

Windows Basics Crash Course (Week 6 Image Review)

By Miseok Kim

Run Commands

- Local Users and Groups
- Control Panel
- Programs and Features
- Local Security Policy
- Local Group Policy Editor
- Services
- Shared Folders
- lusrmgr.msc
- control
- appwiz.cpl
- secpol.msc
- gpedit.msc
- services.msc
- fsmgmt.msc

What are the FIRST things you must always do?

1. READ THE README!!!

2. CHECK ALL FORENSICS
QUESTIONS!!!

Forensics 1 Answer

What is the hidden message in clue.txt?

1. Open clue.txt
2. ZG1kIHlvdSBjaGVjayBmb3lgaGlkZGVuIGZvbGRlcnMgeWV0PyA=
 - a. Testing knowledge of ciphers
 - b. <http://rumkin.com/tools/cipher/>
3. Recognize that the encoded message is Base64 cipher and paste it into a decoder

Answer:

Decrypt ▼

ZG1kIHlvdSBjaGVjayBmb3lgaGlkZGVuIGZvbGRlcnMgeWV0PyA=

This is your encoded or decoded text:

did you check for hidden folders yet?

Hmmmm...
HINT HINT
HINT :-)

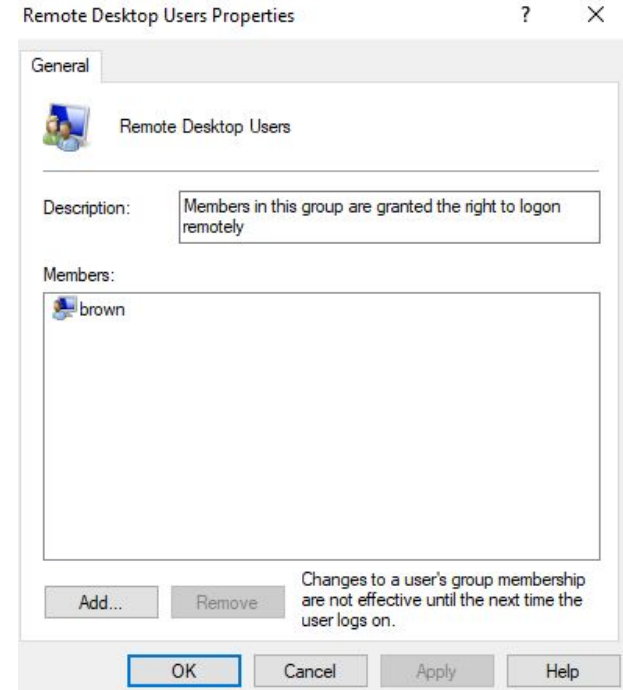
Forensics 2

Who is the user that has an unauthorized access to a group?

1. Open **Local Users and Groups**
2. Open **Groups**
3. Click on each group and check its members

Answer: **brown**

(Remote Desktop Users)

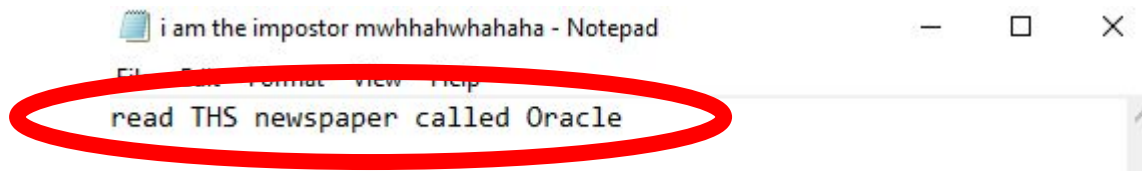


Forensics 3

What is the message from the impostor among us?

