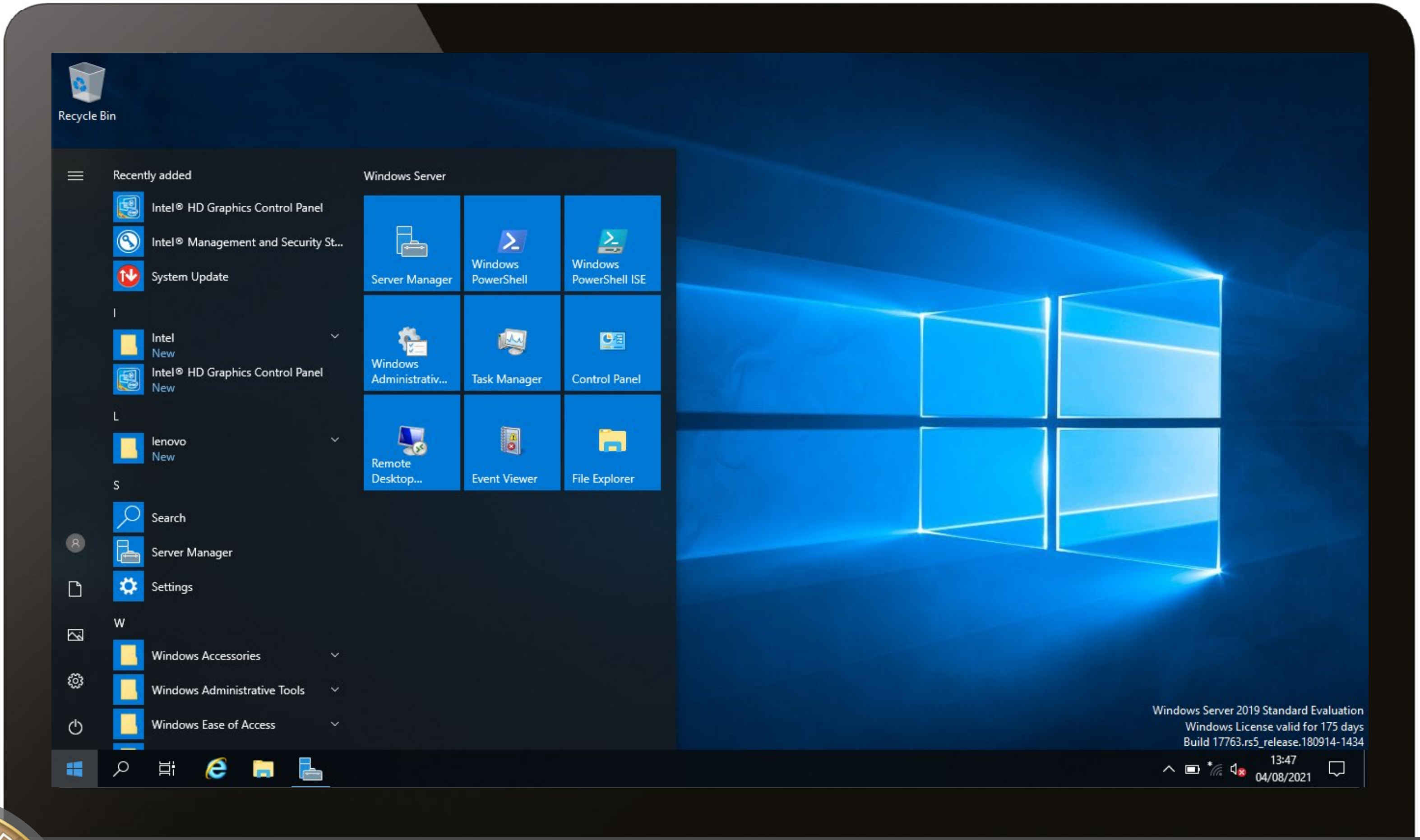
NORTHROP GRUMMAN

STEM LEARNING



Windows Server 2019 Standard Evaluation
Windows License valid for 175 days
Build 17763.rs5_release.180914-1434

CYBERCENTURION
EDUCATE, CHALLENGE, INSPIRE
YOUTH CYBER DEFENCE COMPETITION

Windows Advanced Cyber Security

Contents

Windows 10

As part of this guide, you will:

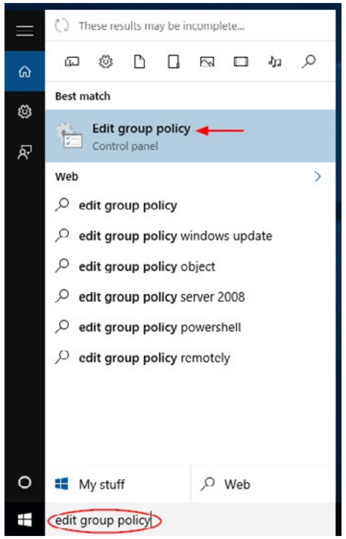
- demonstrate how to use the local group policy for passwords
- identify how to use the UAC
- describe how to use computer management and demonstrate how to add and remove a user, create and remove a group, manage shared folders and how to use the built-in admin account
- define the purpose of auditing and how to enable and edit the auditing policies
- define what a remote desktop service is, why it is a security risk and how to enable and disable remote desktop services
- define what an FTP is, why it is a security risk and how to enable and disable FTP services
- demonstrate how to use the Task Manager to investigate services running

Local group policy

In the last guide on the basics of Cyber Security we looked at passwords and how to enforce a password policy.

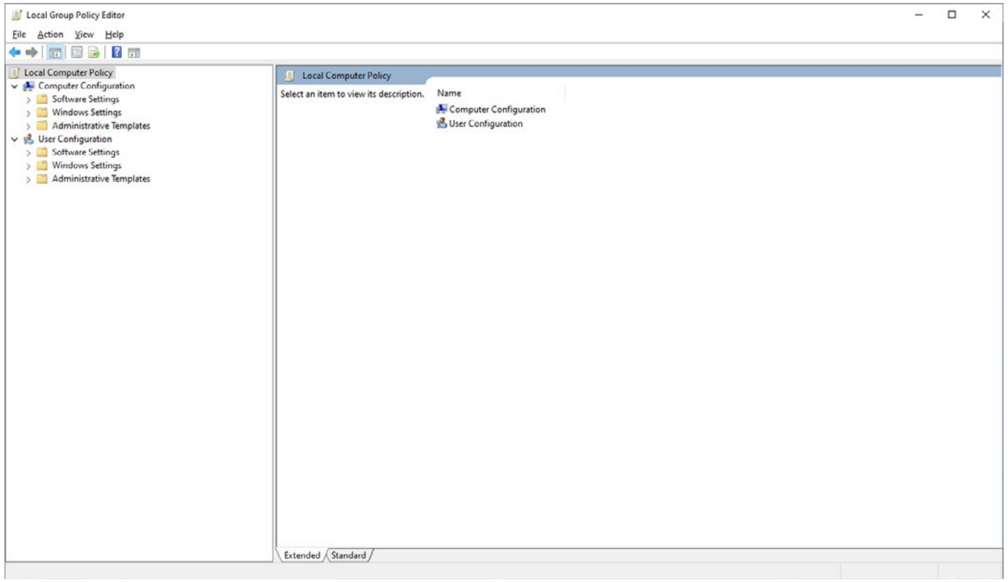
To control the accounts that are set up in Windows you can access the Local **`Group Policy`** and access the advanced settings that are not available when looking in the settings area.

To open this area, the easiest way is to search and open **`edit group policy`** in the search programs area.


These results may be incomplete...
Best match
Edit group policy
Control panel
Web
edit group policy
edit group policy windows update
edit group policy object
edit group policy server 2008
edit group policy powershell
edit group policy remotely
My stuff
Web

edit group policy

This area will allow you to ensure a strict group policy for all users on the device.



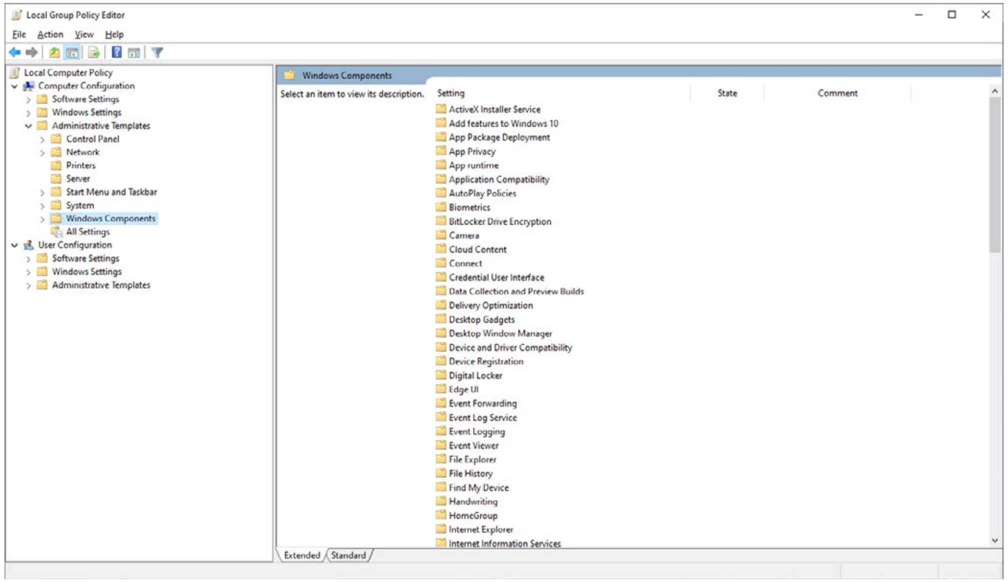
Select an item to view its description.

There are two main areas visible:

- Computer configuration
- User configuration

Both have the same sub folders and allow specific settings related to software, Windows, and administrative templates.

One aspect that can be configured here is the automatic updates for Windows. Under **Computer Configuration** locate the subfolder **Administrative Templates** and open the dropdown menu to locate the folder **Windows components**. Click on this folder to view all on the right-hand panel.



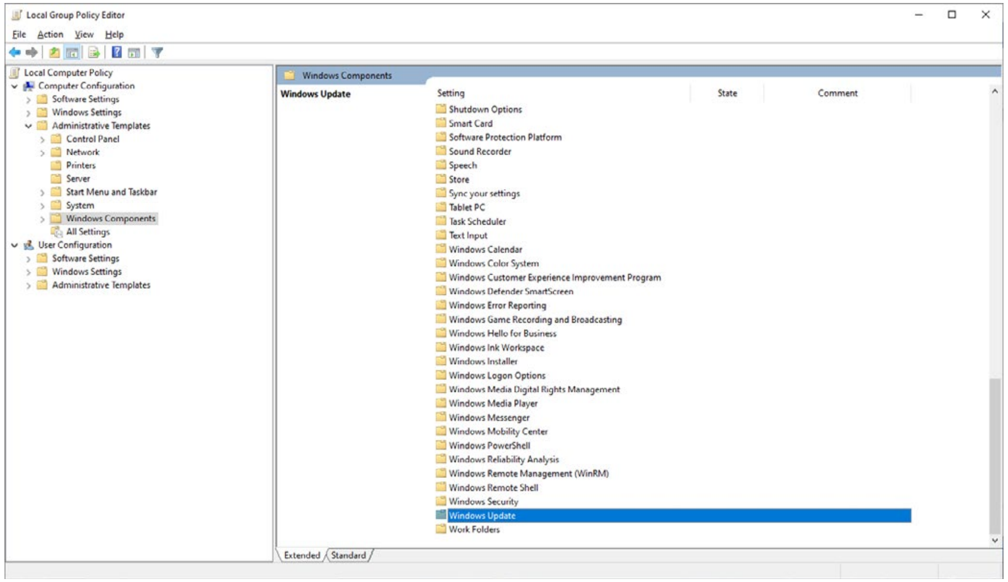
Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Network
    - Printers
    - Server
    - Start Menu and Taskbar
    - System
    - Windows Components
    - All Settings
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

Windows Components

Select an item to view its description.

ActiveX Installer Service
Add features to Windows 10
App Package Deployment
App Privacy
App runtime
Application Compatibility
AutoPlay Policies
Biometrics
BitLocker Drive Encryption
Camera
Cloud Content
Connect
Credential User Interface
Data Collection and Preview Builds
Delivery Optimization
Desktop Gadgets
Desktop Window Manager
Device and Driver Compatibility
Device Registration
Digital Locker
Edge UI
Event Forwarding
Event Log Service
Event Logging
Event Viewer
File Explorer
File History
Find My Device
Handwriting
HomeGroup
Internet Explorer
Internet Information Services

Locate the folder **Windows Update** and double click to open.



Local Computer Policy
- Computer Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates
    - Control Panel
    - Network
    - Printers
    - Server
    - Start Menu and Taskbar
    - System
    - Windows Components
    - All Settings
- User Configuration
  - Software Settings
  - Windows Settings
  - Administrative Templates

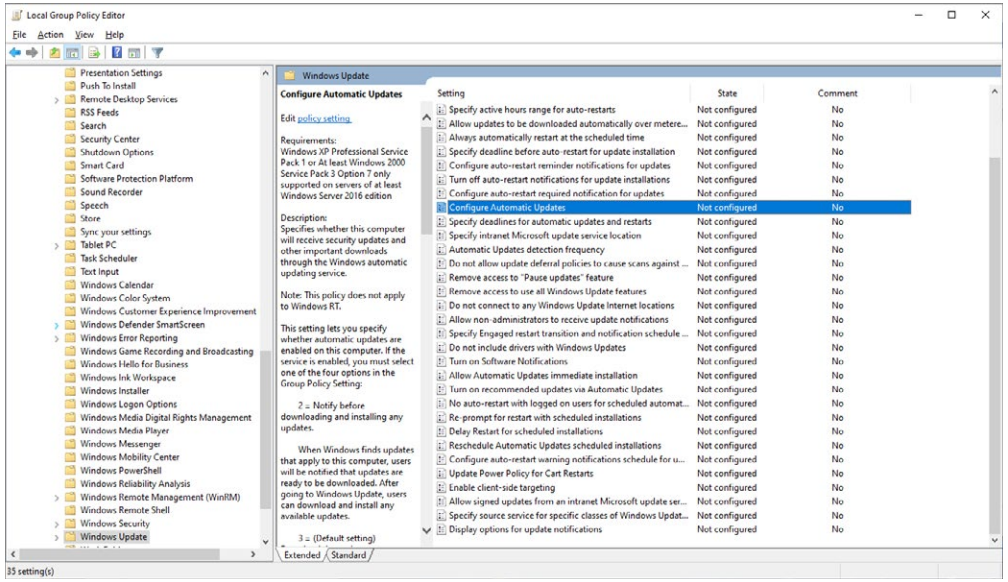
Windows Components

Windows Update

Shutdown Options
Smart Card
Software Protection Platform
Sound Recorder
Speech
Store
Sync your settings
Tablet PC
Task Scheduler
Text Input
Windows Calendar
Windows Color System
Windows Customer Experience Improvement Program
Windows Defender SmartScreen
Windows Error Reporting
Windows Game Recording and Broadcasting
Windows Hello for Business
Windows Ink Workspace
Windows Installer
Windows Logon Options
Windows Media Digital Rights Management
Windows Media Player
Windows Messenger
Windows Mobility Center
Windows PowerShell
Windows Reliability Analysis
Windows Remote Management (WinRM)
Windows Remote Shell
Windows Security
Windows Update
Work Folders

Locate the folder **`Configure Automatic Updates`** and click on it.

