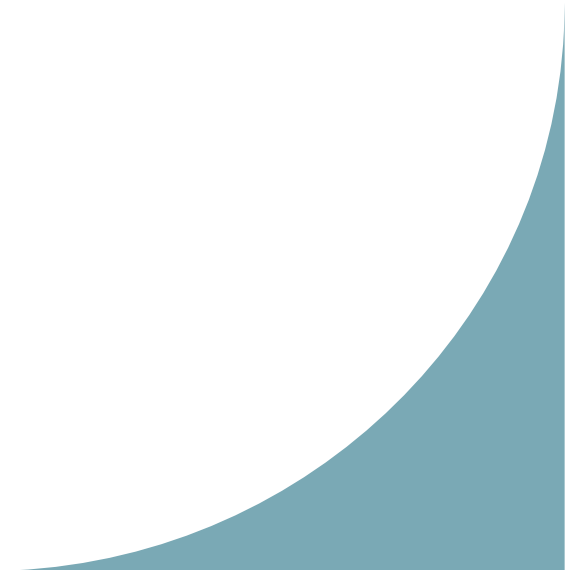
Improving user security (cont'd)

- You can now switch user back to your normal account (using Alt+F4) and carry on working.
- Now that your main account is not an admin account you will be prompted whenever an admin privilege is required and you have the option to say “no” if you were not expecting that to happen



Improving Windows Performance

- Using Task Manager to look at resource usage
- How to find out what applications are launching at startup and how to change that



Using Task Manager

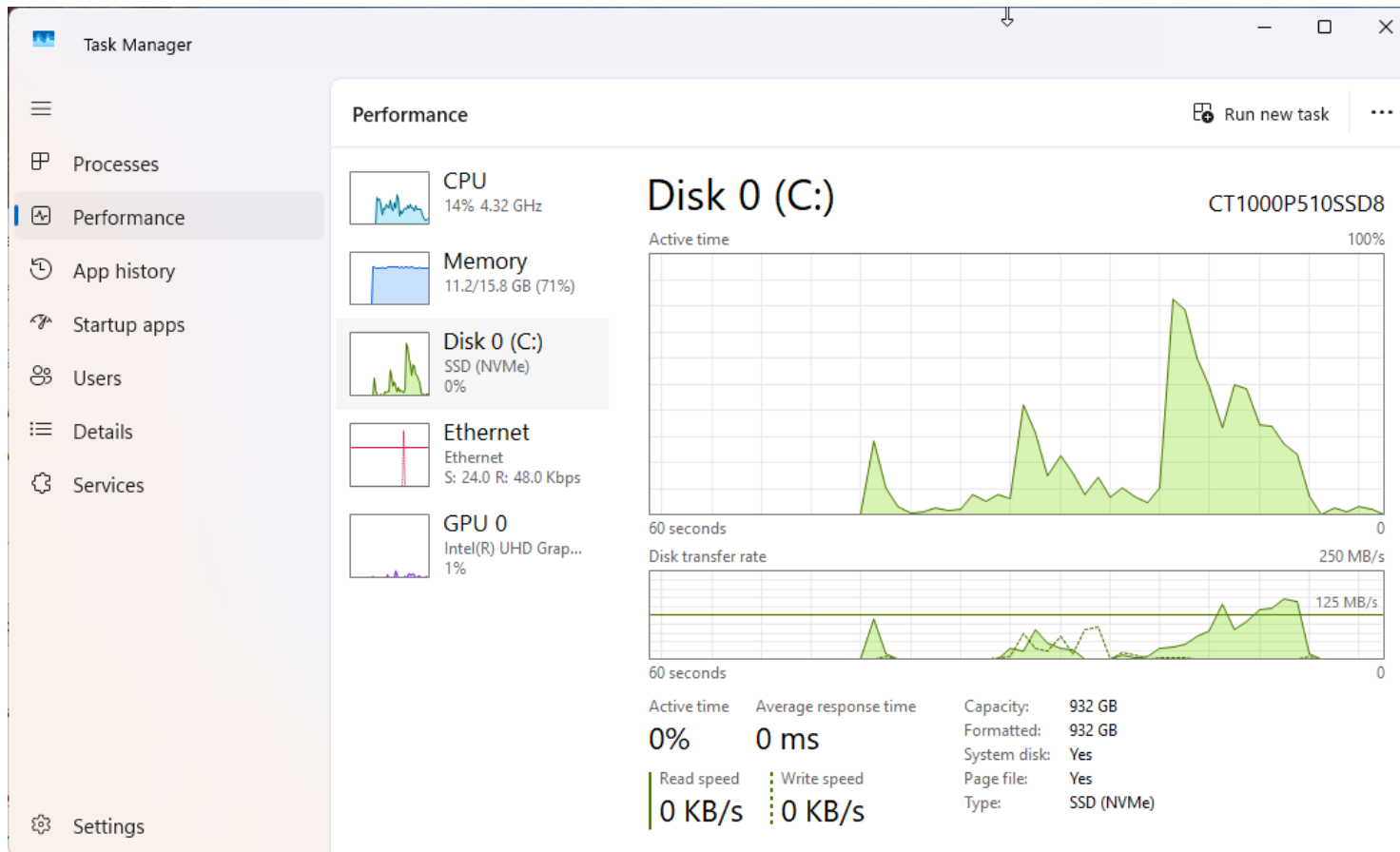
- To launch Task Manager:
 - Right click on the Taskbar and choose Task Manager, or
 - Right click on Start and choose Taks Manager, or
 - Press Ctrl+Shift+Esc