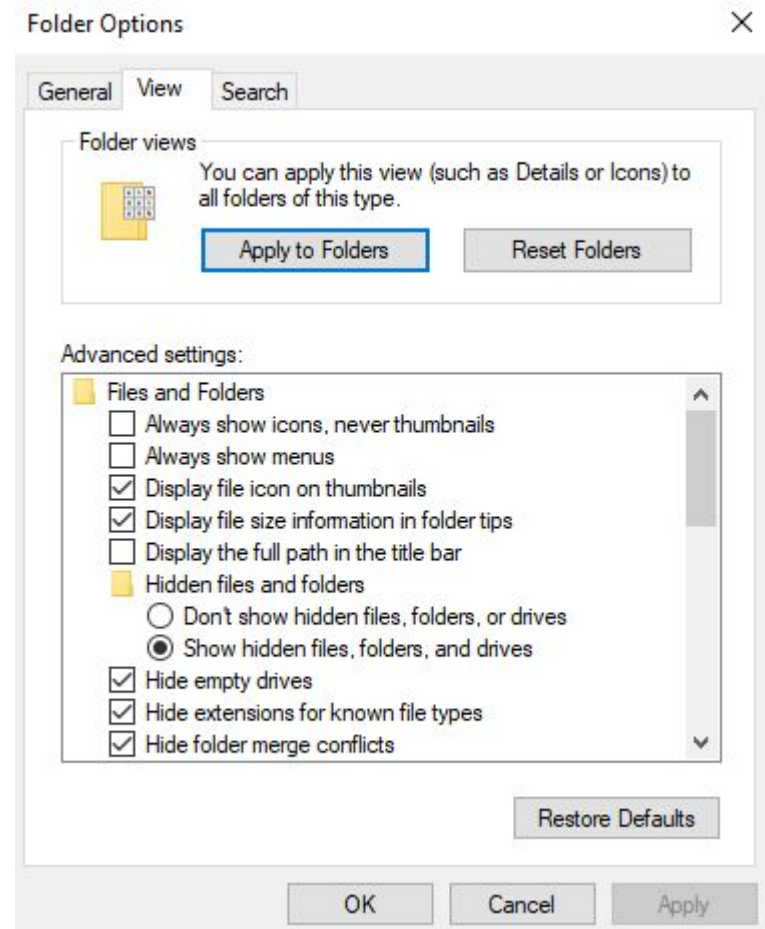
1. Open **Users** folder in the C: drive
2. Make sure hidden folders are shown
3. Go through each user folder and check for suspicious folders or files

Answer: red > Desktop > hidden folder "secret" > i am the impostor
mwhhahwhahaha



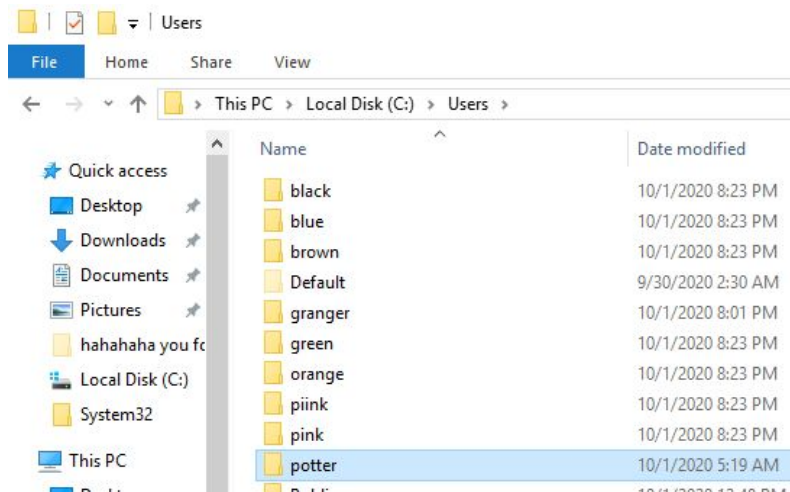
Show hidden folders

1. Click on **View** tab
2. Click on **Options**
3. Click on **View** tab in **Folder Options**.
4. Scroll in **Advanced settings**
5. Select **Show hidden files, folders, and drives**
6. Click **Apply**



Find and delete prohibited media file

- Prohibited media file = .jpg, .png, .gif, .wav, .mp3, .mp4, .mov
 - 99.99 % of the time > hidden
 - Usually in a user's folder, but could be in other folders in the C: drive
1. Manually search through different users' folders or use Everything tool

