// Assignment 2

/ Managing a Network

// by George Hotten

// Interrogating the College Network

To get a list of all devices on my network, I will use a tool called Nmap. Using this, I can iterate through every possible IP address on the network to identify devices.

// My IP address

First, I will need to identify what my IP and subnet are. I can do this by running the following command in the terminal: `ip config /all`

```
Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : solihull.ac.uk
   Description . . . . . . . . . . . : Intel(R) Ethernet Connection (2) I219-V
   Physical Address. . . . . . . . . : 2C-F0-5D-06-EC-64
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::11d6:218a:5ac3:636f%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.20.52.109(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Lease Obtained. . . . . . . . . . : 01 November 2022 09:03:36
   Lease Expires . . . . . . . . . . : 02 November 2022 09:03:16
   Default Gateway . . . . . . . . . : 172.20.52.1
   DHCP Server . . . . . . . . . . . : 192.168.224.99
   DHCPv6 IAID . . . . . . . . . . . : 489484381
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-28-BF-E7-3E-2C-F0-5D-06-EC-64
   DNS Servers . . . . . . . . . . . : 192.168.224.99
                                       192.168.224.101
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

From this, I can see my IP address is 172.20.52.109. Based off our subnet mask, the IP address we will input into Nmap to scan every possible IP address withing the network is 172.20.52.0/23.

/ Our Hostname

To identify our hostname, we can simply run the `hostname` command within command prompt.

```
C:\Users\Net 2>hostname
DESKTOP-4OQ4NU2
```

Our hostname is DESKTOP-4OQ4NU2.

// Scanning the Network

To scan the network, and to obtain information about the type of device, we will use the following Nmap command: `nmap -T4 -A -v 172.20.52.0/23`. Let's break down what this means:

/ nmap – the application we are running

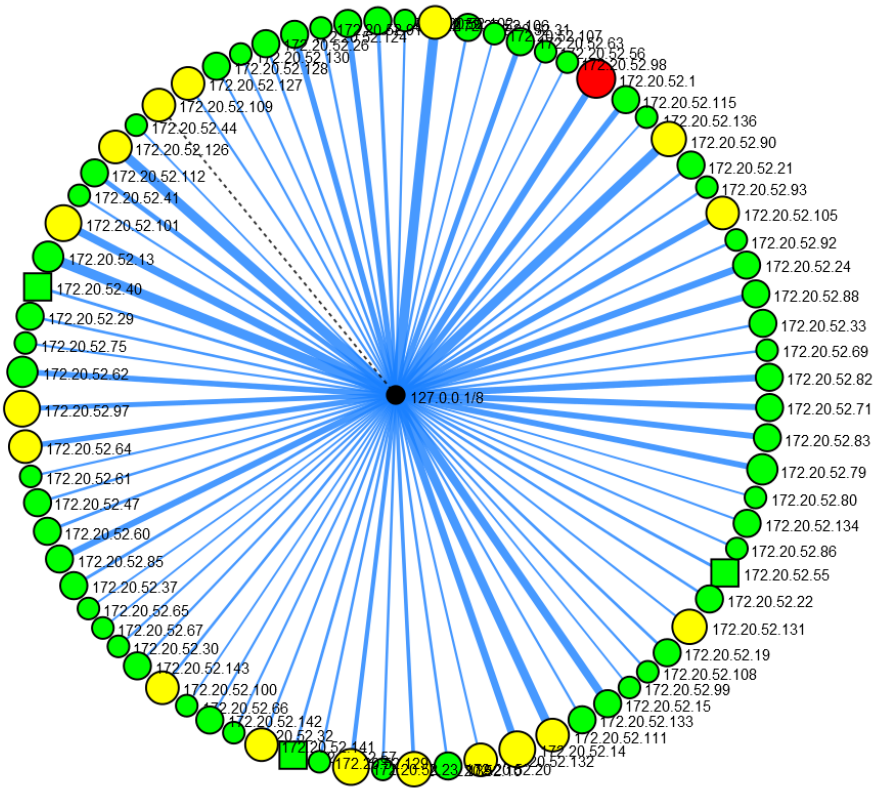
/ -T4 – set timing template

/ -A – enables OS detection, version detection, script scanning and tracert

/ -v – increases level of verbosity.

As some IP addresses from our IP config were from the subnet 192.168.224.0, I will run a scan on this too.

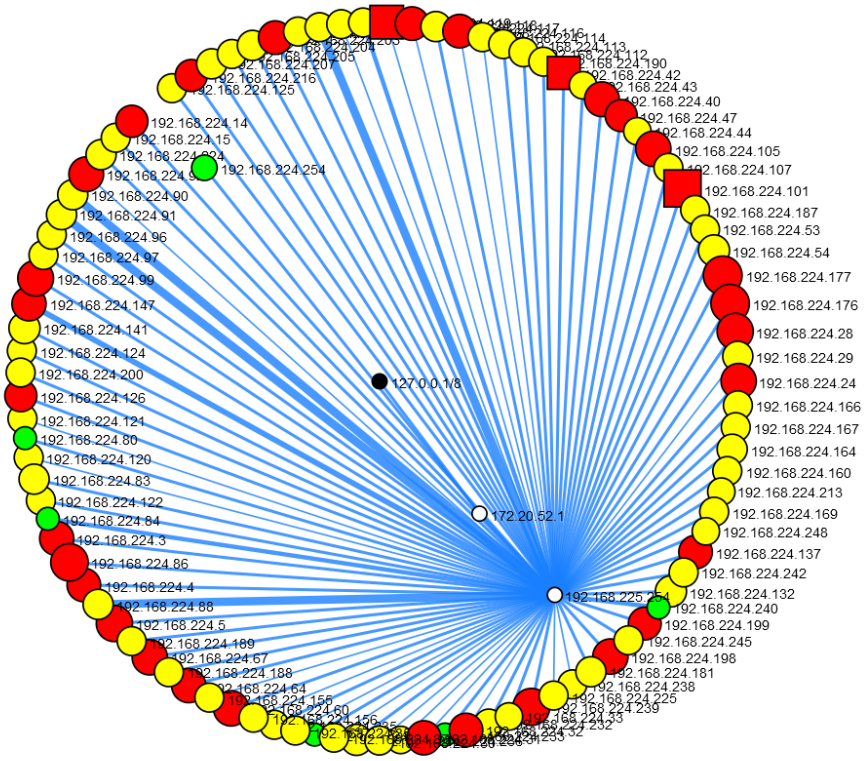
/ Devices on 172.20.52.0



This subnet generally consists of PCs, printers, and access points. Essential services such as DCHP and DNS are not found on this network, and devices must make 2 hops to reach the respective server. This subnet's router is located at 172.20.52.1.

