Security tips for working from home

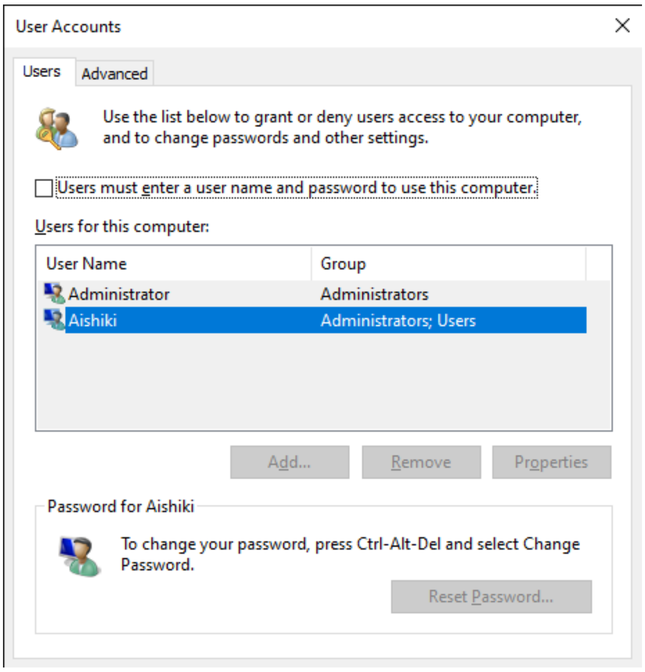
Social distancing is one of the key ways of limiting the spread of the COVID-19 (Coronavirus). This prompts various organisations to request their staff to work from home. However, the onrush to remote working may create additional cybersecurity threats. To overcome those additional cybersecurity threats please follow guidelines mentioned below.

1. Create a local user account

- Select the **Start** button, select **Settings** > **Accounts** and then select **Family & other users.** (In some editions of Windows you'll see **Other users**.)
- Select **Add someone else to this PC**.
- Select **I don't have this person's sign-in information**, and on the next page, select **Add a user without a Microsoft account**.
- Enter a user name, password, password hint or choose security questions, and then select **Next**.

2. Disable Automatic Login:

- Press **Win+R**, enter “**netplwiz**“, which will open the “**User Accounts**” window. Netplwiz is a Windows utility tool for managing user accounts.
- Check the option for “**Users must enter a username and password to use this computer**” and click **Apply**.
- That’s it. **Restart** your computer and the system will prompt you to enter your password at the login screen.



User Accounts

Use the list below to grant or deny users access to your computer, and to change passwords and other settings.

☐ Users must enter a user name and password to use this computer.

Users for this computer:

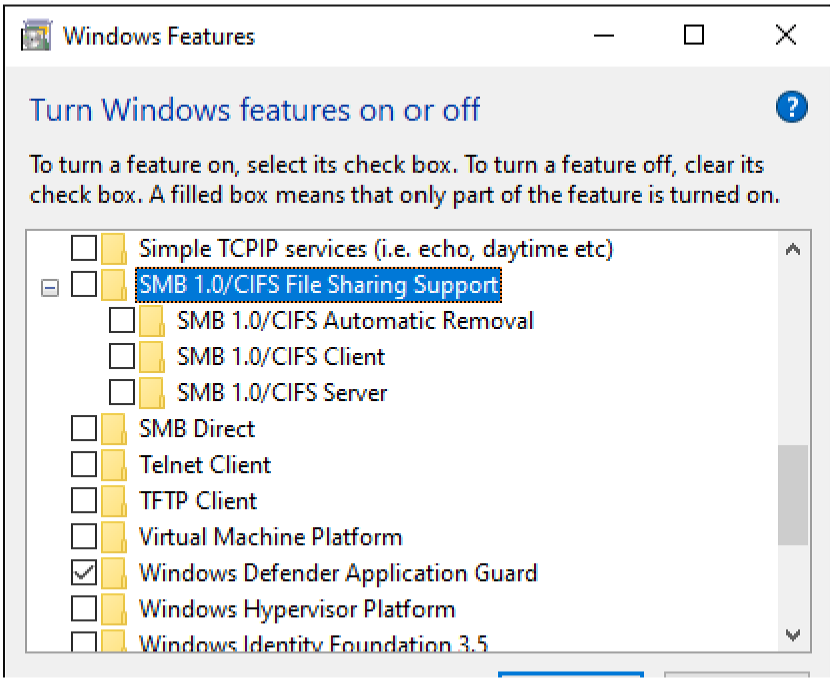
User Name	Group
Administrator	Administrators
Aishiki	Administrators; Users