On the left of the selection, you will get some information to help you with settings.



Configure Automatic Updates

Edit policy setting

Requirements:
Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Description:
Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

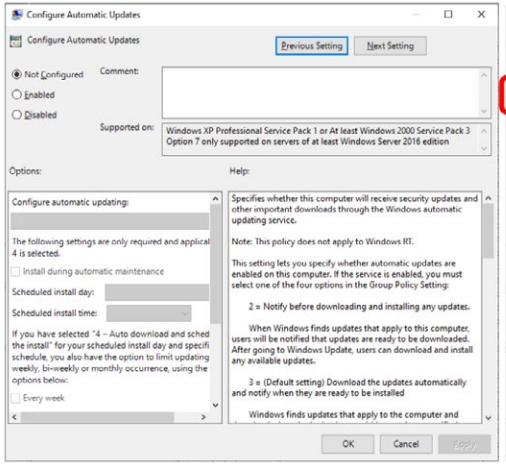
When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting)

Setting	State	Comment
Specify active hours range for auto-restarts	Not configured	No
Allow updates to be downloaded automatically over metere...	Not configured	No
Always automatically restart at the scheduled time	Not configured	No
Specify deadline before auto-restart for update installation	Not configured	No
Configure auto-restart reminder notifications for updates	Not configured	No
Turn off auto-restart notifications for update installations	Not configured	No
Configure auto-restart required notification for updates	Not configured	No
Configure Automatic Updates	Not configured	No
Specify deadlines for automatic updates and restarts	Not configured	No
Specify intranet Microsoft update service location	Not configured	No
Automatic Updates detection frequency	Not configured	No
Do not allow update deferral policies to cause scans against ...	Not configured	No
Remove access to "Pause updates" feature	Not configured	No
Remove access to use all Windows Update features	Not configured	No
Do not connect to any Windows Update Internet locations	Not configured	No
Allow non-administrators to receive update notifications	Not configured	No
Specify Engaged restart transition and notification schedule ...	Not configured	No
Do not include drivers with Windows Updates	Not configured	No
Turn on Software Notifications	Not configured	No
Allow Automatic Updates immediate installation	Not configured	No
Turn on recommended updates via Automatic Updates	Not configured	No
No auto-restart with logged on users for scheduled automat...	Not configured	No
Re-prompt for restart with scheduled installations	Not configured	No
Delay Restart for scheduled installations	Not configured	No
Reschedule Automatic Updates scheduled installations	Not configured	No
Configure auto-restart warning notifications schedule for u...	Not configured	No
Update Power Policy for Cart Restarts	Not configured	No
Enable client-side targeting	Not configured	No
Allow signed updates from an intranet Microsoft update ser...	Not configured	No
Specify source service for specific classes of Windows Updat...	Not configured	No
Display options for update notifications	Not configured	No

Right click on **`Configure Automatic Updates`** and select **`Edit`**.

Within the pop up you can **`enable`** the updates and set the specific day and time and frequency of the updates.



● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Options:

Configure automatic updating:

The following settings are only required and applical 4 is selected.

□ Install during automatic maintenance

Scheduled install day:

Scheduled install time:

If you have selected "4 – Auto download and sched the install" for your scheduled install day and specifi schedule, you also have the option to limit updating weekly, bi-weekly or monthly occurrence, using the options below:

□ Every week

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

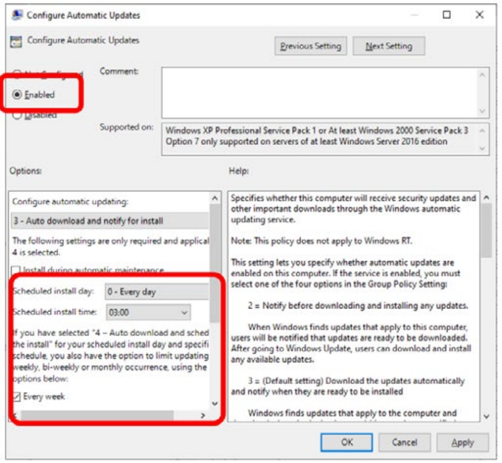
This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3 Option 7 only supported on servers of at least Windows Server 2016 edition

Options:

Configure automatic updating: 3 - Auto download and notify for install

The following settings are only required and applical 4 is selected.

□ Install during automatic maintenance

Scheduled install day: 0 - Every day

Scheduled install time: 03:00

If you have selected "4 – Auto download and sched the install" for your scheduled install day and specifi schedule, you also have the option to limit updating weekly, bi-weekly or monthly occurrence, using the options below:

☑ Every week

Help:

Specifies whether this computer will receive security updates and other important downloads through the Windows automatic updating service.

Note: This policy does not apply to Windows RT.

This setting lets you specify whether automatic updates are enabled on this computer. If the service is enabled, you must select one of the four options in the Group Policy Setting:

2 = Notify before downloading and installing any updates.

When Windows finds updates that apply to this computer, users will be notified that updates are ready to be downloaded. After going to Windows Update, users can download and install any available updates.

3 = (Default setting) Download the updates automatically and notify when they are ready to be installed

Windows finds updates that apply to the computer and

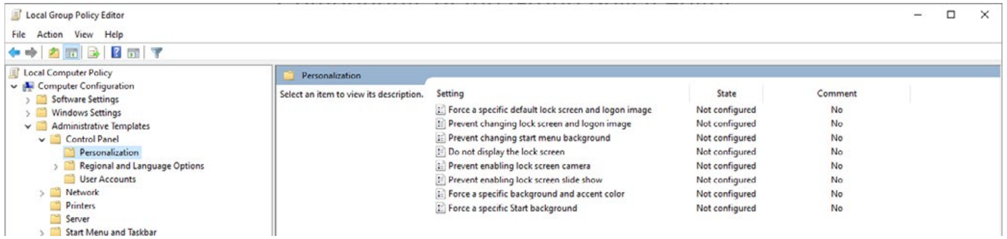
You can do a lot within the **`edit group policy`** window including:

- Limit the number of applications a user can install or access
- Disable the ability to use USB drives
- Restrict the settings a user can access and edit on the control panel
- Set and restrict change of a computer wallpaper

Restrict access to the Edit Group Policy area to stop any other users editing the settings

Return to the first view on the **`Edit Group Policy`** area and select under **`Computer Configuration:`**

- **`Administrative Templates`**
- **`Control Panel`**
- **`Personalization`**

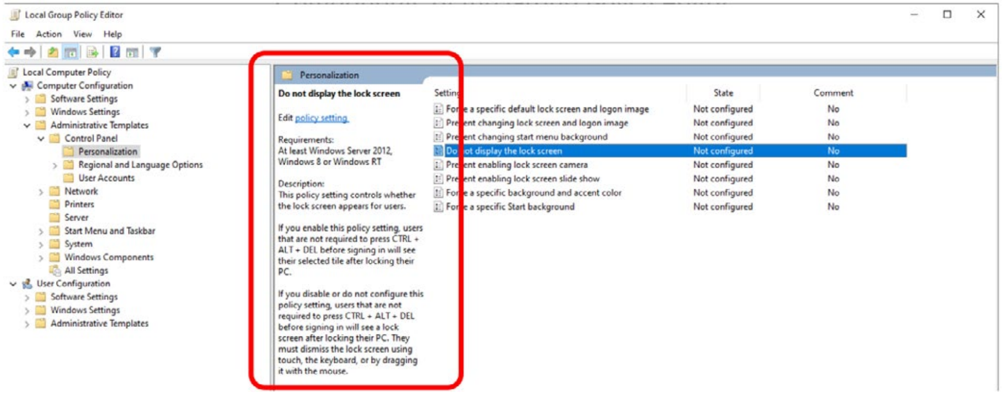


- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
        - Personalization
        - Regional and Language Options
        - User Accounts
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar

Select an item to view its description.

Setting	State	Comment
Force a specific default lock screen and logon image	Not configured	No
Prevent changing lock screen and logon image	Not configured	No
Prevent changing start menu background	Not configured	No
Do not display the lock screen	Not configured	No
Prevent enabling lock screen camera	Not configured	No
Prevent enabling lock screen slide show	Not configured	No
Force a specific background and accent color	Not configured	No
Force a specific Start background	Not configured	No

To view what a setting is capable of and the requirements, click on one of the settings on the right-hand panel to view or you can double click, or right click and edit, on any of the displayed options on the right-hand panel to be able to view the same description as well as change the settings.



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
        - Personalization
        - Regional and Language Options
        - User Accounts
      - Network
      - Printers
      - Server
      - Start Menu and Taskbar
      - System
      - Windows Components
      - All Settings
  - User Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates

Personalization

Do not display the lock screen

Edit policy setting

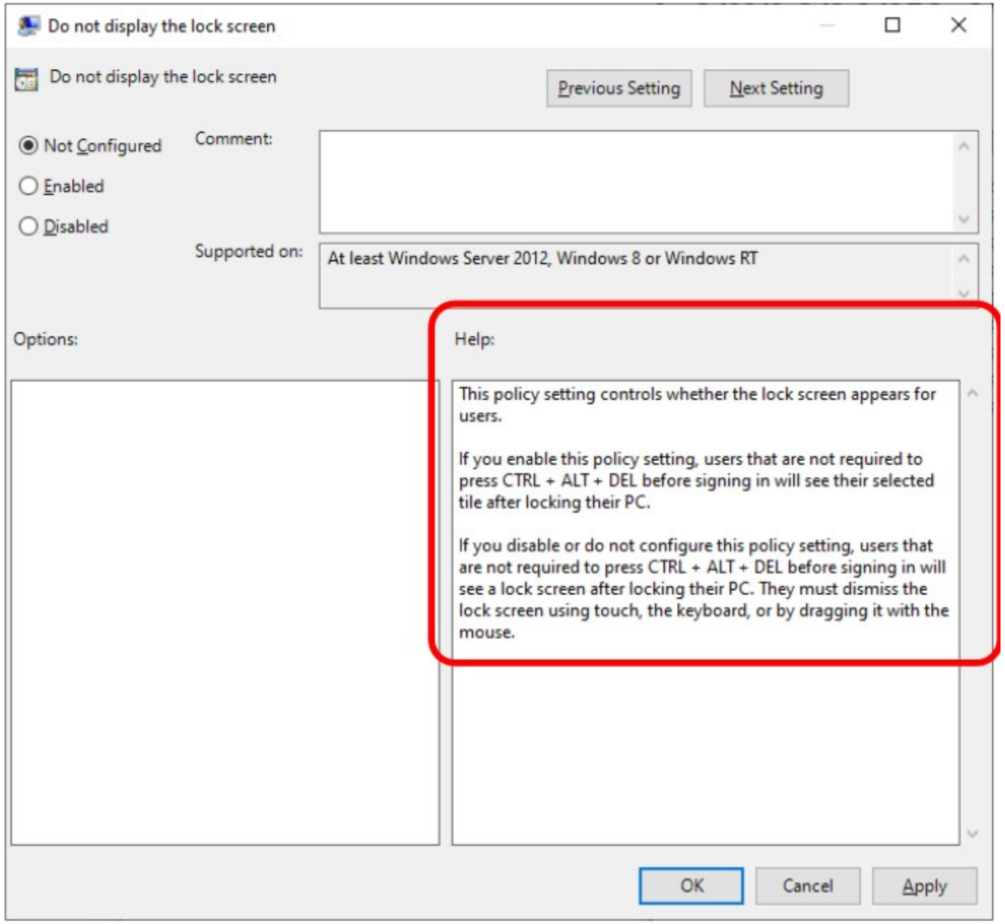
Requirements:
At least Windows Server 2012, Windows 8 or Windows RT

Description:
This policy setting controls whether the lock screen appears for users.

If you enable this policy setting, users that are not required to press CTRL + ALT + DEL before signing in will see their selected tile after locking their PC.

If you disable or do not configure this policy setting, users that are not required to press CTRL + ALT + DEL before signing in will see a lock screen after locking their PC. They must dismiss the lock screen using touch, the keyboard, or by dragging it with the mouse.

Setting	State	Comment
Force a specific default lock screen and logon image	Not configured	No
Prevent changing lock screen and logon image	Not configured	No
Prevent changing start menu background	Not configured	No
Do not display the lock screen	Not configured	No
Prevent enabling lock screen camera	Not configured	No
Prevent enabling lock screen slide show	Not configured	No
Force a specific background and accent color	Not configured	No
Force a specific Start background	Not configured	No


Do not display the lock screen
Do not display the lock screen
Previous Setting
Next Setting
OK
Cancel
Apply

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2012, Windows 8 or Windows RT

Options:

Help:

This policy setting controls whether the lock screen appears for users.

If you enable this policy setting, users that are not required to press CTRL + ALT + DEL before signing in will see their selected tile after locking their PC.

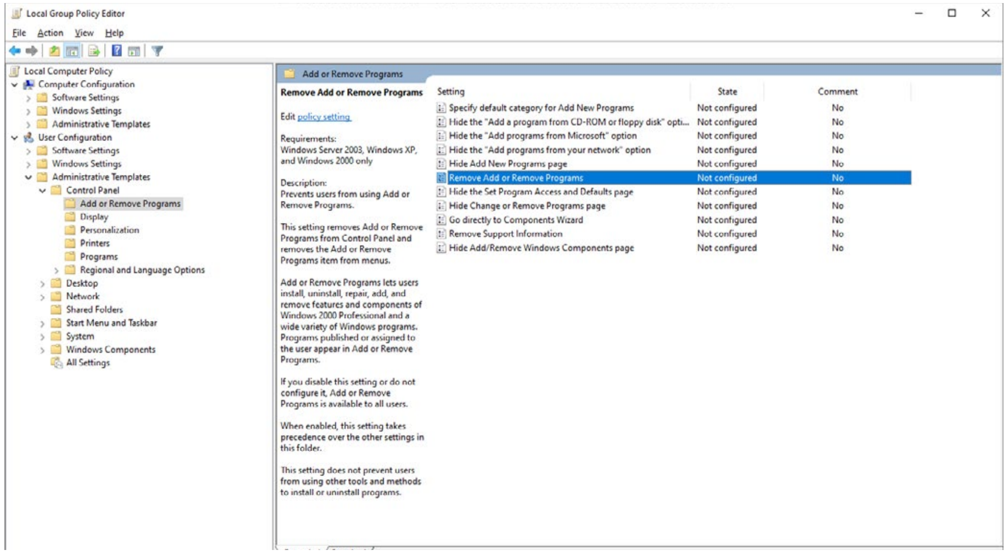
If you disable or do not configure this policy setting, users that are not required to press CTRL + ALT + DEL before signing in will see a lock screen after locking their PC. They must dismiss the lock screen using touch, the keyboard, or by dragging it with the mouse.