Device Type	Amount
General Purpose	75
Printers	1
Networking	2
Servers	0

/ Devices on 192.168.224.0



On this subnet, devices consist mainly of servers including services such as DHCP, DNS, active directory and more. This subnet's router is located at 192.168.224.254.

From the above graph we can also see that the college's primary router to the outside world is located at 192.168.225.254.

Device Type	Amount
General Purpose	0
Printing	1
Networking	3
Servers	96

// Our public IP

```
Tracing route to hotten.uk [172.67.175.41]
over a maximum of 30 hops:

  1    <1 ms    <1 ms    <1 ms  172.20.52.1
  2    <1 ms    <1 ms    <1 ms  212.219.7.1
```

Using tracert, I was able to identify that our public IP address is 212.219.7.1.

// Issues during the interrogation

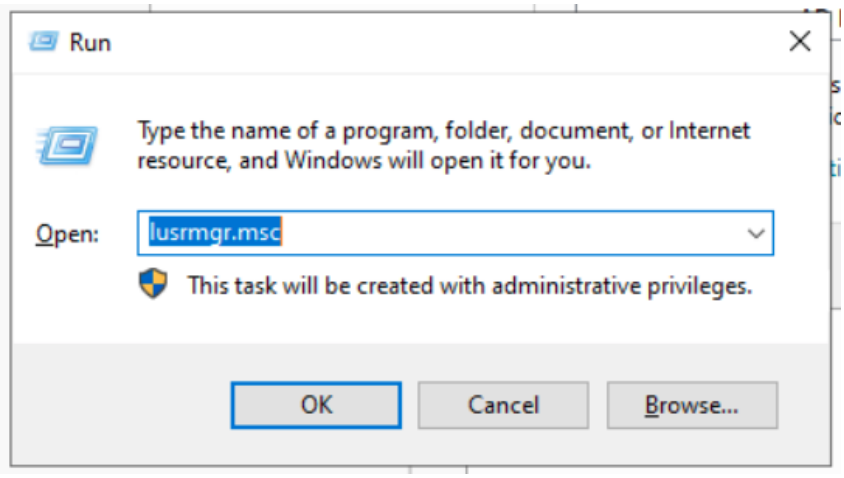
One issue I found the accuracy of Nmap's OS detection to be poor. For example, throughout my scan of the 172.20.52.0 most computers were reported as running Windows XP Service Pack 3, whereas the computers are running Windows 10 and 11.

// Routine Management Tasks

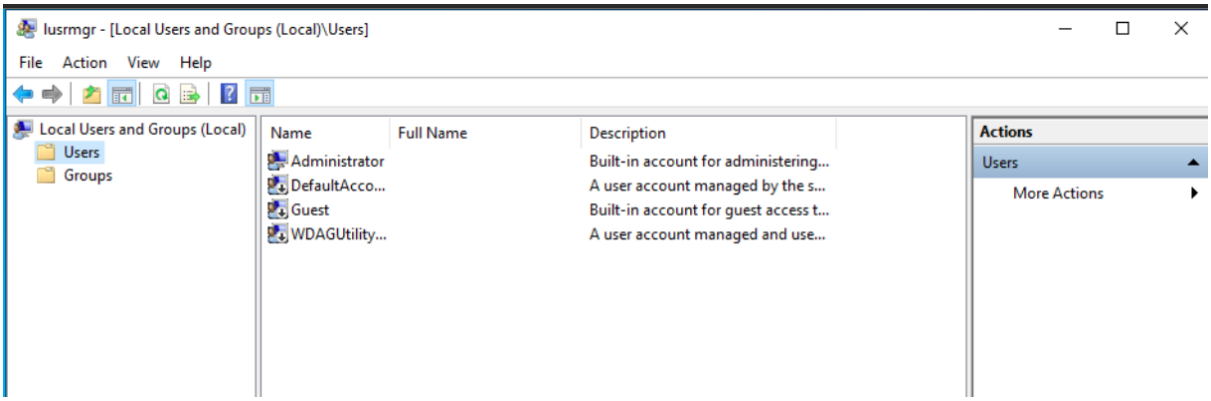
Please note these tasks were performed on Windows Server 2022 and may not be applicable to other versions of Windows.

// Creating a new user

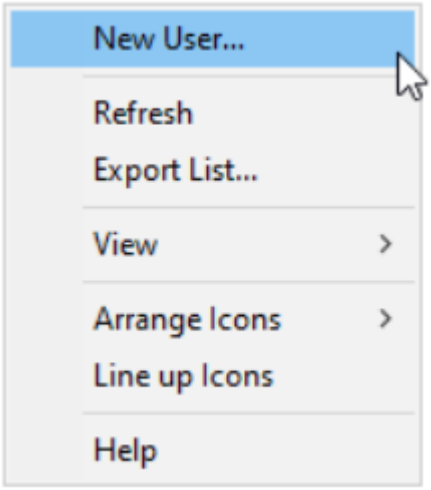
To create a new user, first we must open the Local Users and Groups snap-in. We can do this by using Run, by pressing Windows + R, then typing in lusrmgr.msc.

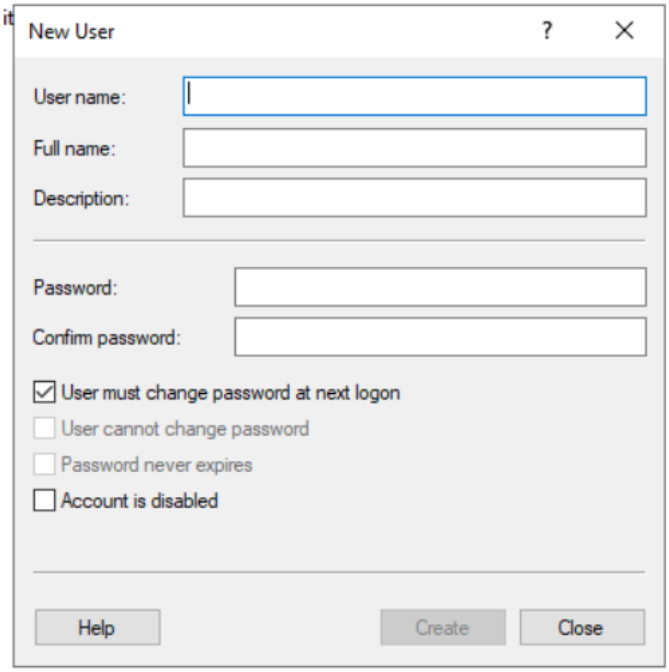


This then opens the Local Users and Groups snap-in, to get to the menu we need, click on "Users" on the left hand side.