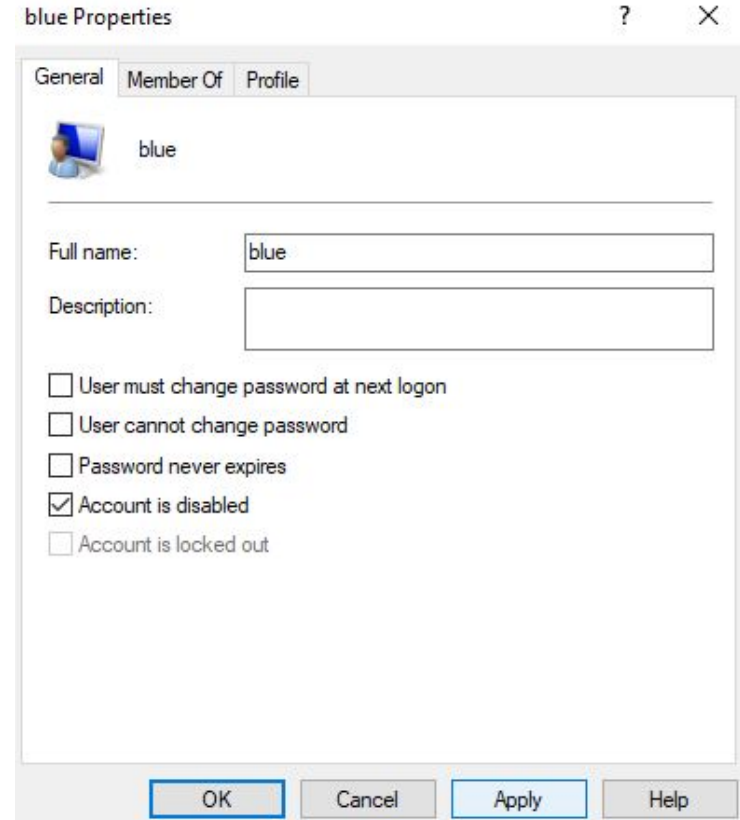


Answer: potter > Pictures > hahahaha you found it > BTS.jpg > Delete file



Disable a user

- Never delete users!
 - Always disable **Administrator** and **Guest** accounts
 - Disable any unauthorized user
1. Right-click on the user
 2. Check **Account is disabled**
 3. Click **Apply**



Every user should have a secure password

Method 1: Local Users and Groups

1. Right-click on an user.
2. Select **Set Password...**
3. Make sure the new password is secure.
4. Click **OK** to confirm