Under the **`User Configuration`** you can edit the settings for users on the device.

For example, under **`User Configuration`**:

- **`Administrative Templates`**
- **`Control Panel`**
- **`Add or Remove programs`**

You can edit the access a user has to view, edit, and access the settings in the control panel.



Remove Add or Remove Programs

Edit policy setting

Requirements:
Windows Server 2003, Windows XP, and Windows 2000 only

Description:
Prevents users from using Add or Remove Programs.

This setting removes Add or Remove Programs from Control Panel and removes the Add or Remove Programs item from menus.

Add or Remove Programs lets users install, uninstall, repair, add, and remove features and components of Windows 2000 Professional and a wide variety of Windows programs. Programs published or assigned to the user appear in Add or Remove Programs.

If you disable this setting or do not configure it, Add or Remove Programs is available to all users.

When enabled, this setting takes precedence over the other settings in this folder.

This setting does not prevent users from using other tools and methods to install or uninstall programs.

Setting	State	Comment
Specify default category for Add New Programs	Not configured	No
Hide the "Add a program from CD-ROM or floppy disk" opti...	Not configured	No
Hide the "Add programs from Microsoft" option	Not configured	No
Hide the "Add programs from your network" option	Not configured	No
Hide Add New Programs page	Not configured	No
Remove Add or Remove Programs	Not configured	No
Hide the Set Program Access and Defaults page	Not configured	No
Hide Change or Remove Programs page	Not configured	No
Go directly to Components Wizard	Not configured	No
Remove Support Information	Not configured	No
Hide Add/Remove Windows Components page	Not configured	No

Cyber Security fact:
There are a lot more settings and options in these areas and it is essential to ensure any users on a device has the correct level of access to allow its use to be secure.

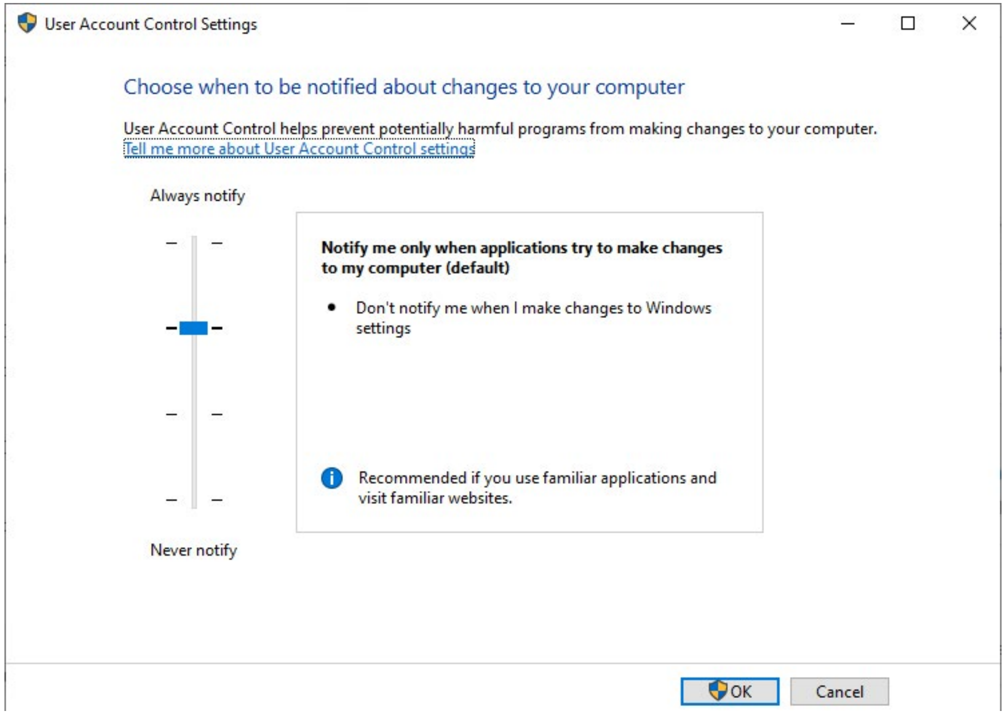
User Account Control (UAC)

User Account Control (UAC) helps prevent malware from damaging a PC and helps organisations deploy a better-managed desktop.

When you search for `User Account Control Settings` using the search programs area, you will open a window like below and here you can see that I can adjust if I am notified when applications try to make changes to my computer and/or if I make changes to settings.

There are different settings here:

- Always notify me when:
  - Applications try to install software or make changes to my computer
  - I make changes to Windows settings
- Notify me only when programs try to make changes to my computer – this is the default setting
  - Don't notify me when I make changes to Windows settings
- Notify me only when programs try to make changes to my computer (do not dim my desktop)
  - Don't notify me when I make changes to Windows settings
- Never notify (Disable UAC) me when:
  - Applications try to install software or make changes to my computer
  - I make changes to Windows settings



User Account Control Settings

Choose when to be notified about changes to your computer

User Account Control helps prevent potentially harmful programs from making changes to your computer.
Tell me more about User Account Control settings

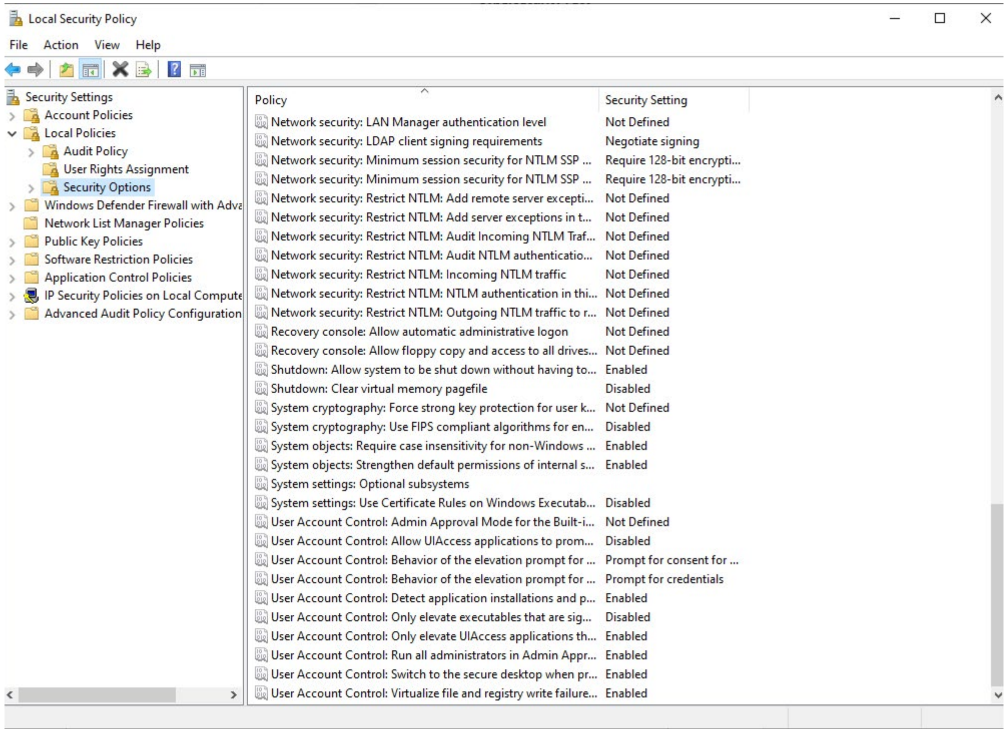
Notify me only when applications try to make changes to my computer (default)

- Don't notify me when I make changes to Windows settings

Recommended if you use familiar applications and visit familiar websites.

Cyber Security fact:
If you do not set this correctly or have this as disabling the UAC, you are not going to be notified when applications make changes to your computer and may give access to areas or files that you do not want freely available. The settings within a computer area there to protect the data and user and should be set accordingly.

To look further at the UAC, you need to open **`Local Security Policy.`** Under **`Local Policies / Security Options`**, you can see a long list of policies and the security setting appear on the right-hand side. Scroll down the list to locate the **`user account control`** policies.



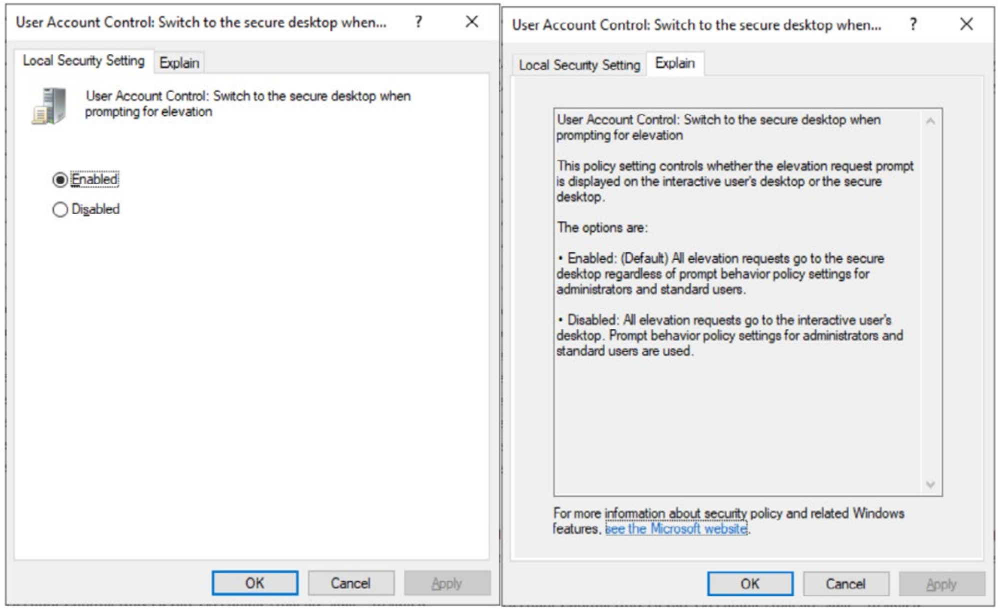
Local Security Policy
File Action View Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Network security: LAN Manager authentication level	Not Defined
Network security: LDAP client signing requirements	Negotiate signing
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Minimum session security for NTLM SSP ...	Require 128-bit encrypti...
Network security: Restrict NTLM: Add remote server excepti...	Not Defined
Network security: Restrict NTLM: Add server exceptions in t...	Not Defined
Network security: Restrict NTLM: Audit Incoming NTLM Traf...	Not Defined
Network security: Restrict NTLM: Audit NTLM authenticatio...	Not Defined
Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
Network security: Restrict NTLM: NTLM authentication in thi...	Not Defined
Network security: Restrict NTLM: Outgoing NTLM traffic to r...	Not Defined
Recovery console: Allow automatic administrative logon	Not Defined
Recovery console: Allow floppy copy and access to all drives...	Not Defined
Shutdown: Allow system to be shut down without having to...	Enabled
Shutdown: Clear virtual memory pagefile	Disabled
System cryptography: Force strong key protection for user k...	Not Defined
System cryptography: Use FIPS compliant algorithms for en...	Disabled
System objects: Require case insensitivity for non-Windows ...	Enabled
System objects: Strengthen default permissions of internal s...	Enabled
System settings: Optional subsystems	
System settings: Use Certificate Rules on Windows Executab...	Disabled
User Account Control: Admin Approval Mode for the Built-i...	Not Defined
User Account Control: Allow UIAccess applications to prom...	Disabled
User Account Control: Behavior of the elevation prompt for ...	Prompt for consent for ...
User Account Control: Behavior of the elevation prompt for ...	Prompt for credentials
User Account Control: Detect application installations and p...	Enabled
User Account Control: Only elevate executables that are sig...	Disabled
User Account Control: Only elevate UIAccess applications th...	Enabled
User Account Control: Run all administrators in Admin Appr...	Enabled
User Account Control: Switch to the secure desktop when pr...	Enabled
User Account Control: Virtualize file and registry write failure...	Enabled

There are 10 Group Policy settings that can be configured for User Account Control (UAC), and you will notice the American spelling of behaviour as behavior.

- **User Account Control:** Admin Approval Mode for the built-in Administrator account
- **User Account Control:** Behavior of the elevation prompt for administrators in Admin Approval Mode
- **User Account Control:** Behavior of the elevation prompt for standard users
- **User Account Control:** Detect application installations and prompt for elevation
- **User Account Control:** Only elevate executables that are signed and validated
- **User Account Control:** Only elevate UIAccess applications that are installed in secure locations
- **User Account Control:** Run all administrators in Admin Approval Mode
- **User Account Control:** Switch to the secure desktop when prompting for elevation
- **User Account Control:** Virtualize file and registry write failures to per-user locations

When you double click or right click and select properties, you will open the window to enable or disable the setting. The pop-up window also has an explain tab, here you can read more about the setting before making changes.



User Account Control: Switch to the secure desktop when prompting for elevation

● Enabled

○ Disabled

User Account Control: Switch to the secure desktop when prompting for elevation

This policy setting controls whether the elevation request prompt is displayed on the interactive user's desktop or the secure desktop.

The options are:

• Enabled: (Default) All elevation requests go to the secure desktop regardless of prompt behavior policy settings for administrators and standard users.

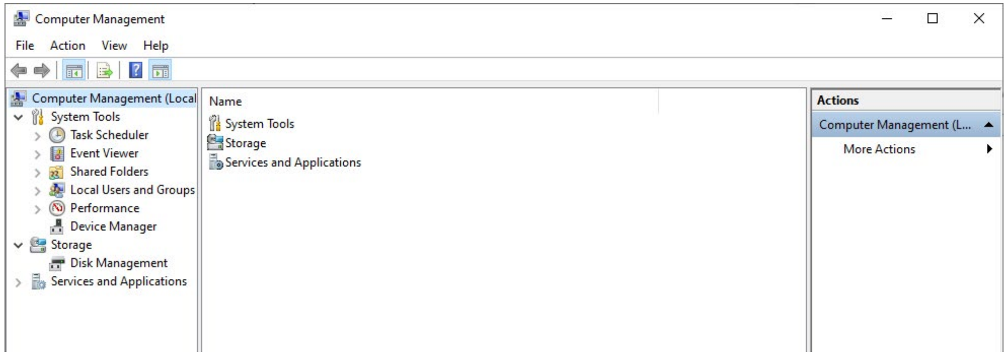
• Disabled: All elevation requests go to the interactive user's desktop. Prompt behavior policy settings for administrators and standard users are used.