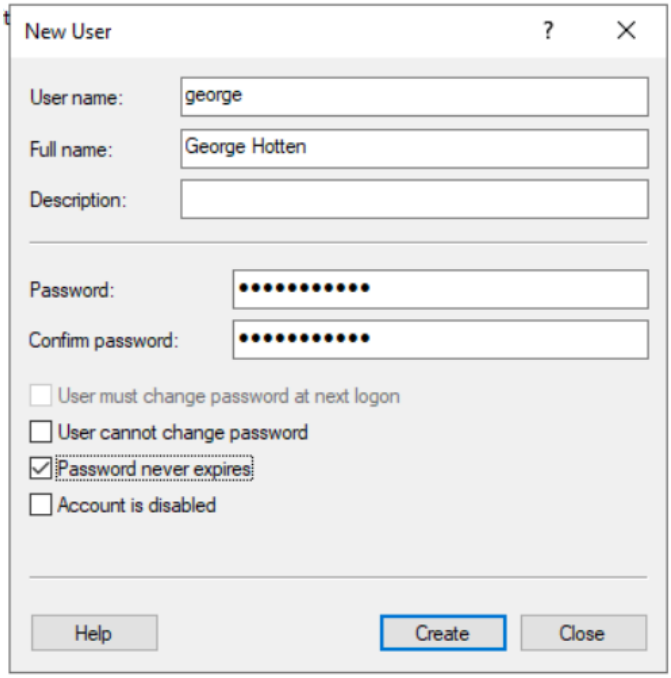


By right clicking and pressing the New User button we can add a new user.

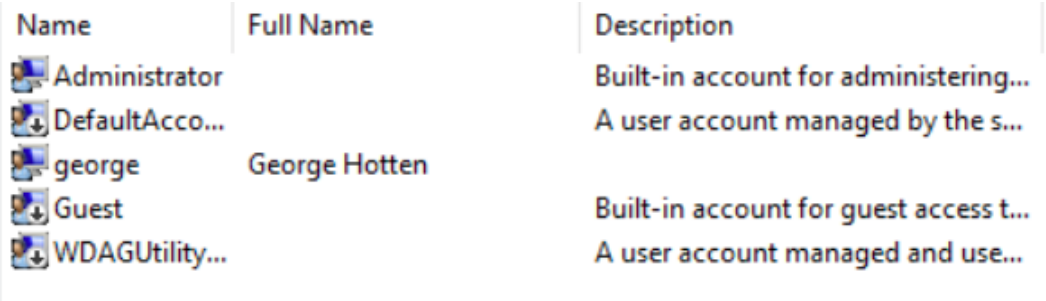




Now I can fill in my details and created press Create.



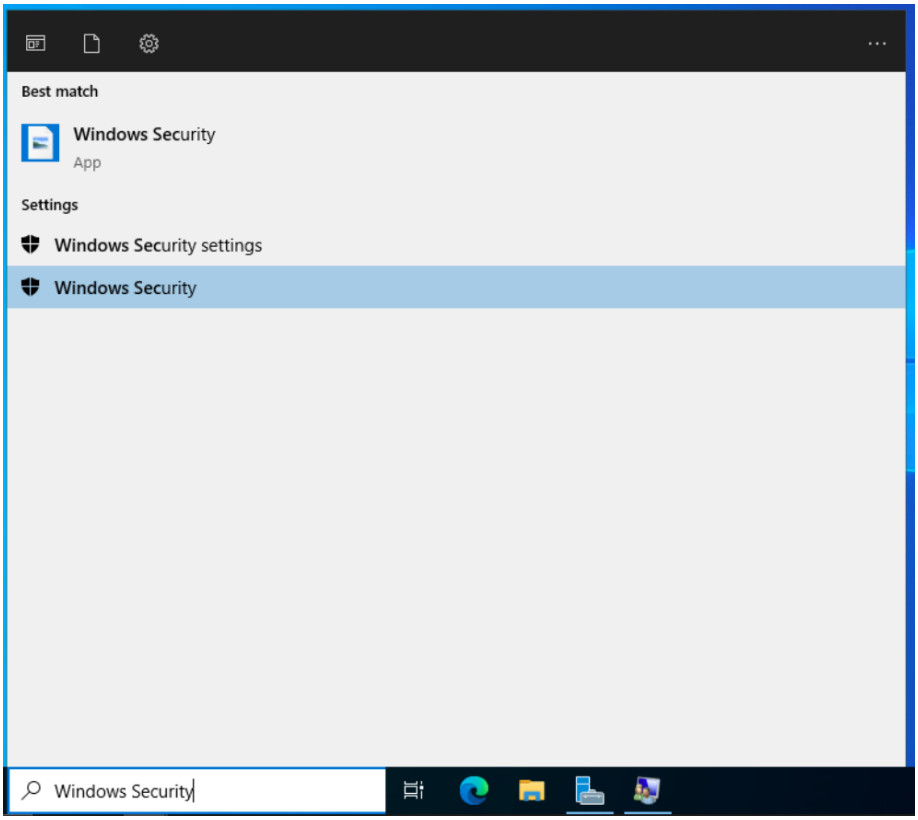
I have selected that my password never expires, however for more security this can be enabled.