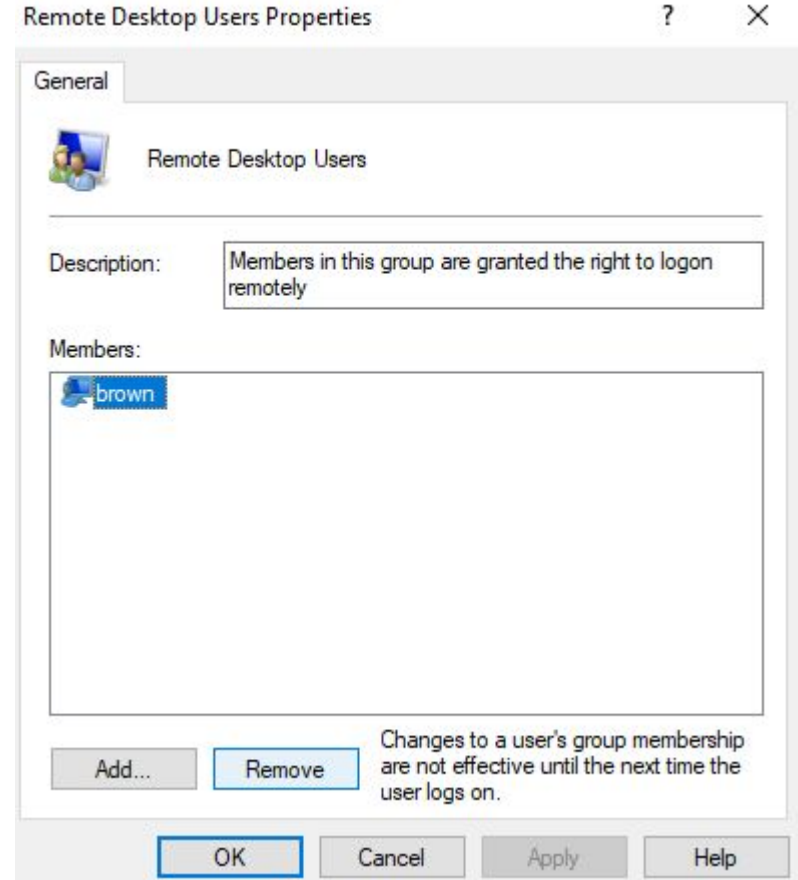


Method 2: Command prompt

1. Type **cmd** in search and select **run as administrator**
2. **net user [username] [password]**

Remove a user from a group

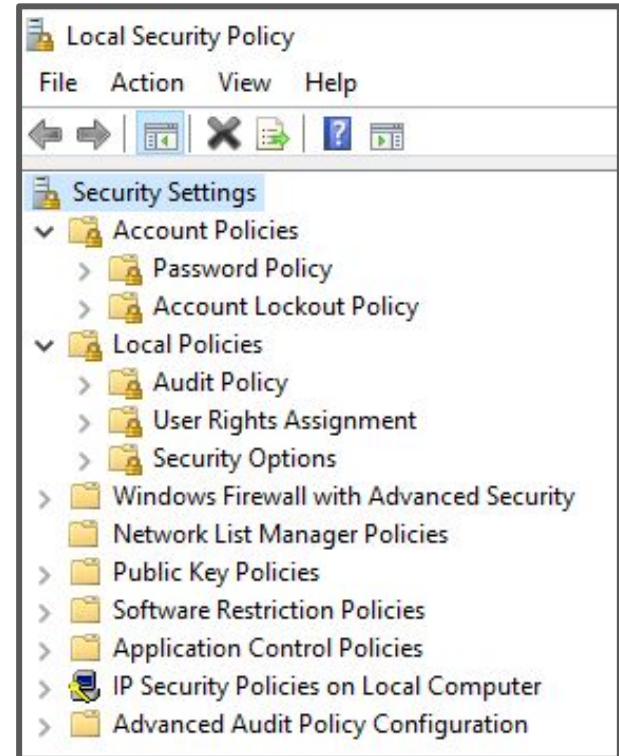
- Reasons?
 - User is not an admin
 - User should not be a member of a certain group
1. Click on the user
 2. Click **Remove**
 3. Click **Apply**



Local Policy - LOTS of points here!







What is the run command to open Local Security Policy?

- Account Policies
 - Password Policy
 - Account Lockout Policy
- Local Policies
 - Audit Policy
 - User Rights Assignment
 - Security Options





Password Policy

1. Enforce password history: 5 passwords remembered
2. Max password age: 90 days
3. Min password age: 30 days
4. Min password length 14 characters
5. Password must meet complexity requirements: Enabled
6. Store passwords using reversible encryption: Disabled










Policy	Security Setting
 Enforce password history	5 passwords remembered
 Maximum password age	90 days
 Minimum password age	30 days
 Minimum password length	14 characters
 Password must meet complexity requirements	Enabled
 Store passwords using reversible encryption	Disabled

Account Lockout Policy

1. Account lockout duration: 30 min
2. Account lockout threshold: 5 invalid logon attempts
3. Reset account lockout counter after: 30 min

Policy	Security Setting
 Account lockout duration	30 minutes
 Account lockout threshold	5 invalid logon attempts
 Reset account lockout counter after	30 minutes










Audit Policy











Policy	Security Setting
 Audit account logon events	Success, Failure
 Audit account management	Success, Failure
 Audit directory service access	Success, Failure
 Audit logon events	Success, Failure
 Audit object access	Success, Failure
 Audit policy change	Success, Failure
 Audit privilege use	Success, Failure
 Audit process tracking	Success, Failure
 Audit system events	Success, Failure

User Rights Assignment and Security Options

- List of optimal conditions are given during competition, but here is a list of suggested configurations

https://docs.google.com/spreadsheets/d/1j6E_liD7ImCv99Mi5h4oTRn-AqYuRlfagy2SNoCkKrU/edit?usp=sharing

Policy	Security Setting
 Access Credential Manager as a trusted caller	
 Access this computer from the network	Everyone,Administrators...
 Act as part of the operating system	
 Add workstations to domain	
 Adjust memory quotas for a process	LOCAL SERVICE,NETWO...
 Allow log on locally	Guest,Administrators,Us...
 Allow log on through Remote Desktop Services	Administrators,Remote ...
 Back up files and directories	Administrators,Backup ...
 Bypass traverse checking	Everyone,LOCAL SERVIC...