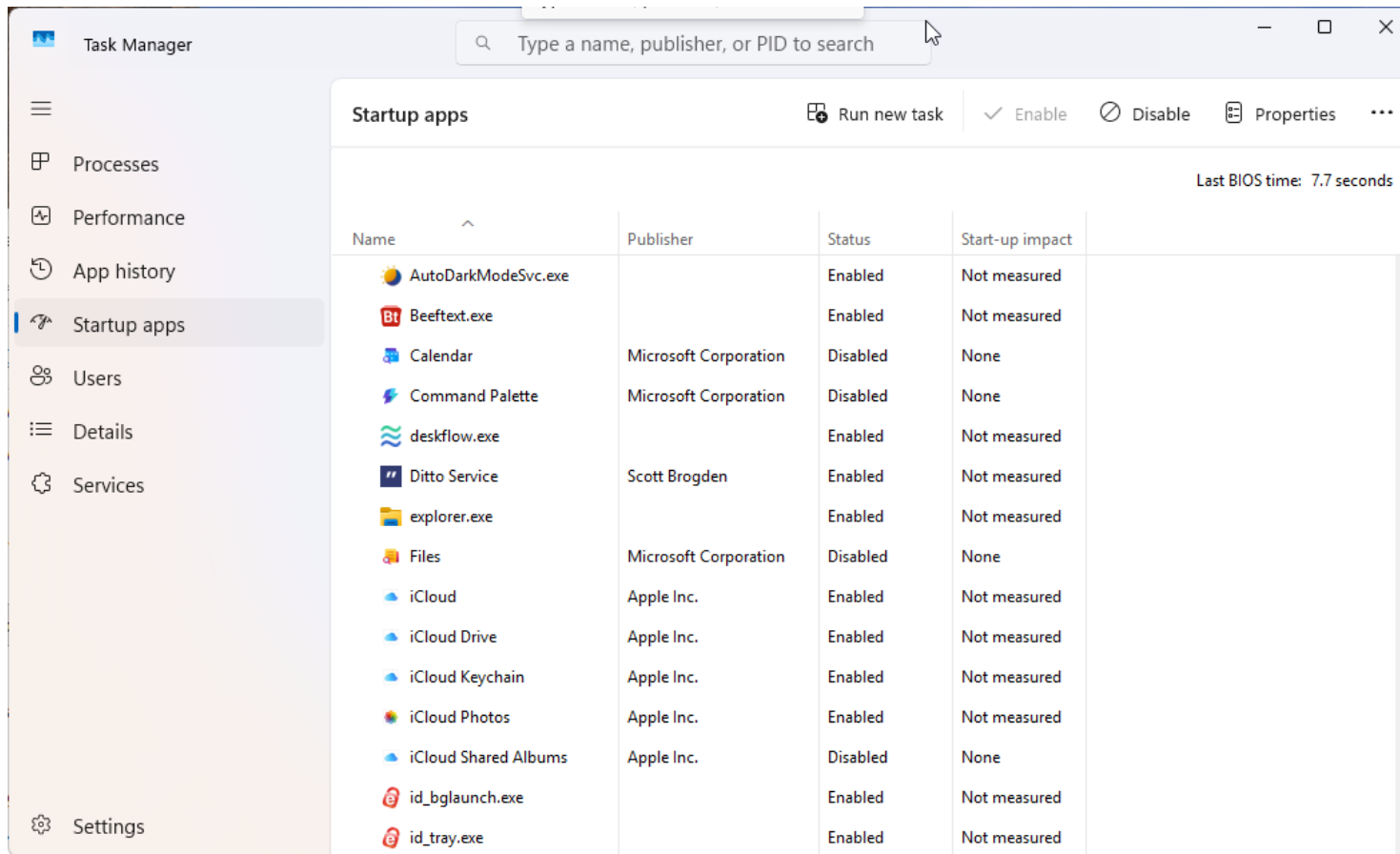
Using Task Manager (Processes)