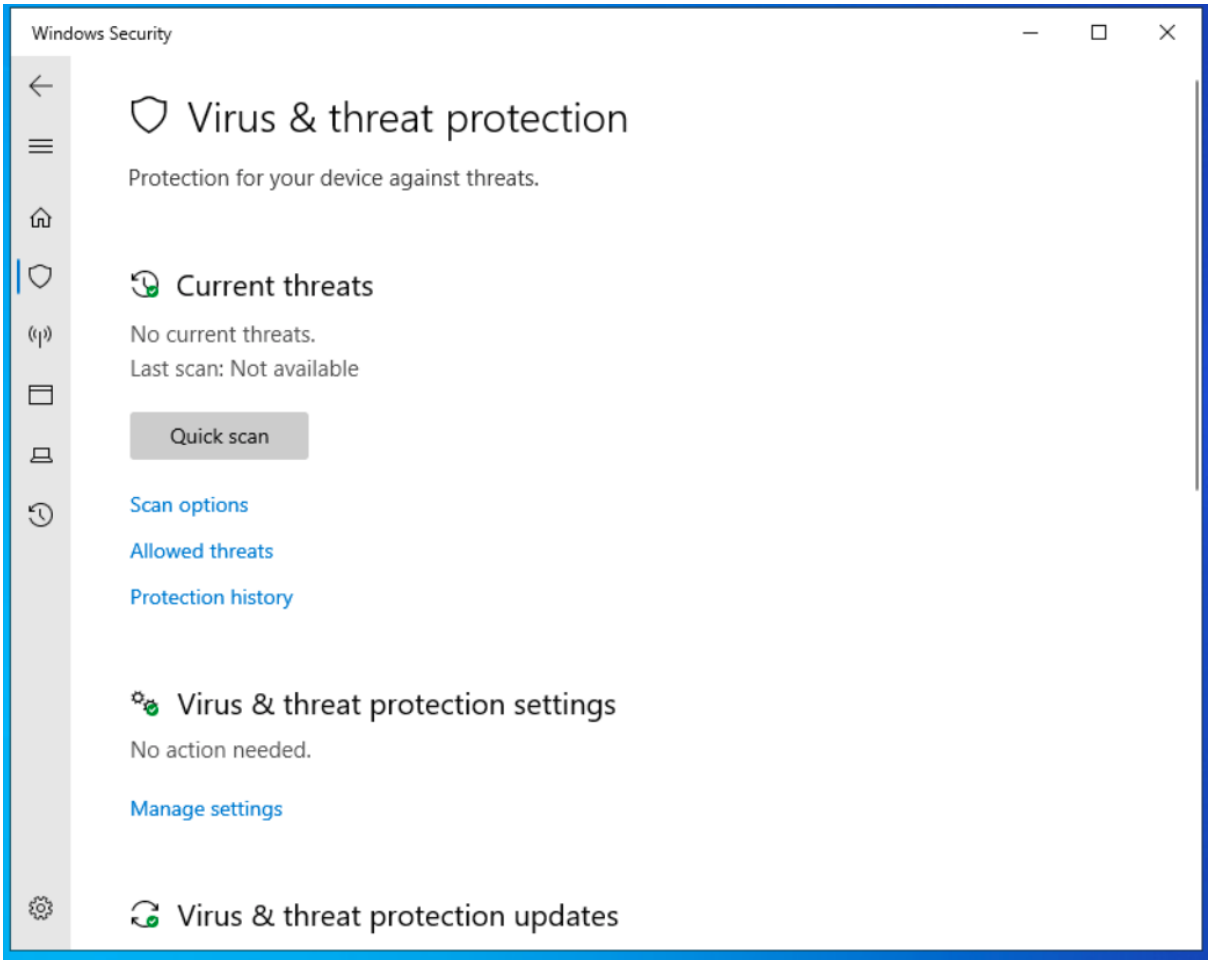
My account is now created. I completed this on 02/11/22. New users can be added whenever they're needed. It is good practice to review your users to ensure details are up-to-date and only accounts that need to be active are active. This can be done every month.

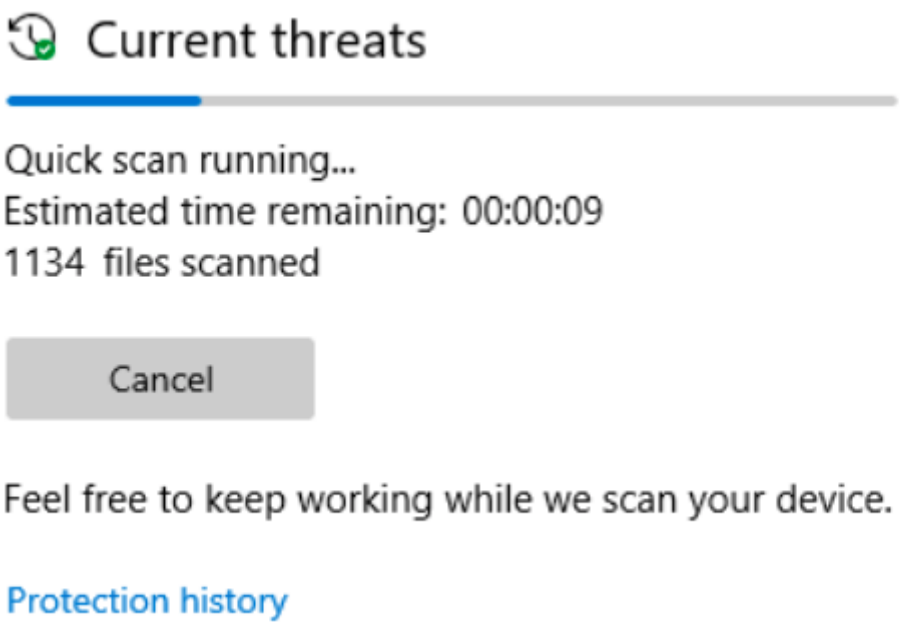
// Running a virus scan

To run a virus scan, we must open the Windows security dashboard. We can access it by typing Windows Security into the search bar.

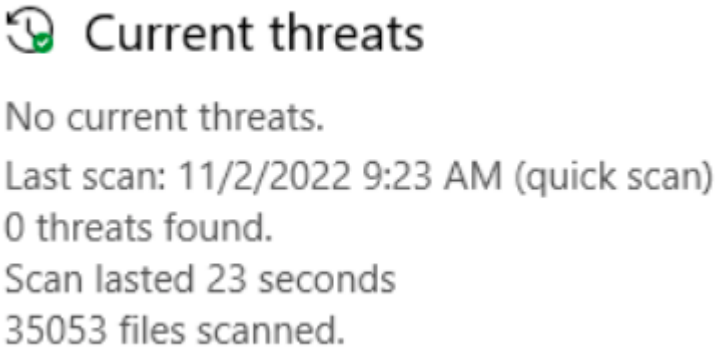


After it opens, we can press Virus and Threat Protection and press Quick Scan.