Policy	Security Setting
 Accounts: Administrator account status	Enabled
 Accounts: Block Microsoft accounts	Not Defined
 Accounts: Guest account status	Disabled
 Accounts: Limit local account use of blank passwords to co...	Enabled
 Accounts: Rename administrator account	Administrator
 Accounts: Rename guest account	Guest
 Audit: Audit the access of global system objects	Disabled
 Audit: Audit the use of Backup and Restore privilege	Disabled
 Audit: Force audit policy subcategory settings (Windows Vis...	Not Defined
 Audit: Shut down system immediately if unable to log secur...	Disabled

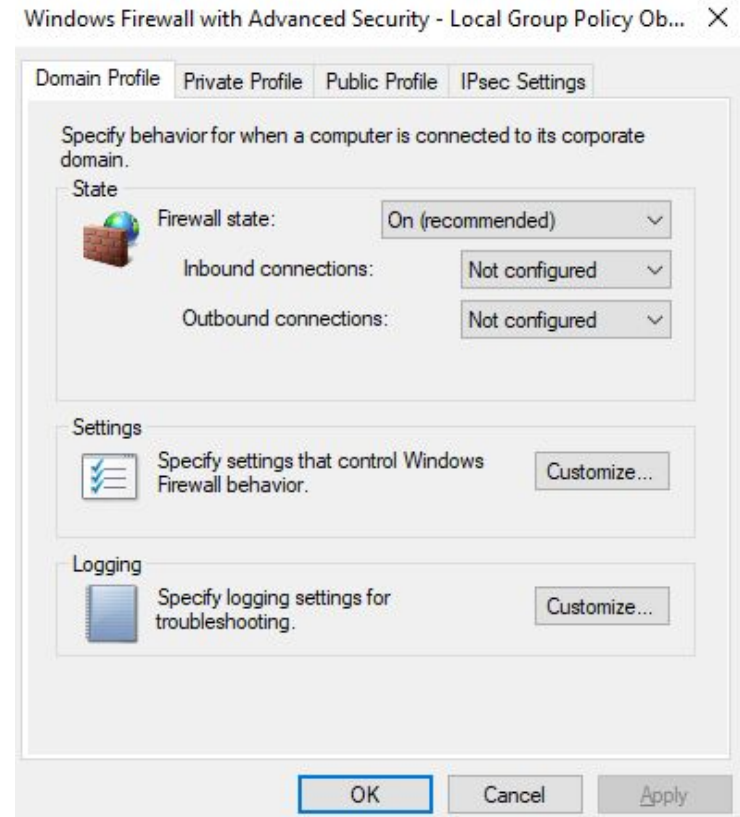
Enable Firewall - Control Panel

1. Use the run command
2. System Security > Windows Firewall
3. Click **Turn Windows Firewall on or off**
4. Select **Turn on Windows Firewall** for both private and public network settings.
5. Click **OK**



Enable Firewall - Windows Firewall with Advanced Security

1. Open either Local Security Policy or Group Policy.
2. Expand **Windows Firewall with Advanced Security** folder
3. Click **Windows Firewall Properties**
4. Select **On (recommended)** for all Firewall profiles (Domain, Private, and Public)
5. Don't forget to click **Apply**