Password for Aishiki

To change your password, press Ctrl-Alt-Del and select Change Password.

3. Disabling SMB On Windows 10: Windows Features Method

- Go to the "Control Panel"
- Select "Programs"
- Select "Programs and Features"
- Click on "Turn Windows features on or off" on the left panel
- "Windows features" window will appear
- Scroll down and uncheck both "SMB 1.0/CIFS File Sharing Support" & "SMB Direct"
- Click "Ok"



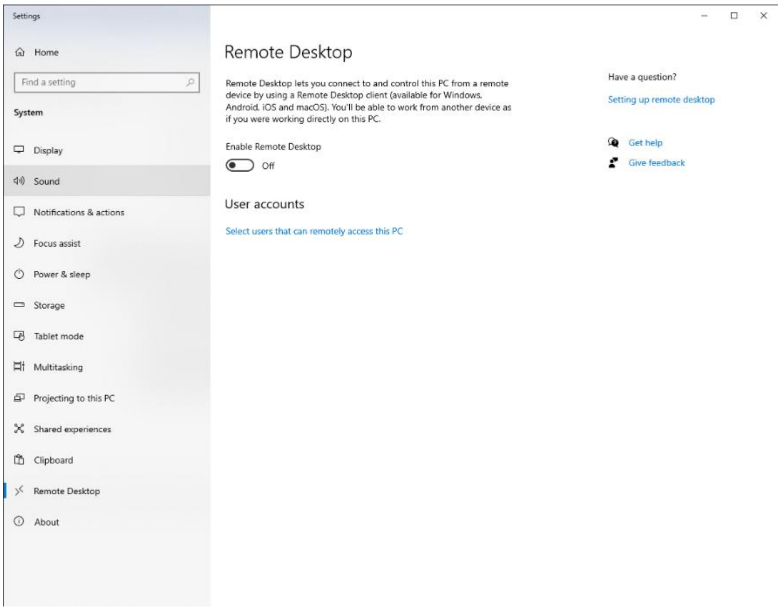
Turn Windows features on or off

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

- □ Simple TCPIP services (i.e. echo, daytime etc)
- □ SMB 1.0/CIFS File Sharing Support
  - □ SMB 1.0/CIFS Automatic Removal
  - □ SMB 1.0/CIFS Client
  - □ SMB 1.0/CIFS Server
- □ SMB Direct
- □ Telnet Client
- □ TFTP Client
- □ Virtual Machine Platform
- ☑ Windows Defender Application Guard
- □ Windows Hypervisor Platform
- □ Windows Identity Foundation 3.5

4. Disabling Remote Access in Windows 10

- **Type "remote desktop settings" in the "Cortana search box".** Select "Allow remote access to your computer". This may seem counter-intuitive, but this opens the Control panel dialog for Remote System Properties.
- **Toggle "Enable Remote Desktop"** switch to **Off** position. **You've** now disabled remote access to your computer.