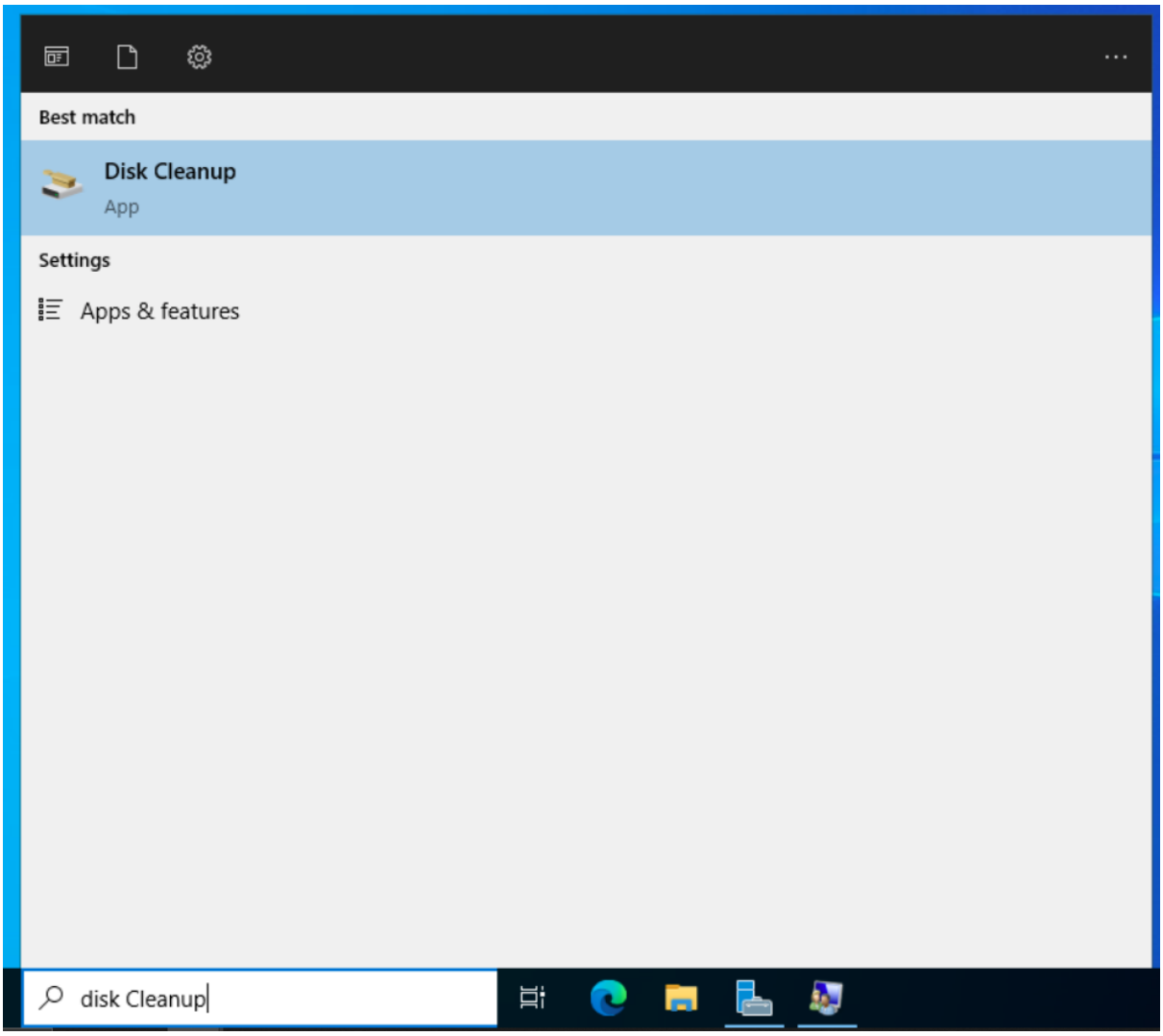
After the scan is completed, you will get a summary of the scan.



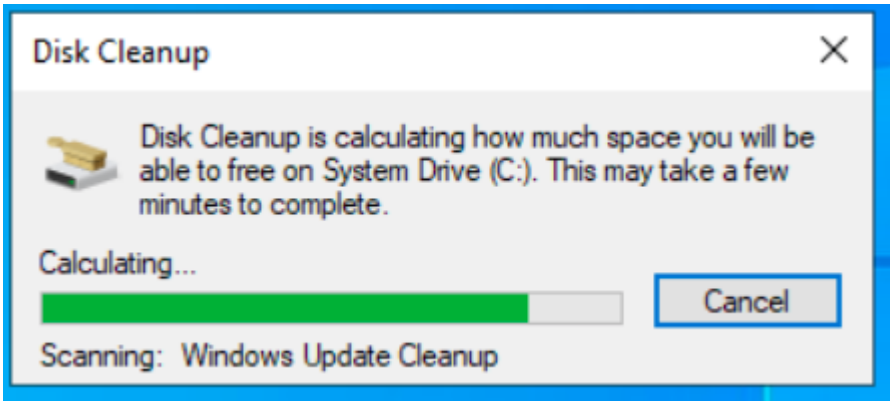
This was completed on 02/11/22. A virus scan should at minimum be completed daily. It can be completed every few hours depending on the severity of the data stored on the device.

// File clean-up

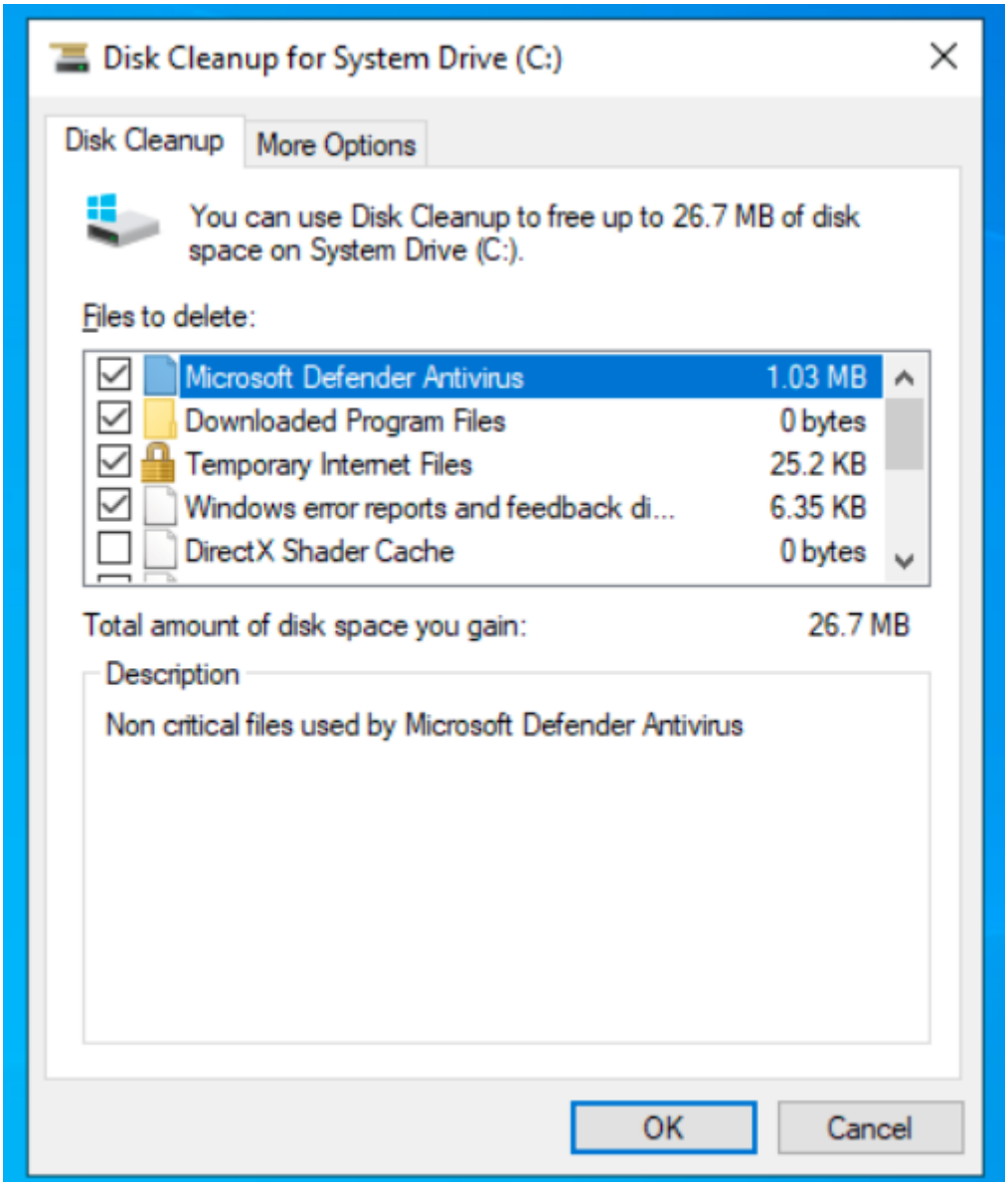
To access the file clean-up utility, you can search Disk Cleanup into the search bar.