Processes		10%	68%	0%	0%
		CPU	Memory	Disk	Network
>	Android Studio	0%	827.7 MB	0 MB/s	0 Mbps
>	Visual Studio Code (14)	3.3%	709.4 MB	0.1 MB/s	0 Mbps
	dart.exe	0%	377.4 MB	0 MB/s	0 Mbps
>	Microsoft 365 Copilot (10)	0.3%	350.6 MB	0 MB/s	0 Mbps
>	Microsoft Edge (15)	0%	329.0 MB	0 MB/s	0 Mbps
>	language_server_windows_x64...	0%	293.1 MB	0 MB/s	0 Mbps
>	Steam Client WebHelper (7)	0.3%	240.1 MB	0 MB/s	0 Mbps
>	Antimalware Service Executable	0.3%	232.7 MB	0 MB/s	0 Mbps
>	Windows Explorer (2)	0.3%	215.2 MB	0 MB/s	0 Mbps
>	Mailspring (7)	0.3%	193.0 MB	0 MB/s	0 Mbps
>	Microsoft Teams (12)	0%	142.8 MB	0 MB/s	0 Mbps
>	IDrive Service	0.3%	139.2 MB	0.1 MB/s	0 Mbps
	dartvm.exe	0%	96.4 MB	0 MB/s	0 Mbps
>	MSPCManager Service (Store) ...	0.3%	89.6 MB	0 MB/s	0 Mbps
>	SupportAssistAgent.exe	0%	87.5 MB	0 MB/s	0 Mbps
>	Task Manager	1.3%	82.6 MB	0 MB/s	0 Mbps

Using Task Manager (Performance)



Using Task Manager (Startup Apps)



The screenshot shows the Windows Task Manager application with the 'Startup apps' tab selected. The left sidebar contains navigation options: Processes, Performance, App history, Startup apps (selected), Users, Details, and Services. The main area displays a list of startup applications with columns for Name, Publisher, Status, and Start-up impact. A search bar at the top allows filtering by name, publisher, or PID. Action buttons for 'Run new task', 'Enable', 'Disable', and 'Properties' are visible. The 'Last BIOS time' is noted as 7.7 seconds.

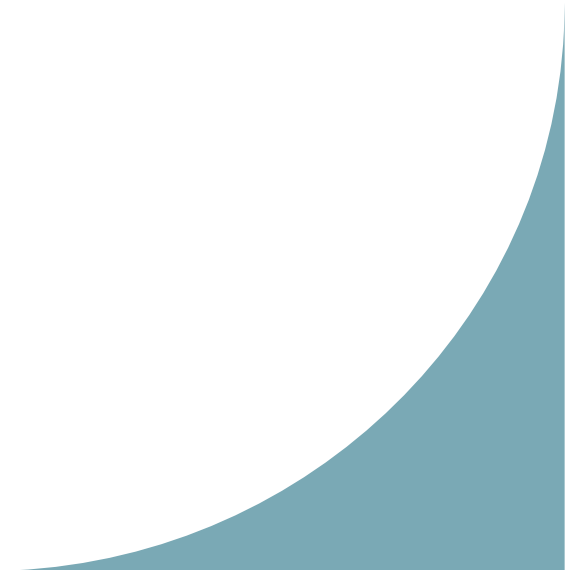
Name	Publisher	Status	Start-up impact
AutoDarkModeSvc.exe		Enabled	Not measured
Beef.txt.exe		Enabled	Not measured
Calendar	Microsoft Corporation	Disabled	None
Command Palette	Microsoft Corporation	Disabled	None
deskflow.exe		Enabled	Not measured
Ditto Service	Scott Brogden	Enabled	Not measured
explorer.exe		Enabled	Not measured
Files	Microsoft Corporation	Disabled	None
iCloud	Apple Inc.	Enabled	Not measured
iCloud Drive	Apple Inc.	Enabled	Not measured
iCloud Keychain	Apple Inc.	Enabled	Not measured
iCloud Photos	Apple Inc.	Enabled	Not measured
iCloud Shared Albums	Apple Inc.	Disabled	None
id_bglaunch.exe		Enabled	Not measured
id_tray.exe		Enabled	Not measured

Startup Apps (cont'd)

- See also:

Settings/Apps/Startup

- to turn off/on startup apps
- If you turn them off you can always start them when you need them...