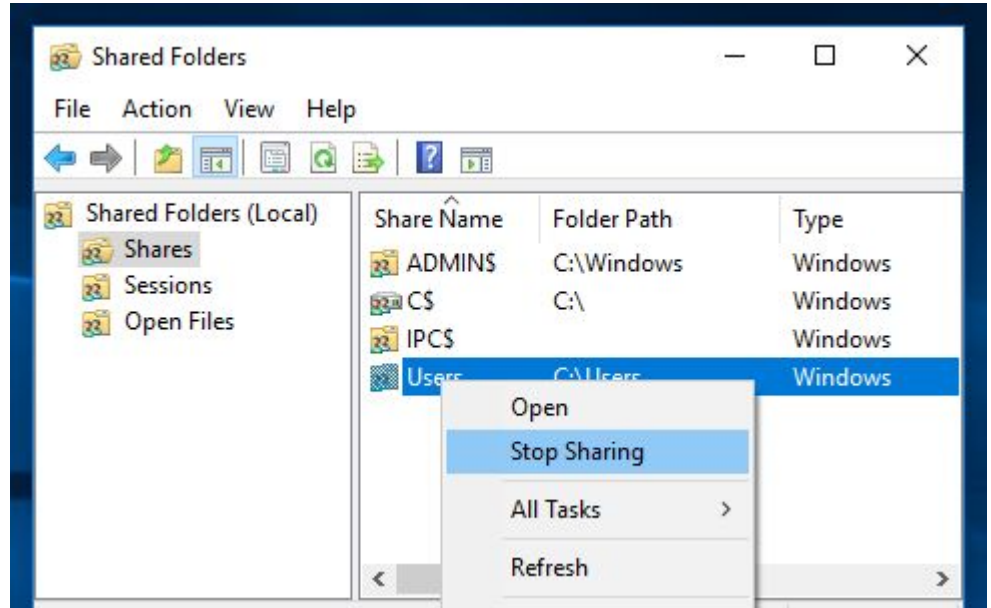


Shared Folders

- Unless the share is a default one, it should not be shared.
- What is the run command to access Shared Folders?
- How do you know if the share is a default one?
- Name three default shares.
 1. ADMIN\$
 2. C\$
 3. IPC\$

Stop sharing a folder

1. Right-click on the shared folder
2. Select **Stop Sharing**
3. Click **Yes**



Uninstall prohibited apps

- What is the run command to open **Programs and Features**?
- List of prohibited apps
 - Any app that allows remote connection/control (ex: Teamviewer)
 - Any gaming app
 - Any social media app
 - Any app not specified in the README







Uninstall prohibited apps (continued)

1. Right-click on an app
2. Click **Uninstall/change**

Uninstall or change a program

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

Organize ▾ Uninstall		☰ ☷ ▾	
Name	Publisher	Installed On	Size
 Everything 1.4.1.992 (x64)	voidtools	10/17/2020	3.00 MB
 Mozilla Firefox 81.0.1 (x64 en-US)	Mozilla	10/17/2020	201 MB
 Oracle VM VirtualBox Guest Additions 6.1.12	Oracle Corporation	9/30/2020	
 TeamViewer	TeamViewer	10/17/2020	100 MB

Uninstall

Update or install apps

- README sometimes specifies approved apps
 - Approved apps should always be in latest versions
- What are some of the approved apps?
 - Firefox
 - Depends on README (Notepad++, 7zip)



-
- [Installer](#) | [GPG Signature](#)
 - [Portable \(zip\)](#) | [GPG Signature](#)
 - [Portable \(7z\)](#) | [GPG Signature](#)

Services












1. Use the run command to open Services

List of services that must be disabled:

1. Remote Desktop
2. IP Helper
3. Telephony

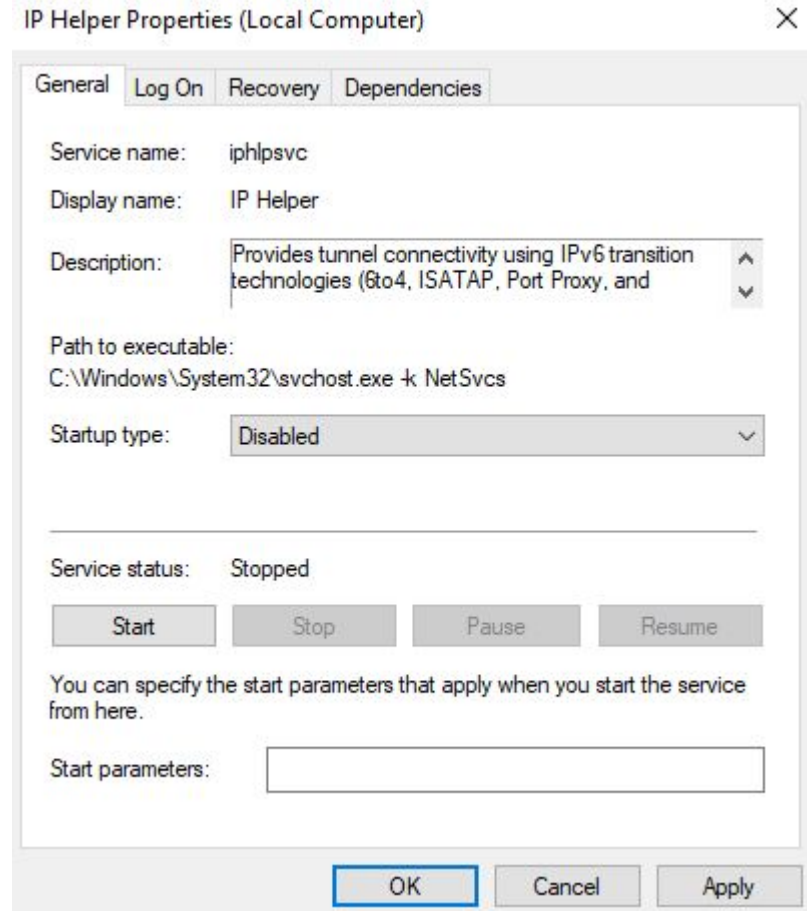
List of approved services:

1. Any default Windows services (Windows Firewall, Windows Updates, etc.)

	Windows Event Collector	This service ...		Manual
	Windows Event Log	This service ...	Running	Automatic
	Windows Firewall	Windows Fi...	Running	Automatic
	Windows Font Cache Service	Optimizes p...	Running	Automatic
	Windows Image Acquisitio...	Provides im...		Manual
	Windows Insider Service	wisvc		Manual
	Windows Installer	Adds, modi...		Manual
	Windows License Manager ...	Provides inf...	Running	Manual (Trig...
	Windows Management Inst...	Provides a c...	Running	Automatic
	Windows Media Player Net...	Shares Win...		Manual
	Windows Mobile Hotspot S...	Provides th...		Manual (Trig...

Stop and disable service

1. Right-click on the service
2. Select **Stop**
3. Open **Properties**
4. Select **Disabled** for Startup type
5. Click **Apply**

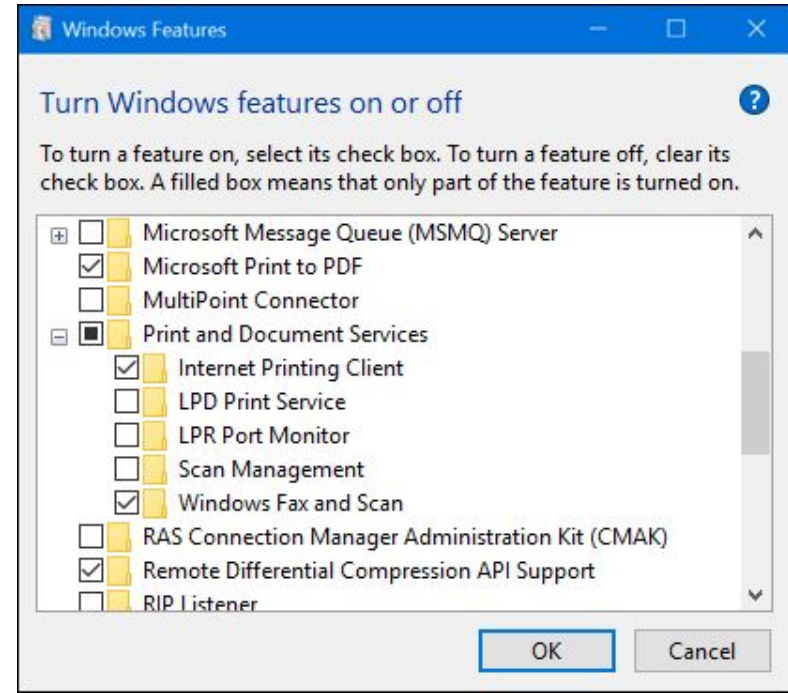


Disable Windows features

1. Open Programs and Features
2. Click **Turn Windows features on or off**
3. Uncheck or check as needed
4. Click **OK**

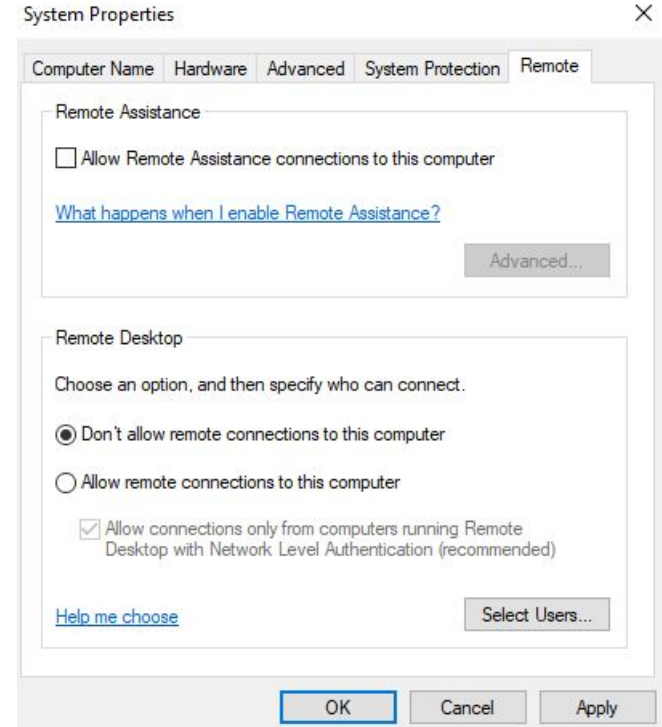
Approved Windows Features: Internet Explorer 11, advanced Windows features, anything specified in README