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

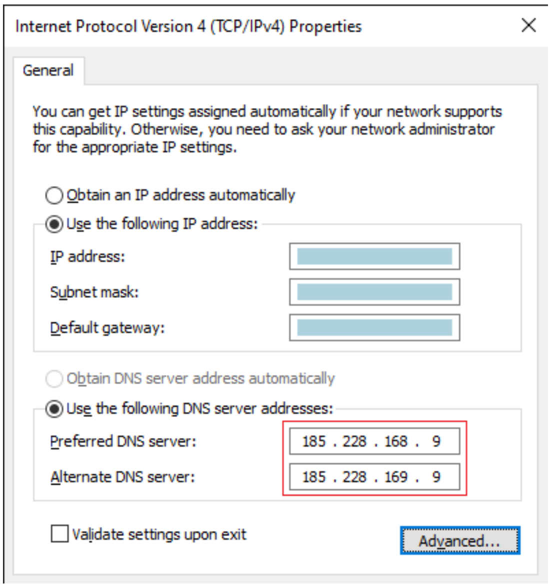
Select users that can remotely access this PC

5. Using DNS Based Content Filtering

Security Filter

This blocks access to phishing, malware and malicious domains. It does not block adult contents.

- **IPv4 address**: *185.228.168.9* and *185.228.169.9*
- **IPv6 address**: *2a0d:2a00:1::2* and *2a0d:2a00:2::2*



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address:
Subnet mask:
Default gateway:

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 185 . 228 . 168 . 9
Alternate DNS server: 185 . 228 . 169 . 9

□ Validate settings upon exit

6. Protect your device with Windows Security

If you have Windows 10, you’ll get the latest antivirus protection with Windows Security. When you run Windows 10 for the first time, Windows Security gets on and actively helps to protect your PC by scanning for malware (malicious software), viruses, and security threats. Windows Security provides real-time protection by scanning everything you download or run on your PC.

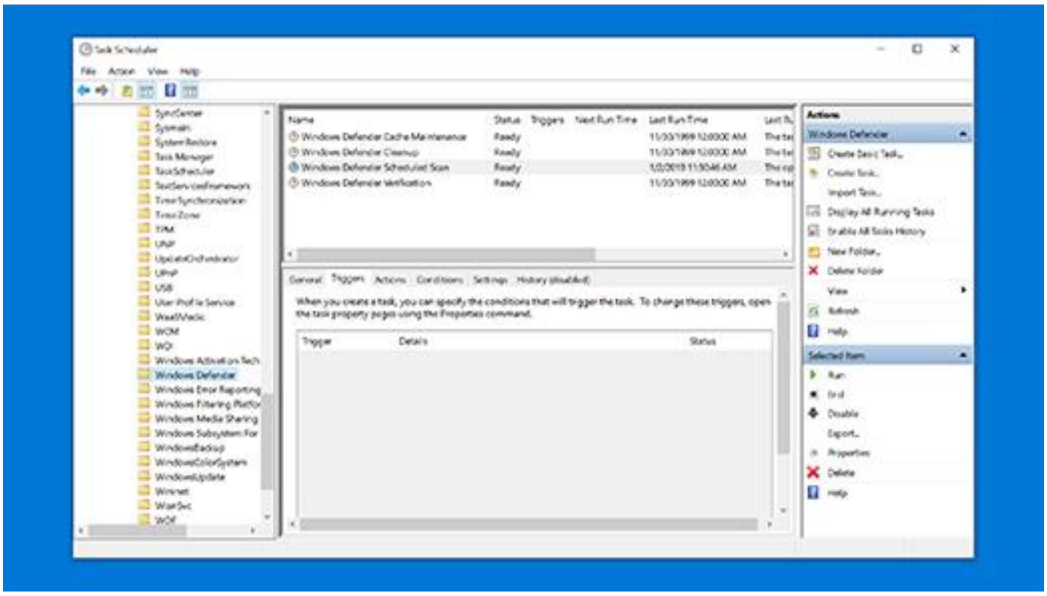
Windows Update downloads updates for Windows Security automatically to help keep your PC safe and protect it from threats.

If you have an earlier version of Windows and are using Microsoft Security Essentials, it is a good idea to move to Windows Security.