For more information about security policy and related Windows features, see the Microsoft website.

For more information on the individual settings – click here.

Computer Management

We have looked at some of the areas of the Computer Management area in the earlier guides. To open use the search programs area.



Adding a user

When you have a system that has one user you do not think about the user settings and access permissions as we log on and use the computer and log off. If there is more than one user that is going to be accessing and using the device, then additional security measures need to be put in place.

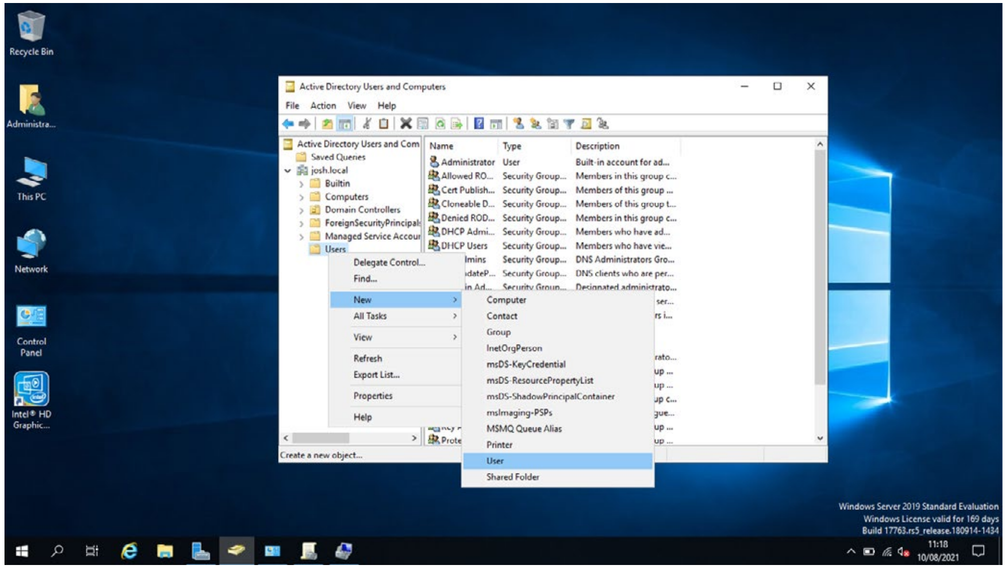
Imagine you have specific files that you have saved on your device and use that for personal or work purposes. Do you want to allow any user to access them? The answer would be on most occasions, no.

Each user requires their own login credentials, folder structure and security permissions and settings. All this can be done when creating a new user.

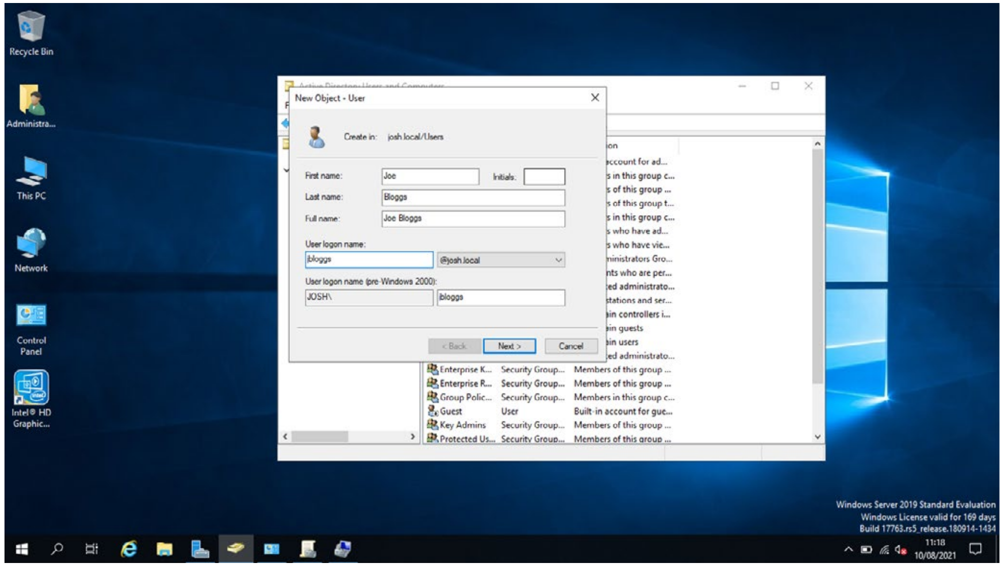
There are two ways to add a new user:

Option 1

To add a new user, you need to open the **`Active Directory Users and Computers`** area and right click on the user's folder and select **`New/User`**.


Recycle Bin
Administra...
This PC
Network
Control Panel
Intel® HD Graphic...
Active Directory Users and Computers
File Action View Help
Active Directory Users and Com
Saved Queries
josh.local
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accour
Users
Name Type Description
Administrator User Built-in account for ad...
Allowed RO... Security Group... Members in this group c...
Cert Publish... Security Group... Members of this group ...
Cloneable D... Security Group... Members of this group t...
Denied ROD... Security Group... Members in this group c...
DHCP Admi... Security Group... Members who have ad...
DHCP Users Security Group... Members who have vie...
Security Group... DNS Administrators Gro...
Security Group... DNS clients who are per...
Security Group... Designated administrato...
Delegate Control...
Find...
New
All Tasks
View
Refresh
Export List...
Properties
Help
Computer
Contact
Group
InetOrgPerson
msDS-KeyCredential
msDS-ResourcePropertyList
msDS-ShadowPrincipalContainer
msImaging-PSPs
MSMQ Queue Alias
Printer
User
Shared Folder
Create a new object...
Windows Server 2019 Standard Evaluation
Windows License valid for 169 days
Build 17763.rs5_release.180914-1434
11:18
10/08/2021

Within the window that appears you can then add the details of the new user, their name, and their logon name.



New Object - User

Create in: josh.local/Users

First name: Joe

Initials:

Last name: Bloggs

Full name: Joe Bloggs

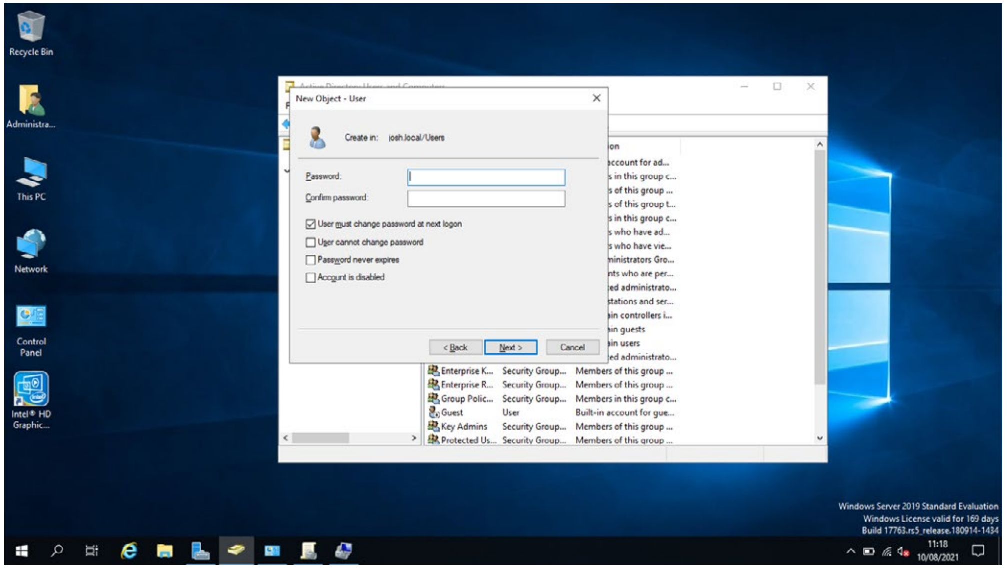
User logon name: jbloggs @josh.local

User logon name (pre-Windows 2000): JOSH\ jbloggs

When you click **next** you can set the password for the new user and that the user must change the password when they next logon.

There are other options that can be selected:

- User cannot change password
- Password never expires
- Account is disabled



New Object - User

Create in: josh.local/Users

Password:

Confirm password:

☑ User must change password at next logon

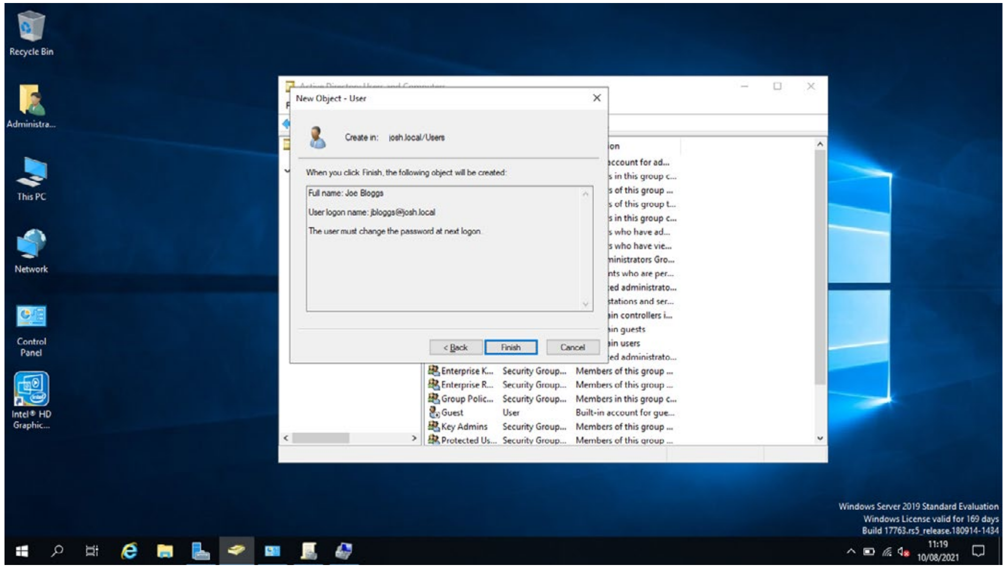
☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Cyber Security fact:
If you leave the password as the password set when the new user is set up, the person who set up the account can then continue to access the new users account and make any changes. This is not good practice for Cyber Security as a password needs to be private and only used by the user. The admin user does still have the ability to reset this password if required.

When you click **next**, you are presented with the details of the new user before selecting finish to finalise the new user set up.



New Object - User

Create in: josh.local/Users

When you click Finish, the following object will be created:

Full name: Joe Bloggs

User logon name: jbloggs@josh.local

The user must change the password at next logon.

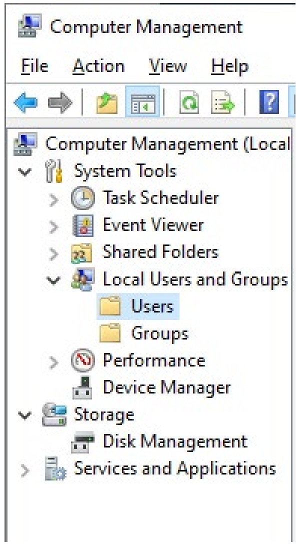
< Back
Finish
Cancel
Windows Server 2019 Standard Evaluation
Windows License valid for 169 days
Build 17763.rs5_release.180914-1434

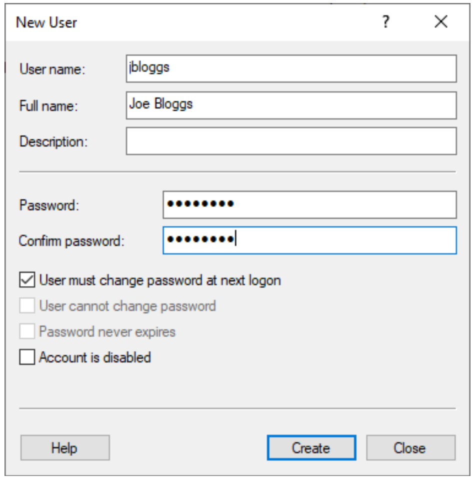
Option 2

When you open **`Computer Management`** locate the **`Users`** within the **`Local Users and Groups`** area.

Right click on the **`Users`** folder and select **`New User.`**

On the pop-up window, you can add the username, full name and set the password with the same settings as previous for ensuring the password is changed when first login occurs.





New User

User name: jbloggs

Full name: Joe Bloggs

Description:

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

☑ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

Removing a user

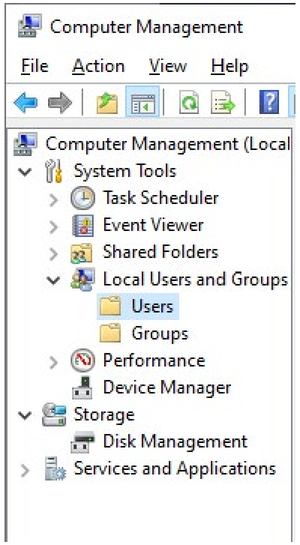
Option 1

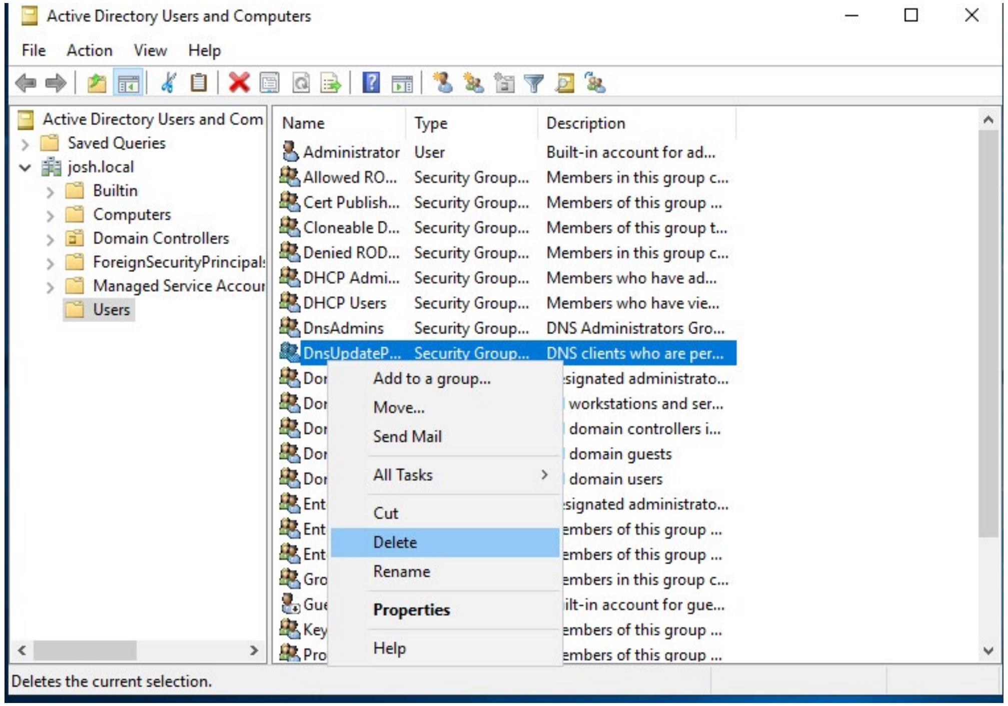
When you open **Computer Management** locate the **Users** within the **Local Users and Groups** area.