Using Task Manager (Users)

Task Manager

Type a name, publisher, or PID to search

Users

Run new task Disconnect Manage user accounts

User	Status	15% CPU	67% Memory	3% Disk	0% Network
> les@larsj.info (184)		10.8%	4,310.6 MB	0.1 MB/s	0.1 Mbps

Processes

Performance

App history

Startup apps

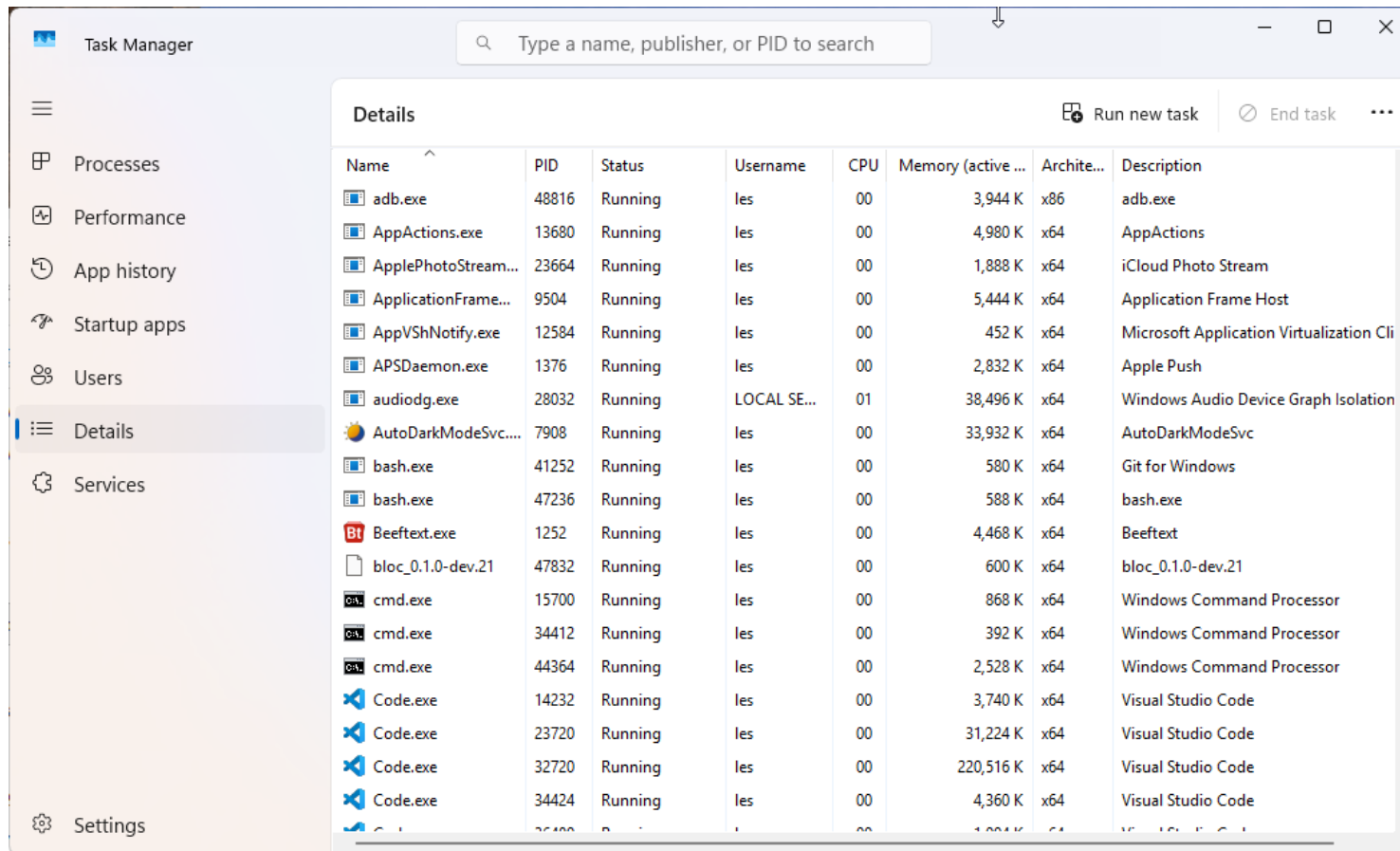
Users

Details

Services

Settings

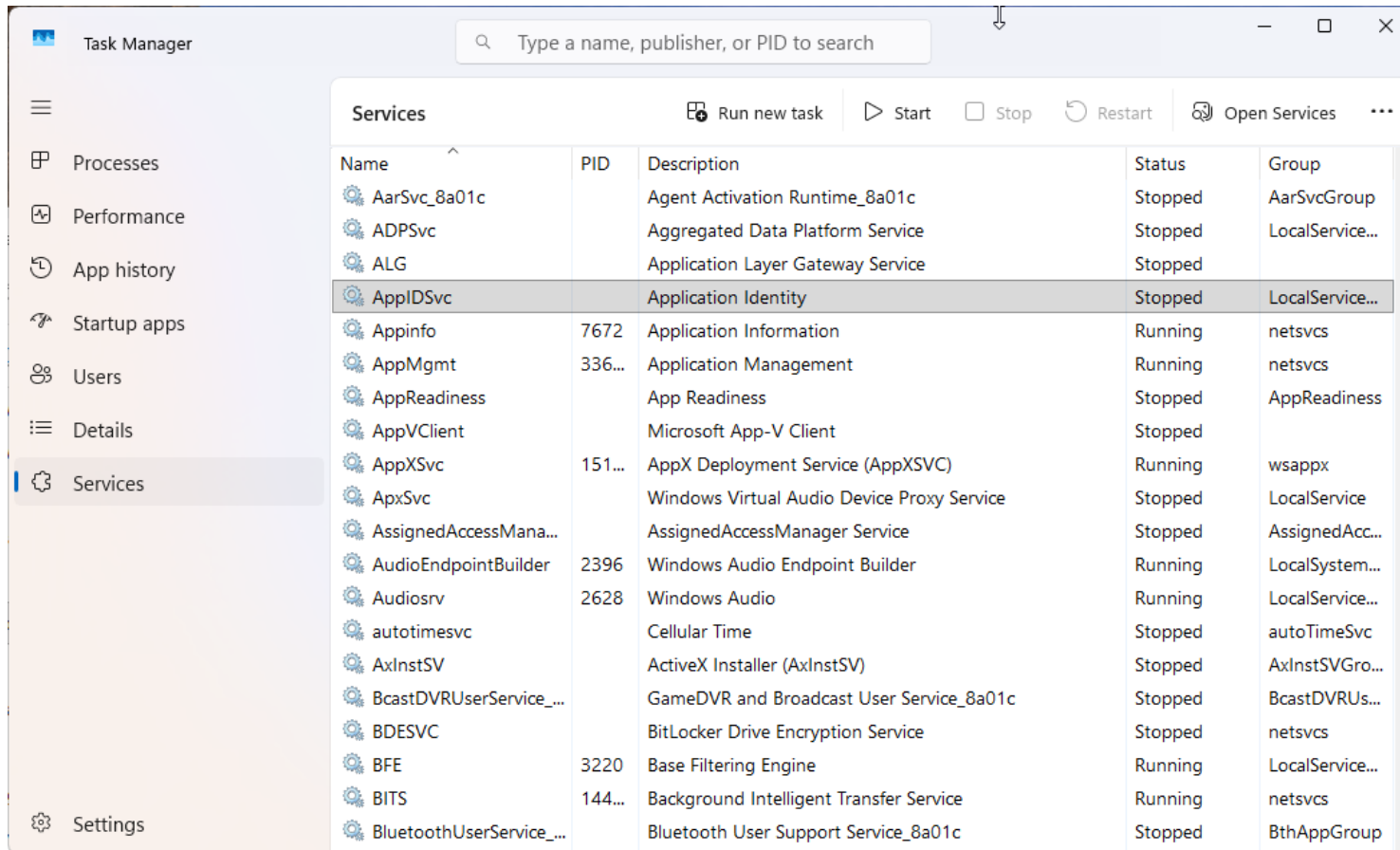
Using Task Manager (Details)