Schedule a scan in Windows Security

Windows Security regularly scans your PC to help keep it safe. If you want to set your own scan schedule:

1. In the search box on the taskbar, type **Task Scheduler** and then select **Task Scheduler** in the list of results.
2. In the left pane of Task Scheduler, expand **Task Scheduler Library** > **Microsoft** > **Windows** and then scroll down and double-click the **Windows Defender** folder.
3. In the top-center pane, double-click **Windows Defender Scheduled Scan**.
4. Select the **Triggers** tab, and then select **New**.
5. Set your time and frequency, and then select **OK**.



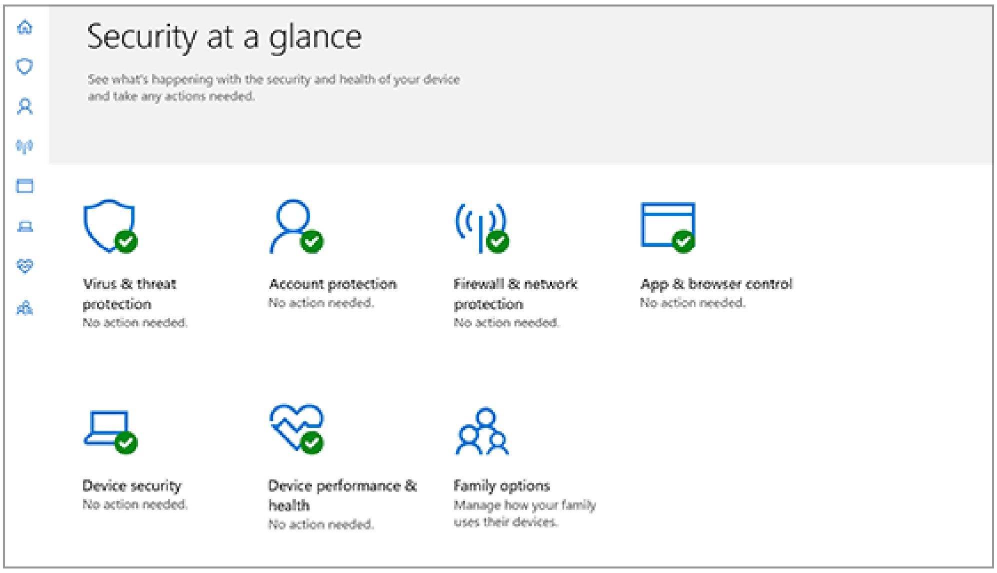
Name	Status	Triggers	Next Run Time	Last Run Time	Last Ru
Windows Defender Cache Maintenance	Ready			11/30/1999 12:00:00 AM	The tas
Windows Defender Cleanup	Ready			11/30/1999 12:00:00 AM	The tas
Windows Defender Scheduled Scan	Ready			1/2/2019 11:50:46 AM	The op
Windows Defender Verification	Ready			11/30/1999 12:00:00 AM	The tas

When you create a task, you can specify the conditions that will trigger the task. To change these triggers, open the task property pages using the Properties command.

Trigger	Details	Status

Turn Windows Security real-time protection on or off

- Select the **Start** button, then select **Settings** > **Update & Security** > **Windows Security** > **Virus & threat protection**.
- **Do one of the following:**
- In the current version of Windows 10: Under **Virus & threat protection settings**, select **Manage settings**, and then switch the **Real-time protection** setting to **On** or **Off**.
- In previous versions of Windows 10: Select **Virus & threat protection settings**, and then switch the **Real-time protection** setting to **On** or **Off**.



Security at a glance

See what's happening with the security and health of your device and take any actions needed.

Virus & threat protection
No action needed.

Account protection
No action needed.

Firewall & network protection
No action needed.

App & browser control
No action needed.

Device security
No action needed.

Device performance & health
No action needed.

Family options
Manage how your family uses their devices.