You will then have a list of users displayed on the right-hand side. You can then right click on any of the users and select **delete**.

Option 2

In the **Active Directory Users and Computers** area, locate the user on the list of options as seen in the image on the right, and right click and delete.





Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RO...	Security Group...	Members in this group c...
Cert Publish...	Security Group...	Members of this group ...
Cloneable D...	Security Group...	Members of this group t...
Denied ROD...	Security Group...	Members in this group c...
DHCP Admi...	Security Group...	Members who have ad...
DHCP Users	Security Group...	Members who have vie...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateP...	Security Group...	DNS clients who are per...
Dor		signated administrato...
Dor		workstations and ser...
Dor		domain controllers i...
Dor		domain guests
Dor		domain users
Ent		signated administrato...
Ent		embers of this group ...
Ent		embers of this group ...
Gro		embers in this group c...
Gue		ilt-in account for gue...
Key		embers of this group ...
Pro		embers of this group ...

Deletes the current selection.

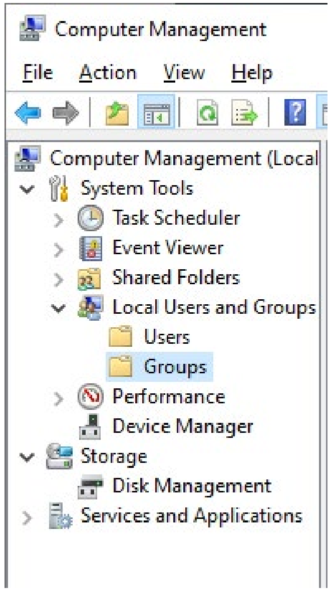
Creating a Group

In the same way as previous sections, we have two options available to create a new group.

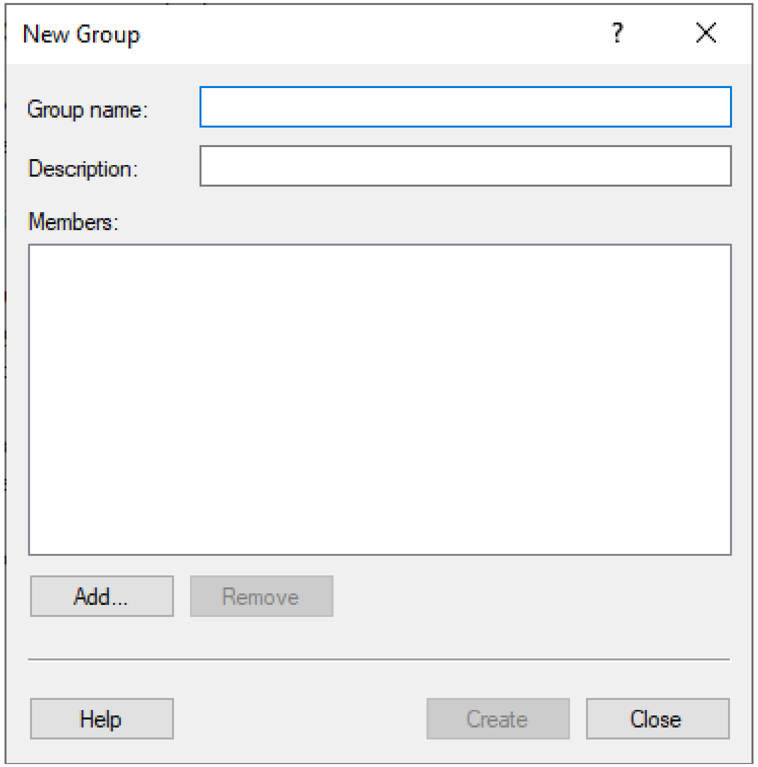
Option 1

When you open **`Computer Management`** locate the **`Groups`** within the **`Local Users and Groups`** area.

Right click on the **`Groups`** folder and select **`New Group`**.



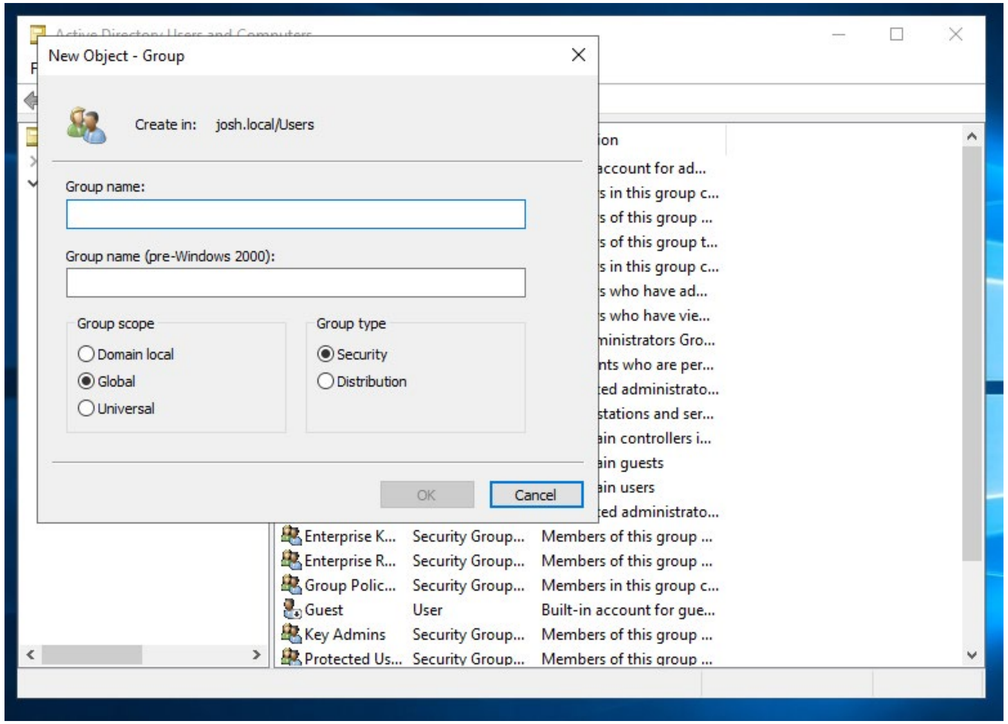
You can create the group name and select the users that will become the members of the group.



Option 2

In the **Active Directory Users and Computers** area, select the **User** folder. Click **Action / New / Group**.

Here you can create the name of the group and the security levels.



New Object - Group

Create in: josh.local/Users

Group name:

Group name (pre-Windows 2000):

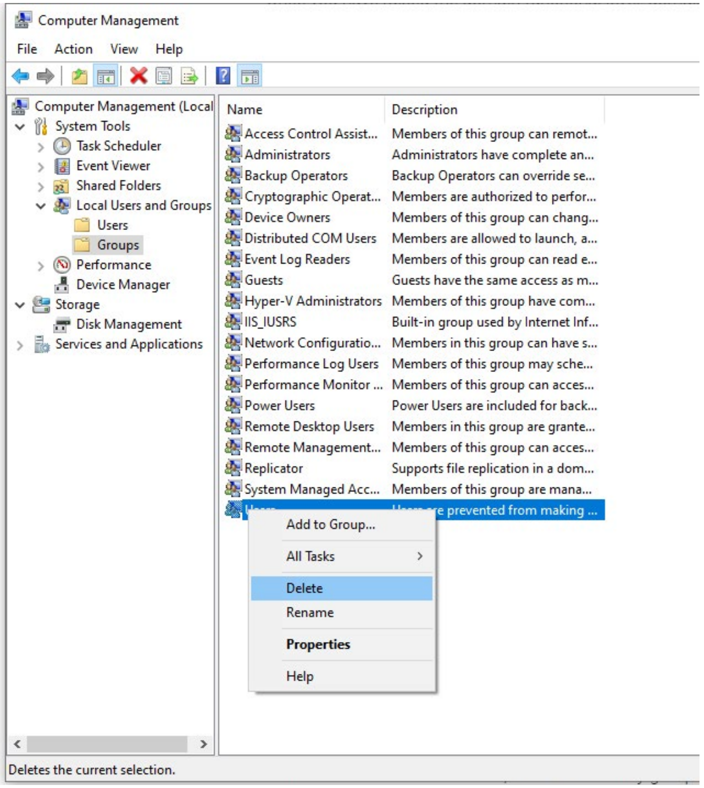
Group scope
○ Domain local
● Global
○ Universal

Group type
● Security
○ Distribution

Enterprise K...	Security Group...	Members of this group ...
Enterprise R...	Security Group...	Members of this group ...
Group Polic...	Security Group...	Members in this group c...
Guest	User	Built-in account for gue...
Key Admins	Security Group...	Members of this group ...
Protected Us...	Security Group...	Members of this group ...

Removing a Group

In the same way as removing a user you can remove a group from the **Computer Management** view and the **Active Directory Users and Computers** areas.



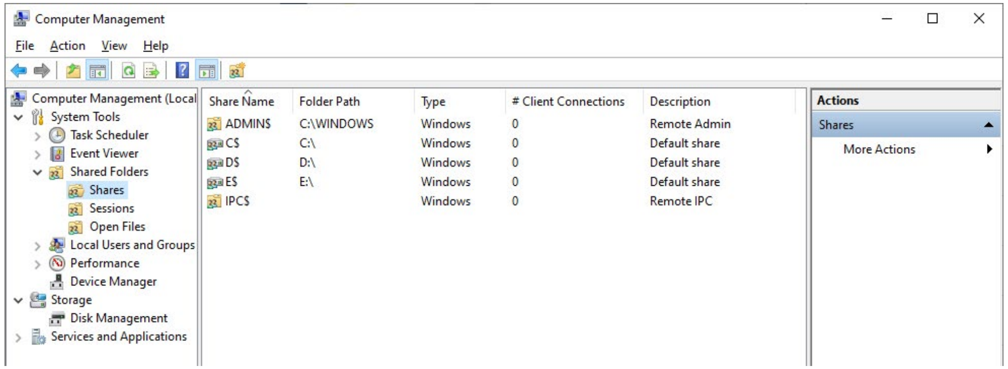
Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
System Managed Acc...	Members of this group are mana...
[illegible]	[illegible]e prevented from making ...

Deletes the current selection.

Shared folders

When you have more than one user using a device, they have their own personal folder directory that they can save and access files from. But what about a file or folder that all users need to have access to? This is set up as a shared folder within the `Computer Management` area.

Locate the `Shared Folders` area and select the `Shares` folder.



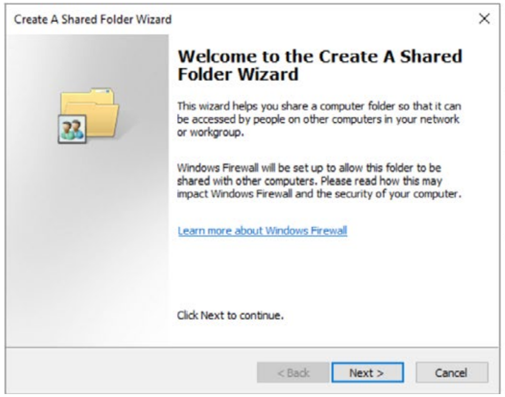
Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\WINDOWS	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
D$	D:\	Windows	0	Default share
E$	E:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC

These are the folders at present that are set up as shared folders, to view the settings on any of these folders, double click or right click to view and edit the settings.

To add a new shared folder, you can right click on the right-hand area where the list of shared folders is visible or right click on the left-hand navigation bar on the folder `Shares`.

When you open this, you will activate a `Create A Shared Folder Wizard` that will walk you through the set up easily.

Click next on the pop-up window and then select the folder you wish to share through the `browse` button and click next.


Create A Shared Folder Wizard

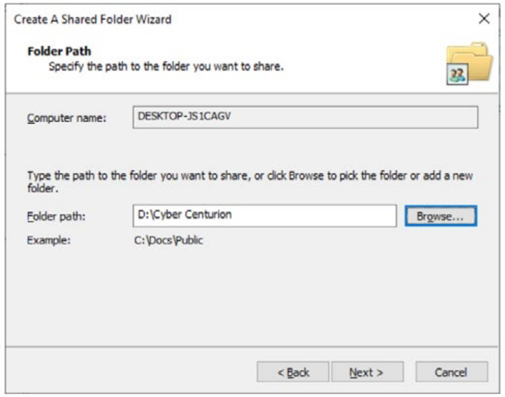
Welcome to the Create A Shared Folder Wizard

This wizard helps you share a computer folder so that it can be accessed by people on other computers in your network or workgroup.

Windows Firewall will be set up to allow this folder to be shared with other computers. Please read how this may impact Windows Firewall and the security of your computer.

Learn more about Windows Firewall

Click Next to continue.


Create A Shared Folder Wizard

Folder Path
Specify the path to the folder you want to share.

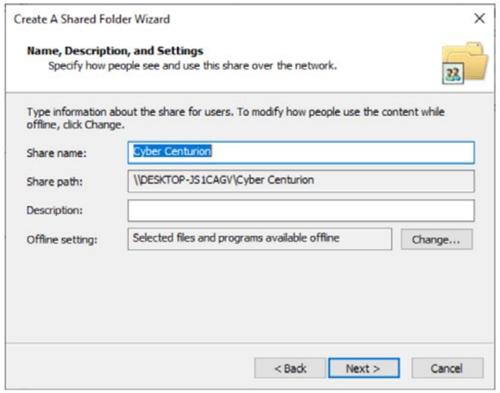
Computer name: DESKTOP-JS1CAGV

Type the path to the folder you want to share, or click Browse to pick the folder or add a new folder.

Folder path: D:\Cyber Centurion

Example: C:\Docs\Public

You can add a description and edit the shared name before clicking next and setting the permission status for the folder. You can leave it as read only so that the users can access but not make any changes or give full access or customise further. Click finish to complete the set up.



Create A Shared Folder Wizard

Name, Description, and Settings

Specify how people see and use this share over the network.