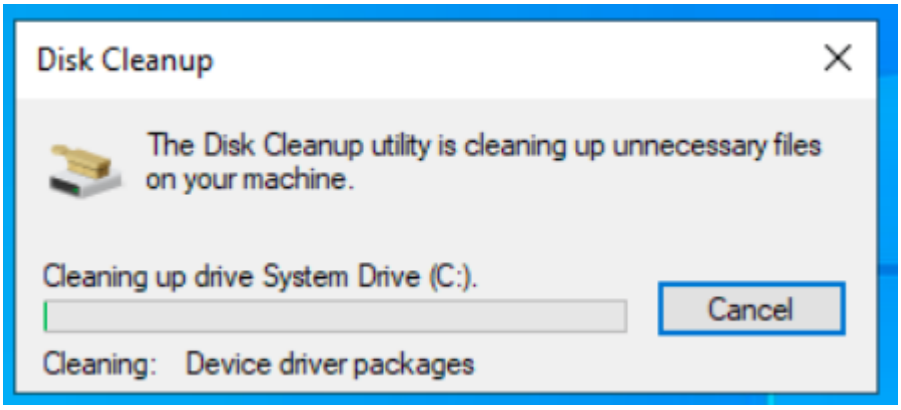
Windows will now scan your drives looking for any files that can be cleaned-up.



After this is completed, a summary of files will be shown, and you can choose what you want to be removed.



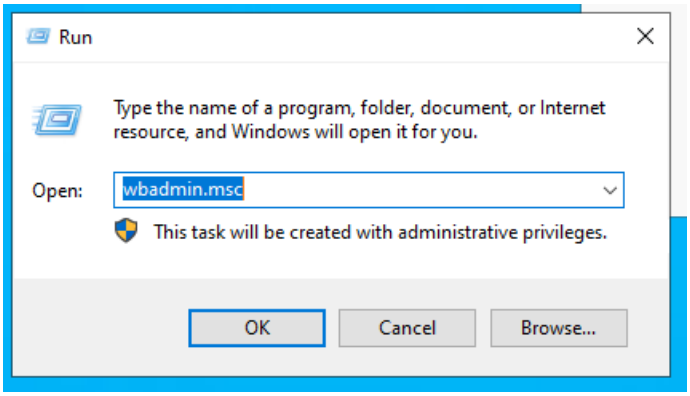
After pressing OK, the system will now start deleting the files selected.



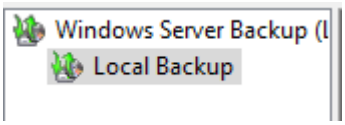
The disk clean-up is now completed. This was completed on 02/11/22. This can be completed between every week and every month.

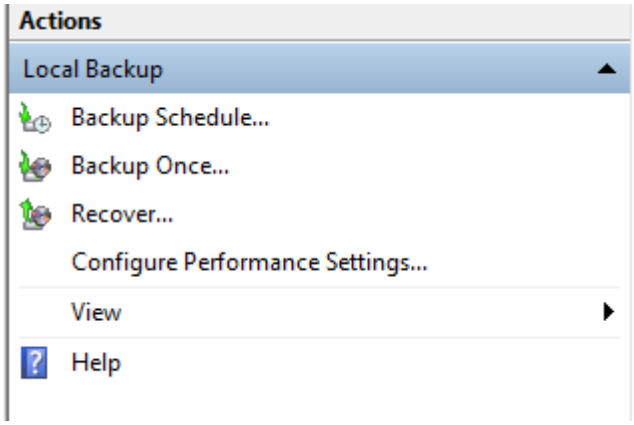
// Backup the configuration

To create a backup, first we must open the Windows Server Backup snap-in. This can be done by typing wbadmin.msc into Window's Run dialogue.

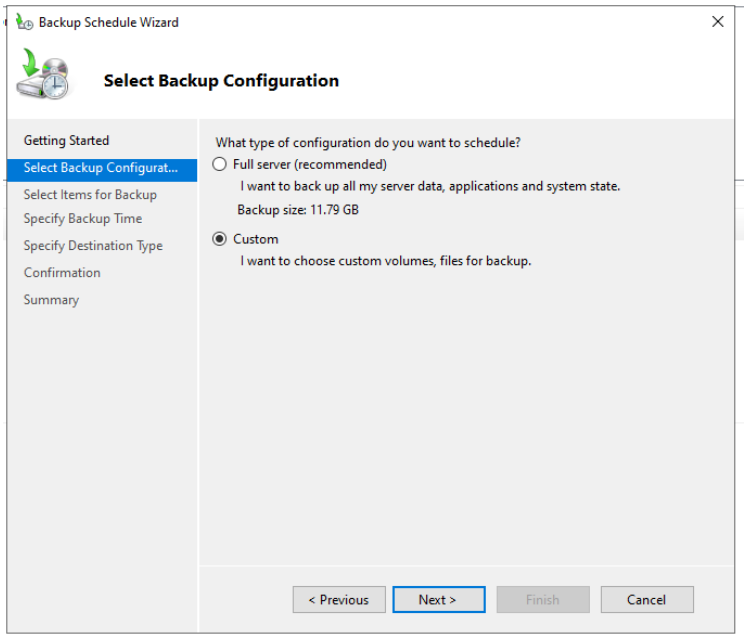


After the snap-in opens, press Local Back up on the right hand-side then press Backup Schedule.