The screenshot shows the Windows Task Manager application in the 'Details' tab. The left sidebar contains navigation options: Processes, Performance, App history, Startup apps, Users, Details (selected), Services, and Settings. The main area displays a table of running processes with columns for Name, PID, Status, Username, CPU, Memory (active), Archite..., and Description. The table lists various processes including adb.exe, AppActions.exe, ApplePhotoStream..., ApplicationFrame..., AppVShNotify.exe, APSDaemon.exe, audiodg.exe, AutoDarkModeSvc..., bash.exe, Beeftext.exe, bloc_0.1.0-dev.21, cmd.exe, and Code.exe. The 'Details' tab is active, and the 'Run new task' and 'End task' buttons are visible at the top right of the table area.

Name	PID	Status	Username	CPU	Memory (active ...	Archite...	Description
adb.exe	48816	Running	les	00	3,944 K	x86	adb.exe
AppActions.exe	13680	Running	les	00	4,980 K	x64	AppActions
ApplePhotoStream...	23664	Running	les	00	1,888 K	x64	iCloud Photo Stream
ApplicationFrame...	9504	Running	les	00	5,444 K	x64	Application Frame Host
AppVShNotify.exe	12584	Running	les	00	452 K	x64	Microsoft Application Virtualization Cli
APSDaemon.exe	1376	Running	les	00	2,832 K	x64	Apple Push
audiodg.exe	28032	Running	LOCAL SE...	01	38,496 K	x64	Windows Audio Device Graph Isolation
AutoDarkModeSvc...	7908	Running	les	00	33,932 K	x64	AutoDarkModeSvc
bash.exe	41252	Running	les	00	580 K	x64	Git for Windows
bash.exe	47236	Running	les	00	588 K	x64	bash.exe
Beeftext.exe	1252	Running	les	00	4,468 K	x64	Beeftext
bloc_0.1.0-dev.21	47832	Running	les	00	600 K	x64	bloc_0.1.0-dev.21
cmd.exe	15700	Running	les	00	868 K	x64	Windows Command Processor
cmd.exe	34412	Running	les	00	392 K	x64	Windows Command Processor
cmd.exe	44364	Running	les	00	2,528 K	x64	Windows Command Processor
Code.exe	14232	Running	les	00	3,740 K	x64	Visual Studio Code
Code.exe	23720	Running	les	00	31,224 K	x64	Visual Studio Code
Code.exe	32720	Running	les	00	220,516 K	x64	Visual Studio Code
Code.exe	34424	Running	les	00	4,360 K	x64	Visual Studio Code

Using Task Manager (Services)



The screenshot shows the Windows Task Manager application with the 'Services' tab selected. The left sidebar contains navigation options: Processes, Performance, App history, Startup apps, Users, Details, Services (selected), and Settings. The main pane displays a list of services with columns for Name, PID, Description, Status, and Group. A search bar at the top of the main pane allows filtering by name, publisher, or PID. Action buttons at the top of the list include 'Run new task', 'Start', 'Stop', 'Restart', and 'Open Services'.

Name	PID	Description	Status	Group
AarSvc_8a01c		Agent Activation Runtime_8a01c	Stopped	AarSvcGroup
ADPSvc		Aggregated Data Platform Service	Stopped	LocalService...
ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalService...
Appinfo	7672	Application Information	Running	netsvcs
AppMgmt	336...	Application Management	Running	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppVClient		Microsoft App-V Client	Stopped	
AppXSvc	151...	AppX Deployment Service (AppXSVC)	Running	wsappx
ApxSvc		Windows Virtual Audio Device Proxy Service	Stopped	LocalService
AssignedAccessMana...		AssignedAccessManager Service	Stopped	AssignedAcc...
AudioEndpointBuilder	2396	Windows Audio Endpoint Builder	Running	LocalSystem...
Audiosrv	2628	Windows Audio	Running	LocalService...
autotimesvc		Cellular Time	Stopped	autoTimeSvc
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVGro...
BcastDVRUserService_...		GameDVR and Broadcast User Service_8a01c	Stopped	BcastDVRUs...
BDESVC		BitLocker Drive Encryption Service	Stopped	netsvcs
BFE	3220	Base Filtering Engine	Running	LocalService...
BITS	144...	Background Intelligent Transfer Service	Running	netsvcs
BluetoothUserService_...		Bluetooth User Support Service_8a01c	Stopped	BthAppGroup

Topics for future meetings