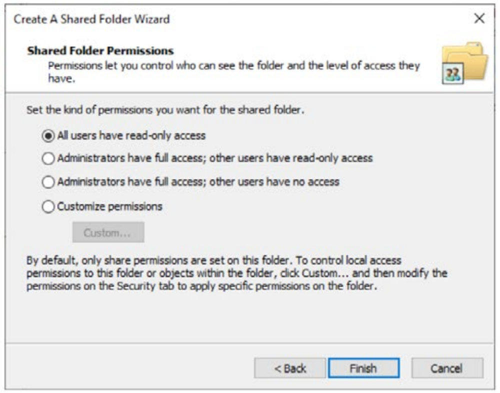
Type information about the share for users. To modify how people use the content while offline, click Change.

Share name: Cyber Centurion

Share path: \\DESKTOP-JS1CAGV\Cyber Centurion

Description:

Offline setting: Selected files and programs available offline



Create A Shared Folder Wizard

Shared Folder Permissions

Permissions let you control who can see the folder and the level of access they have.

Set the kind of permissions you want for the shared folder.

● All users have read-only access

○ Administrators have full access; other users have read-only access

○ Administrators have full access; other users have no access

○ Customize permissions

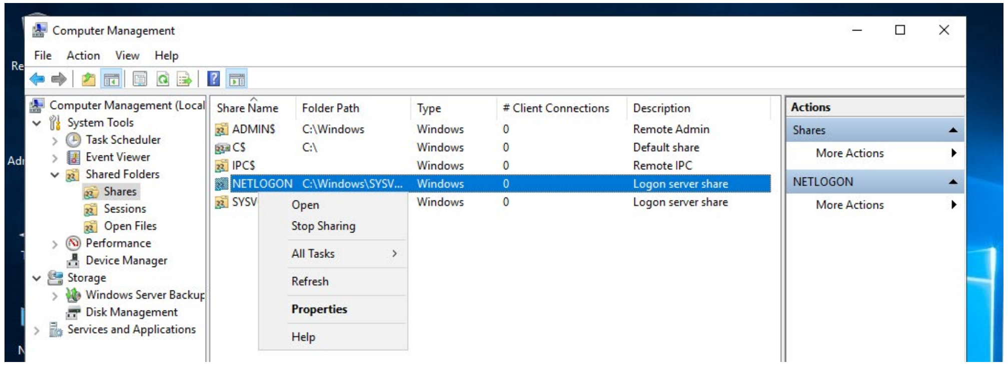
By default, only share permissions are set on this folder. To control local access permissions to this folder or objects within the folder, click Custom... and then modify the permissions on the Security tab to apply specific permissions on the folder.

Now when any user is logged in to their account, they will be able to access this folder with the permission settings you have specified.

Cyber Security fact:

It is important to only allow the correct level of access to files and folders to ensure the user cannot edit sensitive information as well as monitor version control. Version control is where you save a file as a new version to ensure you are aware of any updates to the document.

To stop the sharing of a file, locate the folder within the `Shares` area and right click and select `Stop Sharing`.



Computer Management

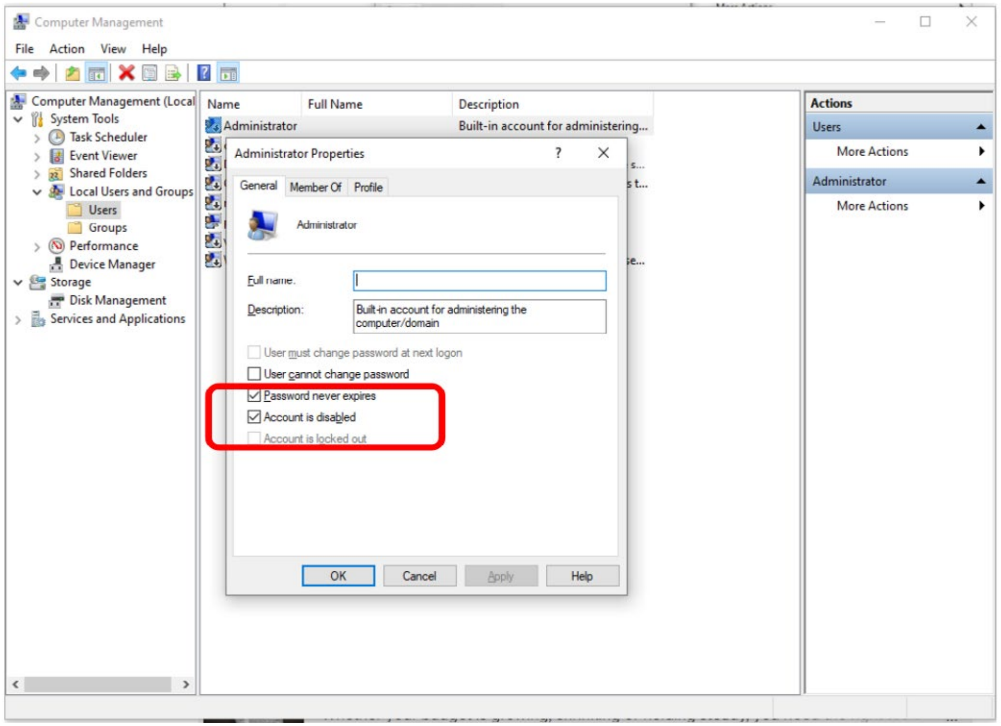
Share Name	Folder Path	Type	# Client Connections	Description
ADMIN$	C:\Windows	Windows	0	Remote Admin
C$	C:\	Windows	0	Default share
IPC$		Windows	0	Remote IPC
NETLOGON	C:\Windows\SYSV...	Windows	0	Logon server share
SYSV		Windows	0	Logon server share

Built in administrator account

You may have noticed that the list of users has an administrator user, this is set up and disabled as default when Windows is set up. An administrator user will have all permissions set to allow full access and you could edit and add/delete any settings. This could cause a security risk as well as editing something by mistake that could stop the system from working as expected. For this reason, the account is set as disabled and only through the `Computer Management` area can you enable the user.

It is recommended to only enable the administrator user for the period required and then disable to stop any errors being made when using the user account by mistake.

To enable the user, locate the user from the list of users in the Computer Management area and either double click or right click and select properties.



Full name:

Description: Built-in account for administering the computer/domain

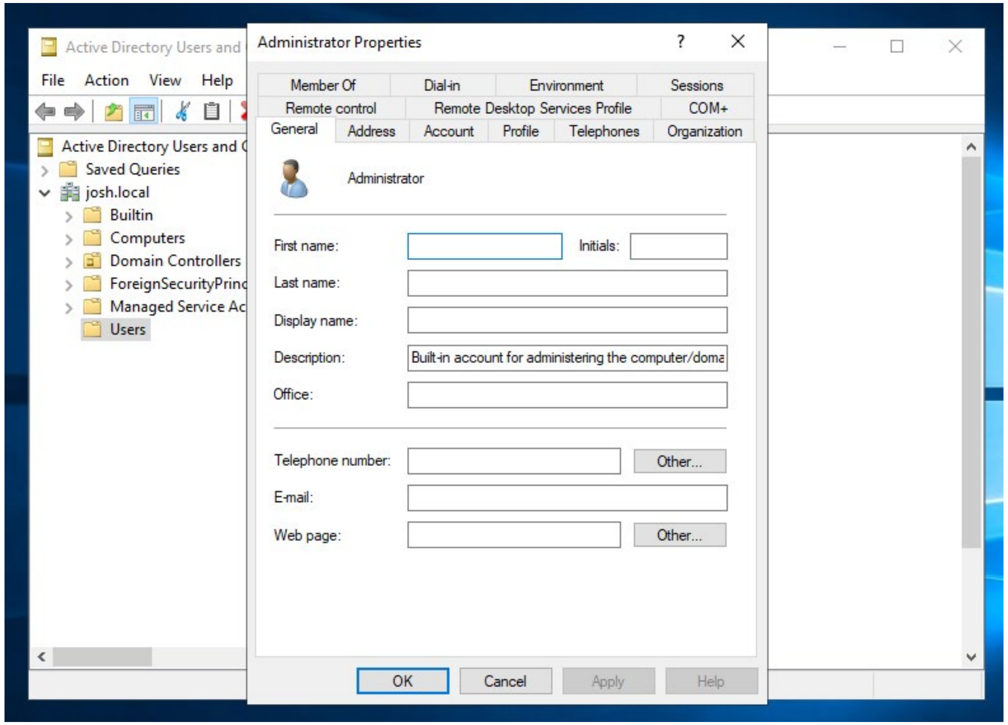
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
☑ Account is disabled
□ Account is locked out

Untick the `Account is disabled` checkbox and click apply to enable the user account for use.

When a new system is set up there are numerous default settings and these are set in line with the company creating the operating systems own settings. Your needs as the owner of the computer or the devices may differ. It is important to understand the settings and what should and should not be enabled and disabled. This will enable the system to be secure, used securely and maintain its security to the needs of the user.

Remember an admin user will have full access to the system and should be used only when required, to minimise the risk to the security and running of the system.

You can also access the administrator properties of the user through the `Active Directory of Users and Computers`. Right click or double click the admin user to view and edit the properties.



Administrator

Description: Built-in account for administering the computer/doma

Auditing

This section will look at the use of auditing in Windows to enhance the security and manageability of the network.

What is Auditing

The aim of auditing settings is to identify attacks that are both successful and not, that could be a threat to your device and/or network.

For example, identifying successful and failed logins can help identify when a user has accessed their account to identify a suspicious login outside of known logins as well as attempts to hack into the account logged as failed attempts.

By default, all auditing tools are disabled when first installed and if you are considering using these tools, they will need to be enabled.

The event categories that you can choose to audit are:

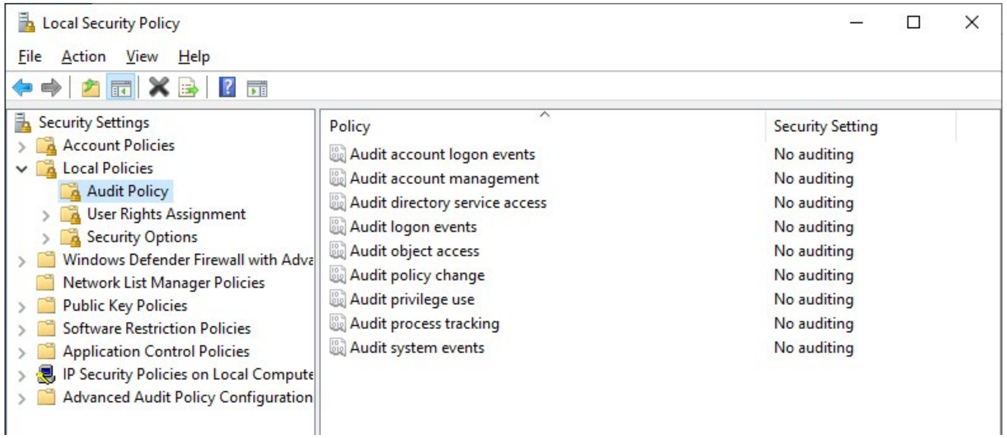
- Audit account logon events
- Audit account management
- Audit directory service access
- Audit logon events
- Audit object access
- Audit policy change
- Audit privilege use
- Audit process tracking
- Audit system events

How to enable/edit auditing policies

Open **Local Security Policy** by searching for in the program search area.

Locate the **Audit Policy** within the **Local Policies** area.

As you can see from the image below, all the settings are disabled, and no auditing is taking place as default.



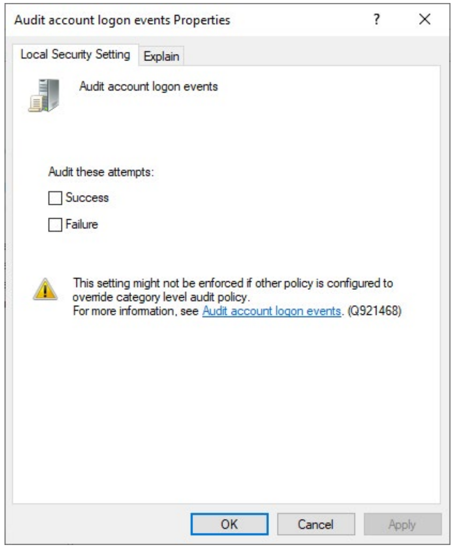
Security Settings
- Account Policies
- Local Policies
  - Audit Policy
  - User Rights Assignment
  - Security Options
- Windows Defender Firewall with Adva
- Network List Manager Policies
- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Local Compute
- Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

Let's look at one of the policies, **Audit account logon events**. To access the settings, double click or right click and select properties.

You are now presented with the options for this audit, to create a log of success or failure attempts to login.

For security purposes you may want to just capture when a failed attempt has been made and this may show when someone is trying to hack into the users account.



Audit account logon events

Audit these attempts:

☐ Success

☐ Failure

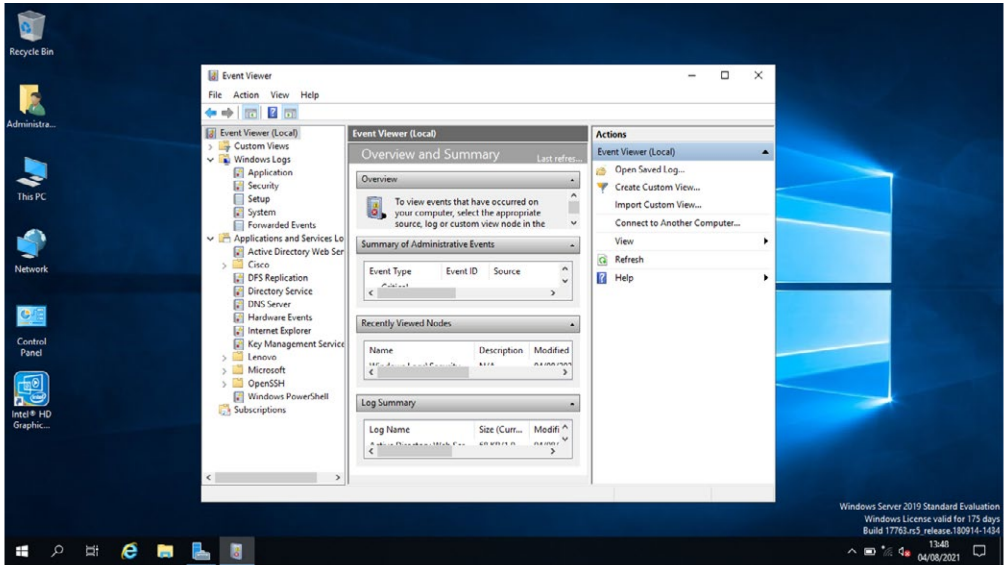
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit account logon events. (Q921468)

Or you may want all to allow a trail of when the account was used in case a user's account has been compromised and it can then be seen when it was used outside the users own use.

There is an **`explain`** tab on the pop-up window also that offers further guidance on the setting/policy to aid the correct use.