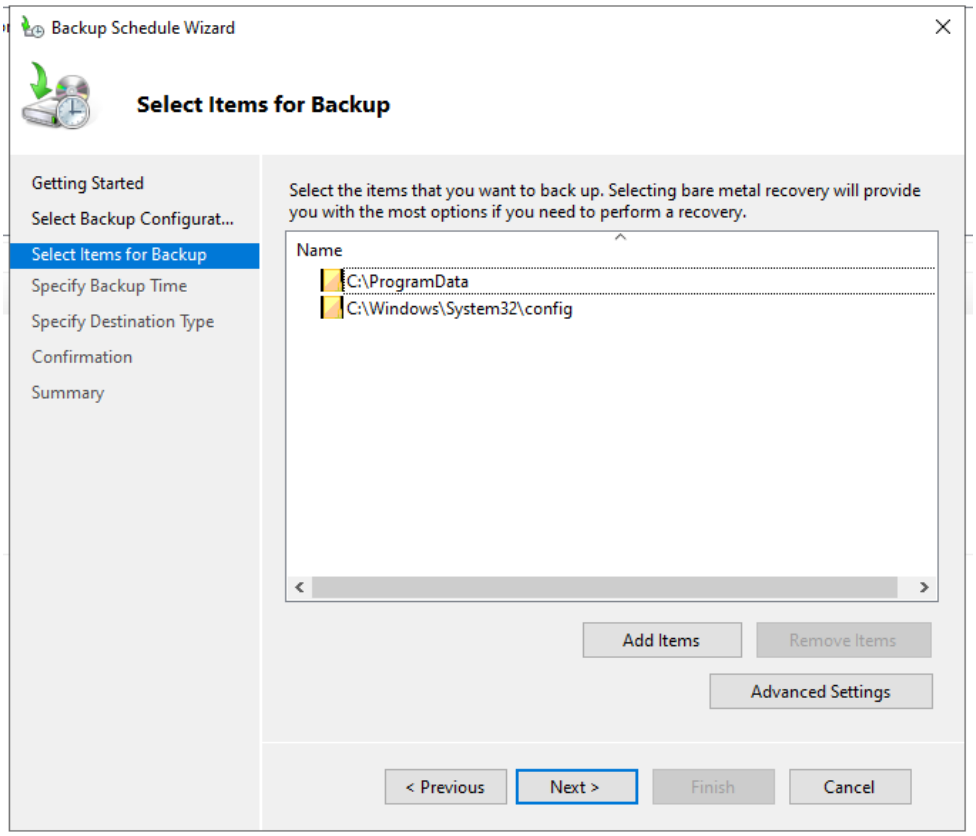




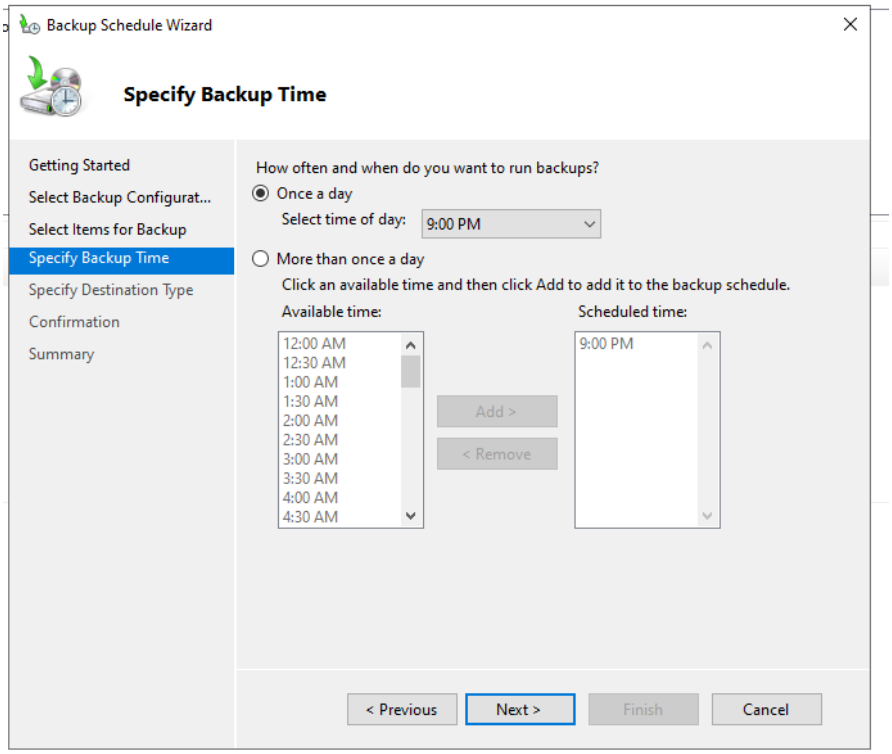
After the wizard opens, select Custom Backup



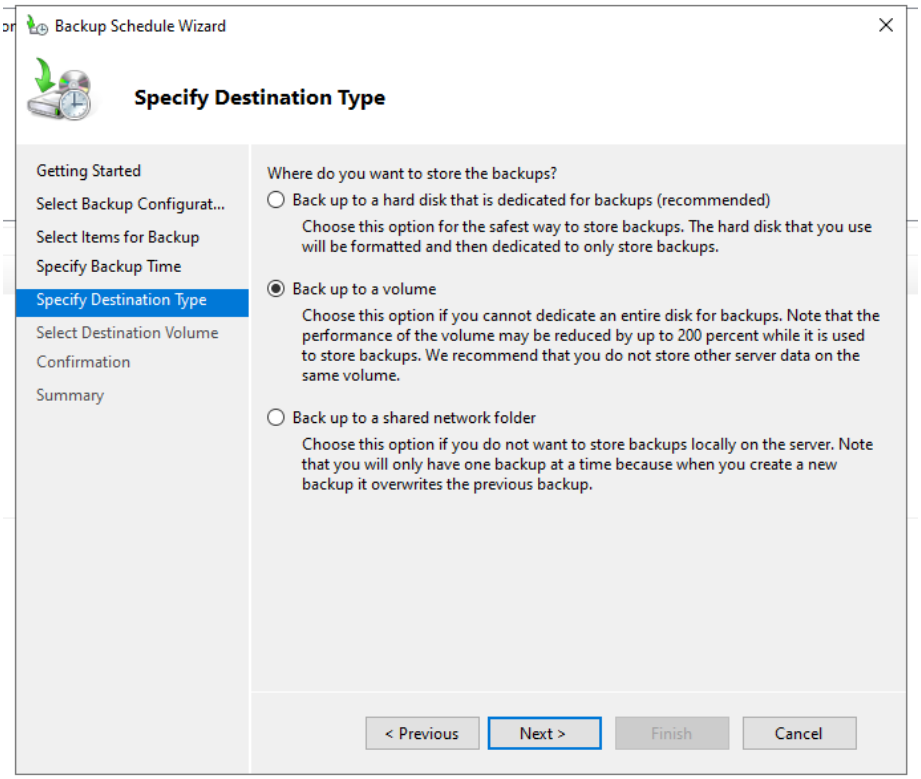
After continuing, select the following item to be backed up: C:\ProgramData and C:\Windows\System32\config. The config path contains the registry and other system configurations.