Disabled Windows Features: RIP Listener, Telnet Client



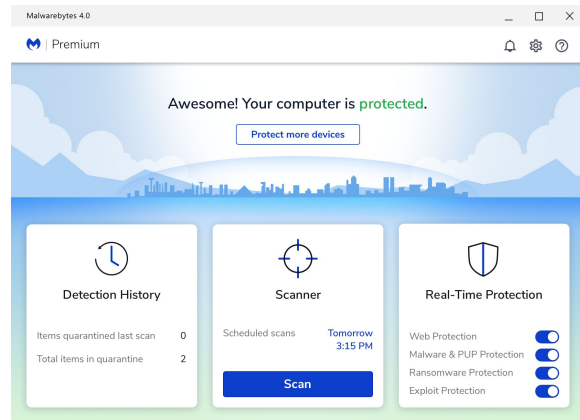
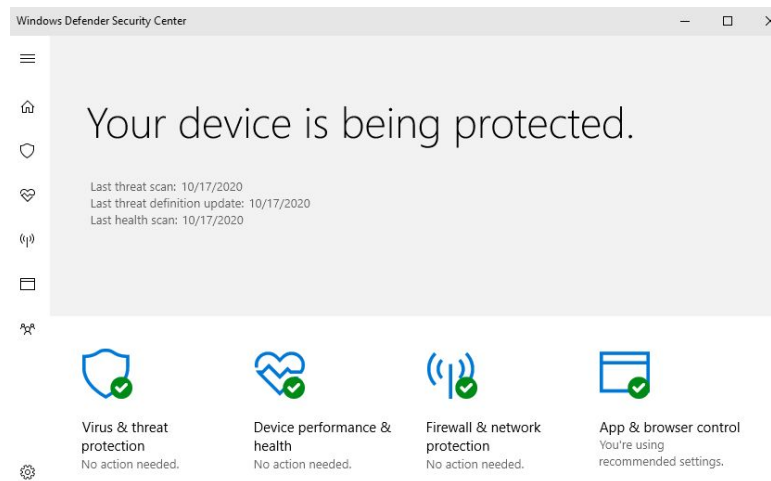
Remote Desktop

- Control Panel > System and Security >
System > Advanced system settings
1. Click on **Remote** tab
 2. Uncheck **Allow Remote Assistance connections to this computer**
 3. Click **Don't allow remote connections to this computer**
 4. Click **Apply**



Finding Malware

- Enable Windows Defender
 - Windows Settings > Update & security > Windows Defender
- Download and run third-party antimalware programs
 - Malwarebytes
 - Avast



Sigh Windows Updates...

- Good news! They are automatic in Windows 10
- Bad news...they take a loooooooooooooooooong time

1. Open Windows Settings
2. Open Update & security
3. Click Windows Update
4. Click **Restart now**

Windows Update

Update status



A restart is required to finish installing the following updates:

- Feature update to Windows 10, version 1903

[Update history](#)



Your device is scheduled to restart outside of active hours. (Active hours are 8:00 AM to 5:00 PM.)

Restart now