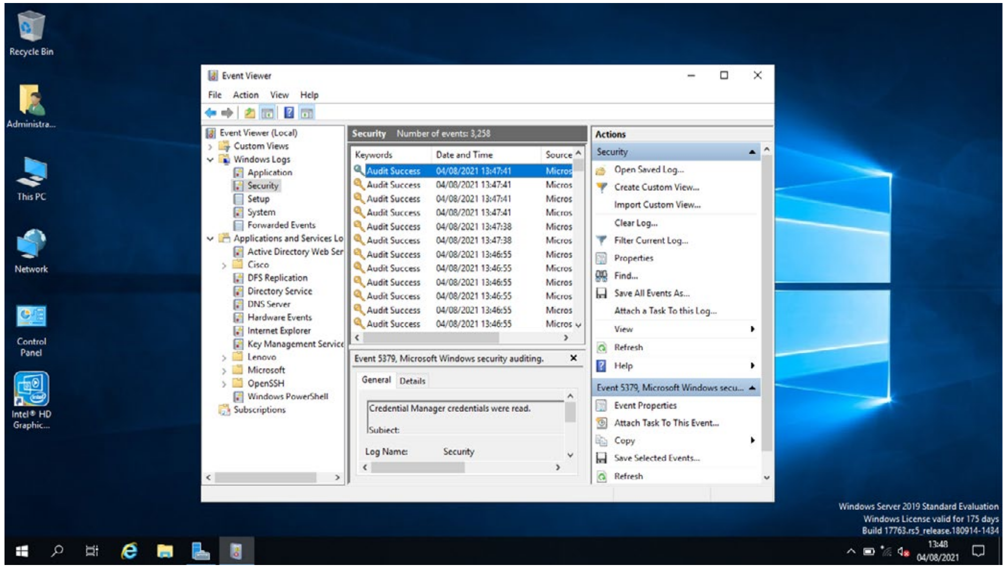
To view an audit, you need to open **`Event Viewer`**.

You can create specific logs, view, and create a saved log and create custom views on the main area.



To view events that have occurred on your computer, select the appropriate source, log or custom view node in the

Under **`Windows Logs / Security`** you can view all data gathered through the audit process.



Security Number of events: 3,258

Keywords	Date and Time	Source
Audit Success	04/08/2021 13:47:41	Micros
Audit Success	04/08/2021 13:47:41	Micros
Audit Success	04/08/2021 13:47:41	Micros
Audit Success	04/08/2021 13:47:41	Micros
Audit Success	04/08/2021 13:47:38	Micros
Audit Success	04/08/2021 13:47:38	Micros
Audit Success	04/08/2021 13:46:55	Micros
Audit Success	04/08/2021 13:46:55	Micros
Audit Success	04/08/2021 13:46:55	Micros
Audit Success	04/08/2021 13:46:55	Micros
Audit Success	04/08/2021 13:46:55	Micros
Audit Success	04/08/2021 13:46:55	Micros

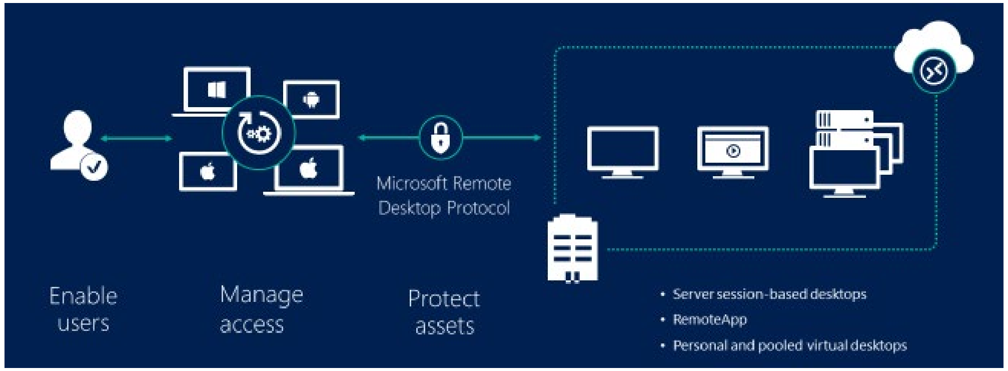
Event 5379, Microsoft Windows security auditing.

Credential Manager credentials were read.

Subject:

Log Name: Security

Remote Desktop Services (RDS)


Enable users
Manage access
Microsoft Remote Desktop Protocol
Protect assets
• Server session-based desktops
• RemoteApp
• Personal and pooled virtual desktops

What are remote desktop services

The use of remote desktop services allows you to connect to and control the device from a remote your device from another through a remote connection.

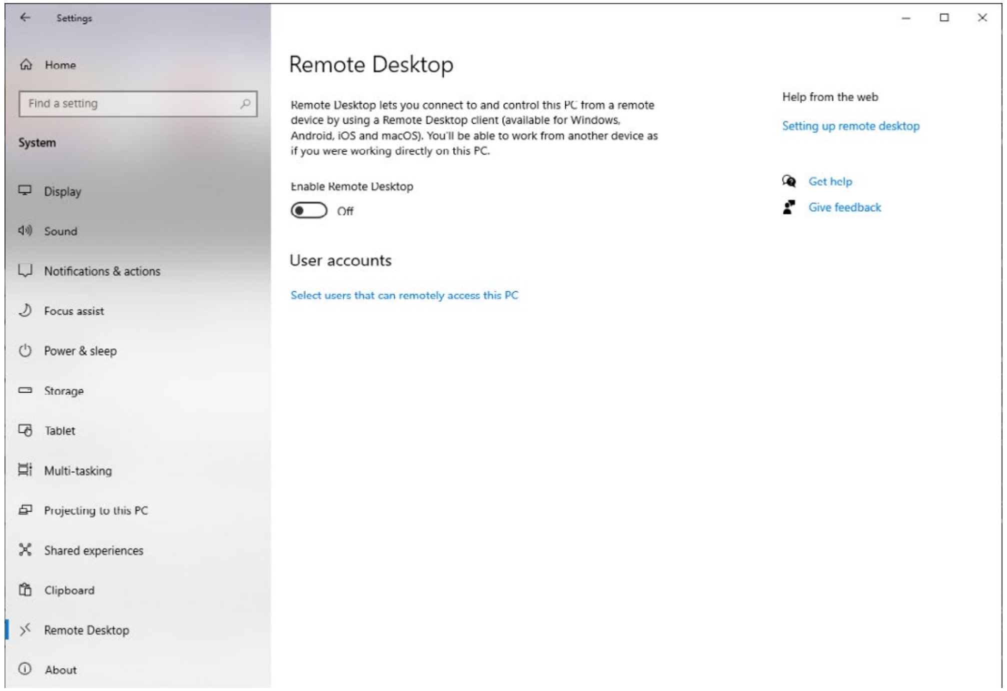
Why are they a security risk

Let us consider what would be a security risk of having one device controlling another. If you give remote desktop access to an additional device and that device is accessed, they then have access to not only the device they have accessed but also the remotely connected device too.

How to enable/disable remote desktop services

To enable the remote desktop that is disabled as default, open the `Settings / System / Remote Desktop`.

You will see the option to turn this on and off.



Remote Desktop

Remote Desktop lets you connect to and control this PC from a remote device by using a Remote Desktop client (available for Windows, Android, iOS and macOS). You'll be able to work from another device as if you were working directly on this PC.

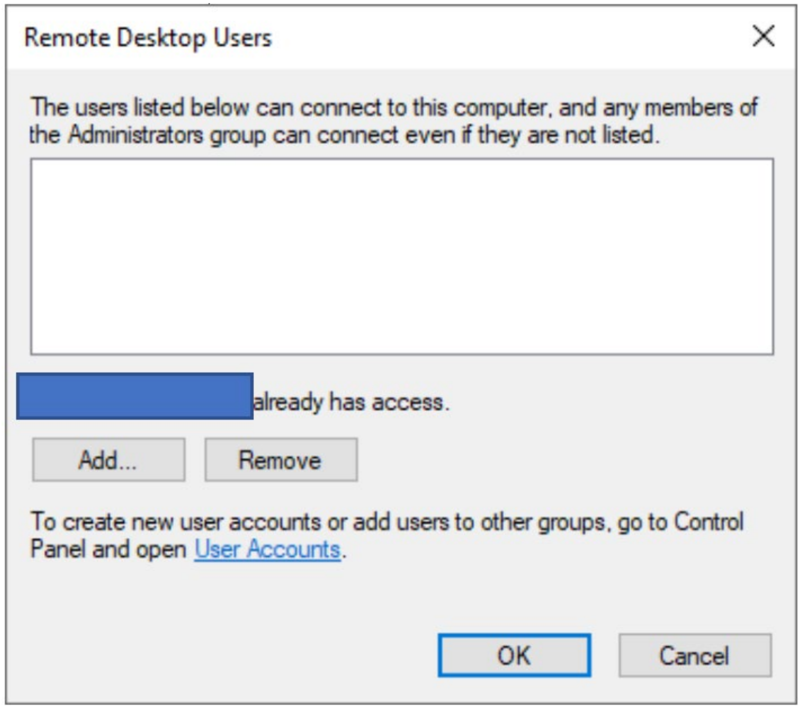
Enable Remote Desktop

Off

User accounts

Select users that can remotely access this PC

By clicking on the Select users that can remotely access this PC you will see a pop up where you can add user details to add.



Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

[redacted] already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

File Transfer Protocol (FTP) services

What is FTP

The file transfer protocol sets the rules for sending files over the internet and on Windows by default is switched off if you switch it on the files are transferred decrypted.

This is usually on port 21 and if you use this the firewall may need to be enabled to allow it through.

Why is it a security risk

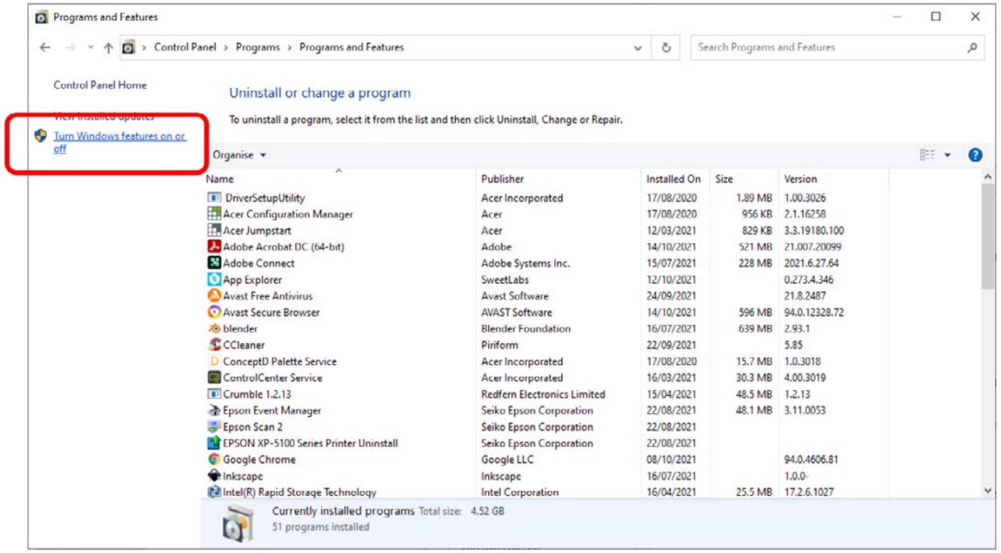
Turning it on means sending files decrypted over the internet which also poses the risk of being intercepted and read as they are fully accessible without encryption.

This is usually on port 21 and if you use this the firewall may need to be enabled to allow it through.

How to enable/disable FTP services

To access and enable the FTP services you need to open the **`Control Panel / Programs / Programs and Features`**

On the left-hand side select the **`Turn Windows features on or off`** option.



Programs and Features

Control Panel › Programs › Programs and Features

Search Programs and Features

Control Panel Home

View installed updates

Turn Windows features on or off

Uninstall or change a program

To uninstall a program, select it from the list and then click Uninstall, Change or Repair.

Organise ▾

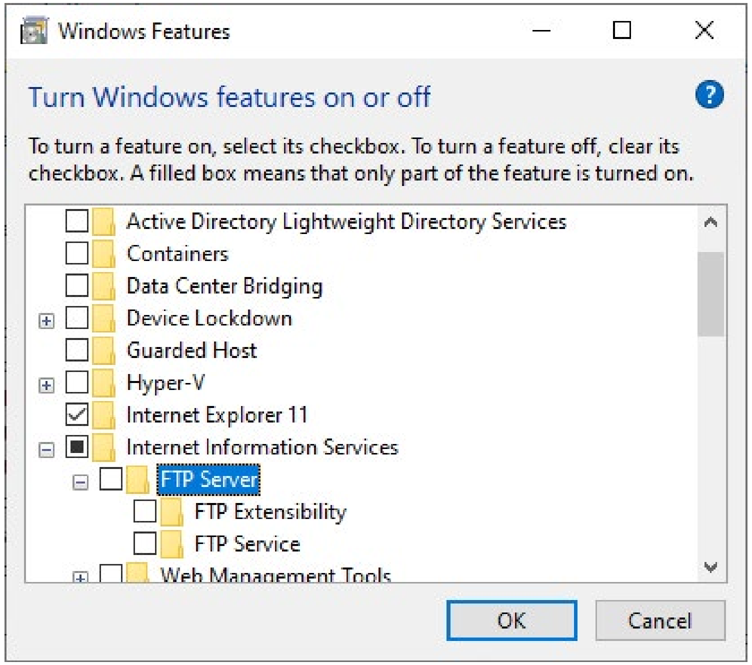
Name	Publisher	Installed On	Size	Version
DriverSetupUtility	Acer Incorporated	17/08/2020	1.89 MB	1.00.3026
Acer Configuration Manager	Acer	17/08/2020	956 KB	2.1.16258
Acer Jumpstart	Acer	12/03/2021	829 KB	3.3.19180.100
Adobe Acrobat DC (64-bit)	Adobe	14/10/2021	521 MB	21.007.20099
Adobe Connect	Adobe Systems Inc.	15/07/2021	228 MB	2021.6.27.64
App Explorer	SweetLabs	12/10/2021		0.273.4.346
Avast Free Antivirus	Avast Software	24/09/2021		21.8.2487
Avast Secure Browser	AVAST Software	14/10/2021	596 MB	94.0.12328.72
blender	Blender Foundation	16/07/2021	639 MB	2.93.1
CCleaner	Piriform	22/09/2021		5.85
ConceptD Palette Service	Acer Incorporated	17/08/2020	15.7 MB	1.0.3018
ControlCenter Service	Acer Incorporated	16/03/2021	30.3 MB	4.00.3019
Crumble 1.2.13	Redfern Electronics Limited	15/04/2021	48.5 MB	1.2.13
Epson Event Manager	Seiko Epson Corporation	22/08/2021	48.1 MB	3.11.0053
Epson Scan 2	Seiko Epson Corporation	22/08/2021		
EPSON XP-5100 Series Printer Uninstall	Seiko Epson Corporation	22/08/2021		
Google Chrome	Google LLC	08/10/2021		94.0.4606.81
Inkscape	Inkscape	16/07/2021		1.0.0-
Intel(R) Rapid Storage Technology	Intel Corporation	16/04/2021	25.5 MB	17.2.6.1027

Currently installed programs Total size: 4.52 GB

51 programs installed

You will then have a pop-up window with lots of Windows's features to turn on and off by checking the relevant box next to the heading.

Locate the folder **`Internet Information Services`** and click the plus sign to open the folders within. The FTP server is one option here to select as well as two folders within. To turn on add a tick to the checkbox next to the FTP Server.



Windows Features

Turn Windows features on or off

To turn a feature on, select its checkbox. To turn a feature off, clear its checkbox. A filled box means that only part of the feature is turned on.

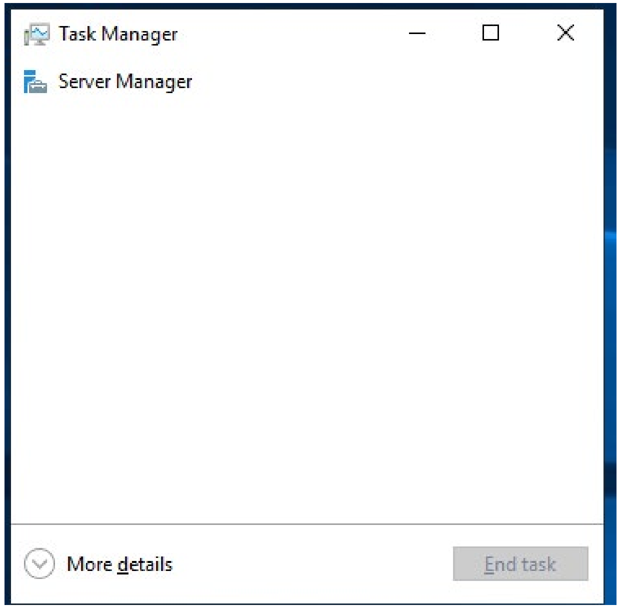
- □ Active Directory Lightweight Directory Services
- □ Containers
- □ Data Center Bridging
- ⊞ □ Device Lockdown
- □ Guarded Host
- ⊞ □ Hyper-V
- ☑ Internet Explorer 11
- ⊟ ■ Internet Information Services
  - ⊟ □ FTP Server
    - □ FTP Extensibility
    - □ FTP Service
  - ⊞ □ Web Management Tools

Task Manager

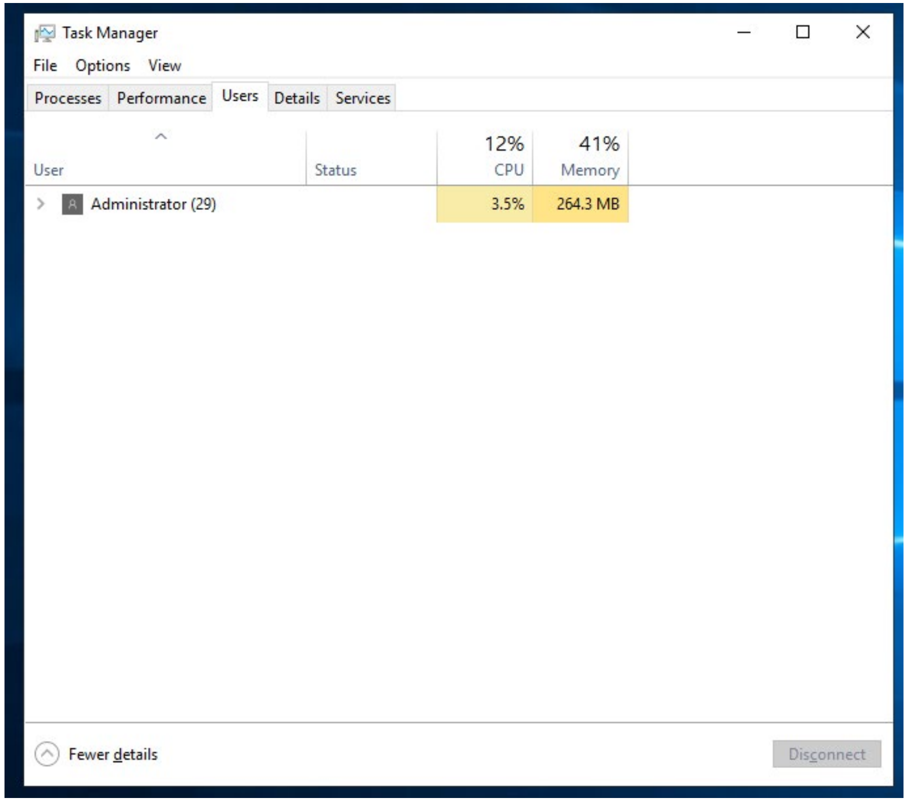
The task manager is used to identify what is currently being run on the device as well as stopping applications or actions being run instantly.

To access `Task Manager` search for it in the programs search area.

You can select `More details` to view the `Process`, `Performance`, `App history`, `Startup`, `Users`, `Details and Services`.



You can also see the users that are logged in on the `Users` tab and see the memory being used.



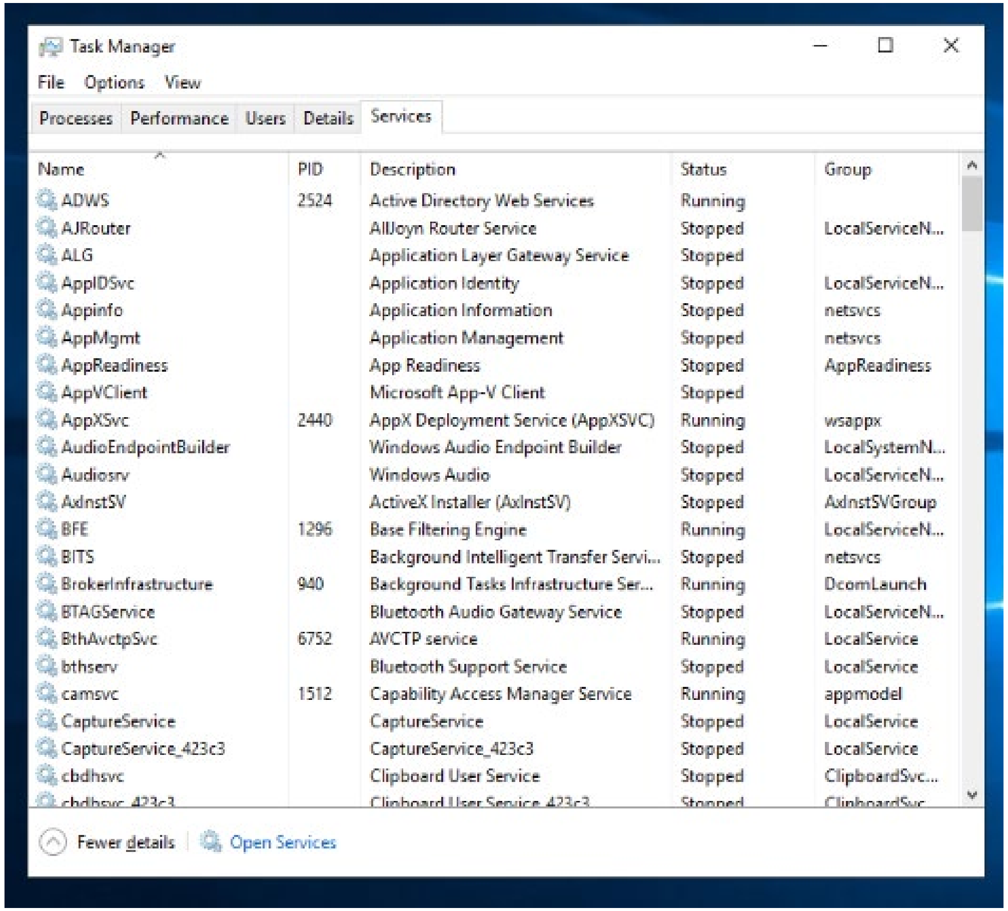
User	Status	12% CPU	41% Memory
Administrator (29)		3.5%	264.3 MB

Services

If you select the **Services** tab you are presented with the view on the right:

Here you can view all the services running and stopped on the device. You can right click to **Start, Stop, Open Services and Search Online**.

If anything looks suspicious or you are unsure what it is there for, do not just end the task as you may find it is an essential tool for running the computer. Instead, right click and select **Search online**. It will open a web browser and search for the file and give you advice on what the process or application is.



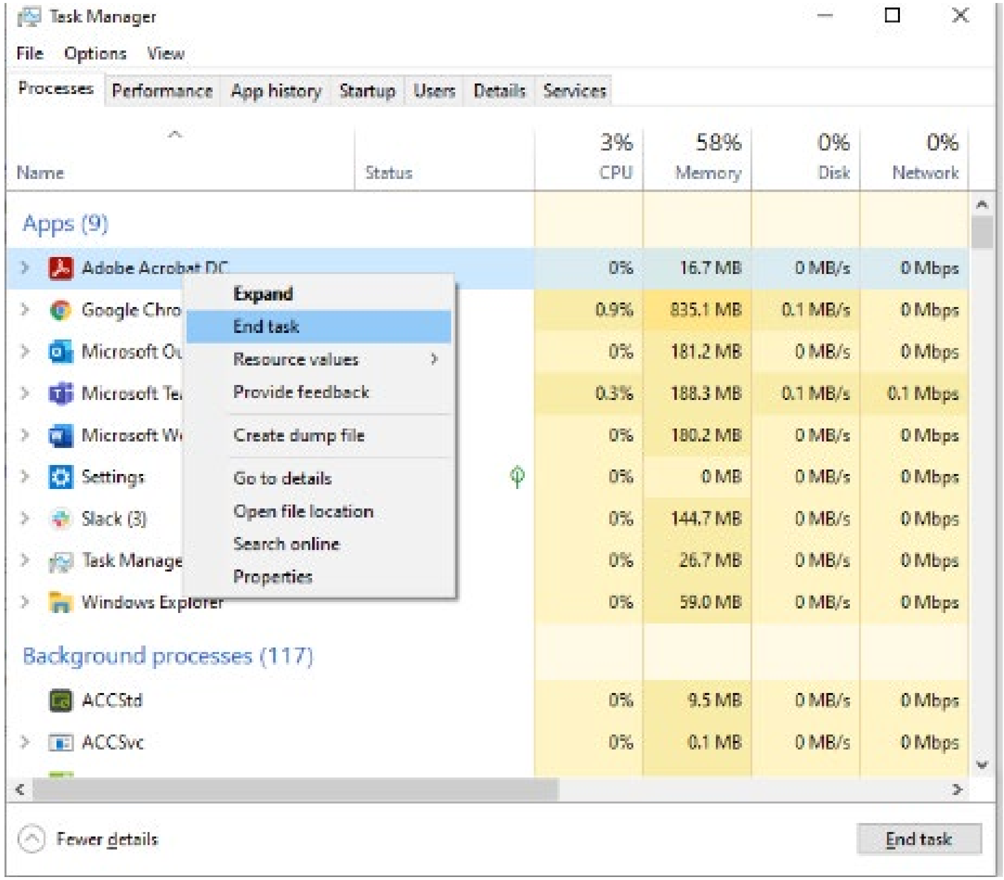
Name	PID	Description	Status	Group
ADWS	2524	Active Directory Web Services	Running	
AJRouter		AllJoyn Router Service	Stopped	LocalServiceN...
ALG		Application Layer Gateway Service	Stopped	
AppIDSvc		Application Identity	Stopped	LocalServiceN...
Appinfo		Application Information	Stopped	netsvcs
AppMgmt		Application Management	Stopped	netsvcs
AppReadiness		App Readiness	Stopped	AppReadiness
AppVClient		Microsoft App-V Client	Stopped	
AppXSvc	2440	AppX Deployment Service (AppXSVC)	Running	wsappx
AudioEndpointBuilder		Windows Audio Endpoint Builder	Stopped	LocalSystemN...
Audiosrv		Windows Audio	Stopped	LocalServiceN...
AxInstSV		ActiveX Installer (AxInstSV)	Stopped	AxInstSVGroup
BFE	1296	Base Filtering Engine	Running	LocalServiceN...
BITS		Background Intelligent Transfer Servi...	Stopped	netsvcs
BrokerInfrastructure	940	Background Tasks Infrastructure Ser...	Running	DcomLaunch
BTAGService		Bluetooth Audio Gateway Service	Stopped	LocalServiceN...
BthAvctpSvc	6752	AVCTP service	Running	LocalService
bthserv		Bluetooth Support Service	Stopped	LocalService
camsvc	1512	Capability Access Manager Service	Running	appmodel
CaptureService		CaptureService	Stopped	LocalService
CaptureService_423c3		CaptureService_423c3	Stopped	LocalService
cbdhsvc		Clipboard User Service	Stopped	ClipboardSvc...
cbdhsvc_423c3		Clipboard User Service_423c3	Stopped	ClipboardSvc

How to stop a running service

When you first open **Task Manager**, you are presented with a list of running applications. You can simply click on and select **End Task** to stop the application or action running. If you select **More details**, you can access the process and services tabs that are running and use right click and **end task** to terminate the selected process or service.

As previously mentioned, if you are unsure, it is best to right click and select **Search online**, to be sure before ending a process, application or service that is essential to the running of the device.

Cyber Security fact:
If something looks suspicious or is using a large amount of memory, it is worth investigating to ensure it is not a malicious service running on the system



Name	Status	3% CPU	58% Memory	0% Disk	0% Network
Apps (9)					
Adobe Acrobat DC		0%	16.7 MB	0 MB/s	0 Mbps
Google Chro		0.9%	835.1 MB	0.1 MB/s	0 Mbps
Microsoft Ou		0%	181.2 MB	0 MB/s	0 Mbps
Microsoft Te		0.3%	188.3 MB	0.1 MB/s	0.1 Mbps
Microsoft W		0%	180.2 MB	0 MB/s	0 Mbps
Settings		0%	0 MB	0 MB/s	0 Mbps
Slack (3)		0%	144.7 MB	0 MB/s	0 Mbps
Task Manage		0%	26.7 MB	0 MB/s	0 Mbps
Windows Explorer		0%	59.0 MB	0 MB/s	0 Mbps
Background processes (117)					
ACCStd		0%	9.5 MB	0 MB/s	0 Mbps
ACCSvc		0%	0.1 MB	0 MB/s	0 Mbps

Useful links

- https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks
- https://www.ncsc.gov.uk/section/advice-guidance/all-topics
- https://docs.microsoft.com/en-us/windows/security/threat-protection/