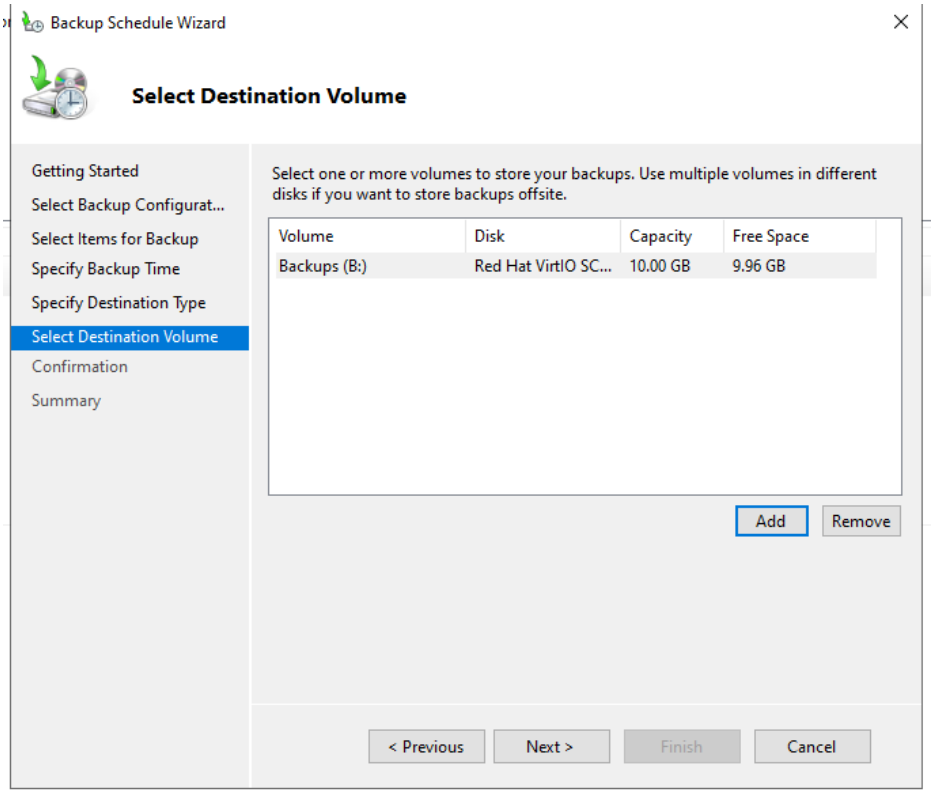
After progressing, you can choose how often the data should be backed up. In this example, we will run the backup every day at 9PM, however it can be run as often as every half-hour.



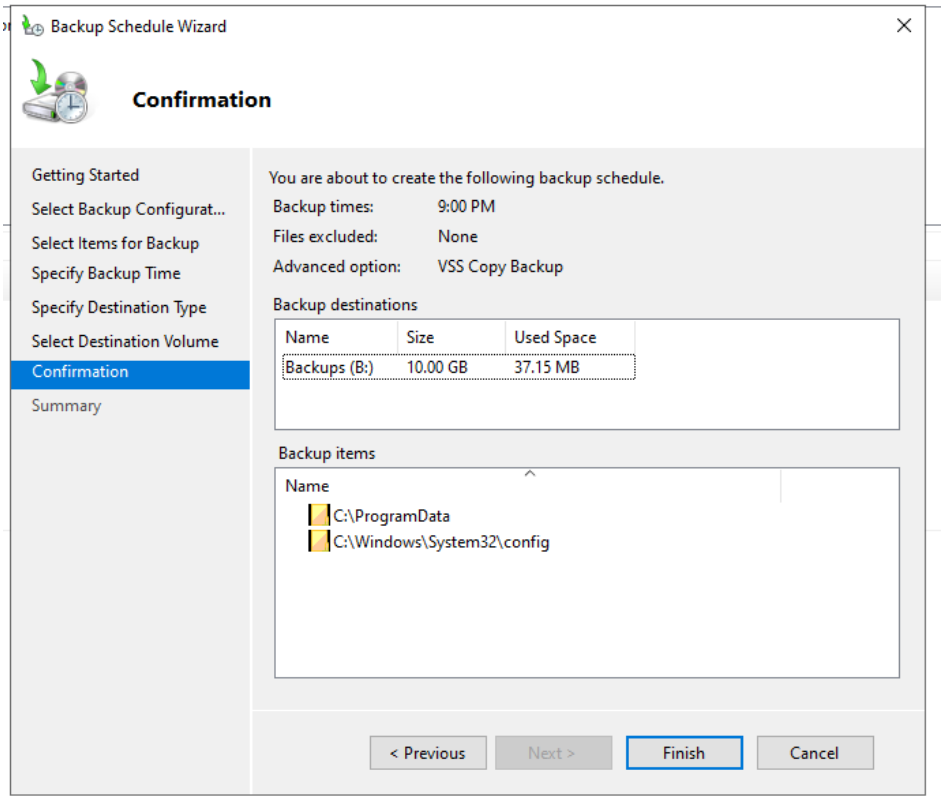
Now you can choose where the back-up is stored to. A separate drive is recommended, however for this demo I will use a volume I partitioned.

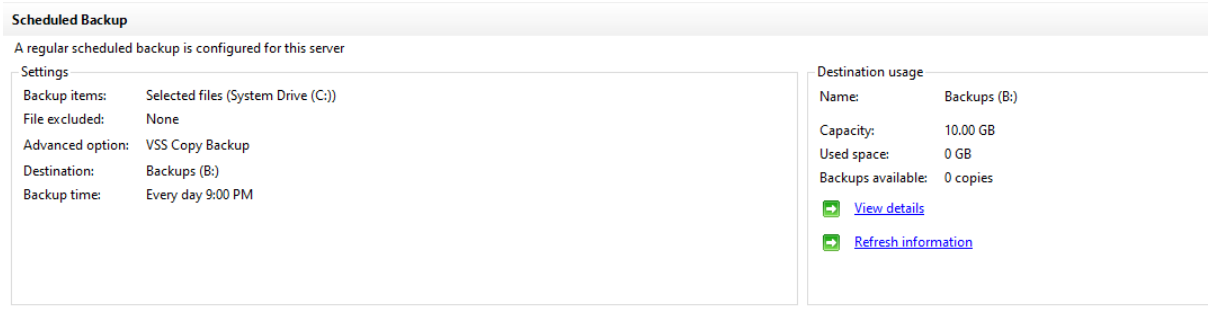


I will now select the volume I want my backups to be stored to.



Finally, after confirming everything is correct, we can finish the setup.



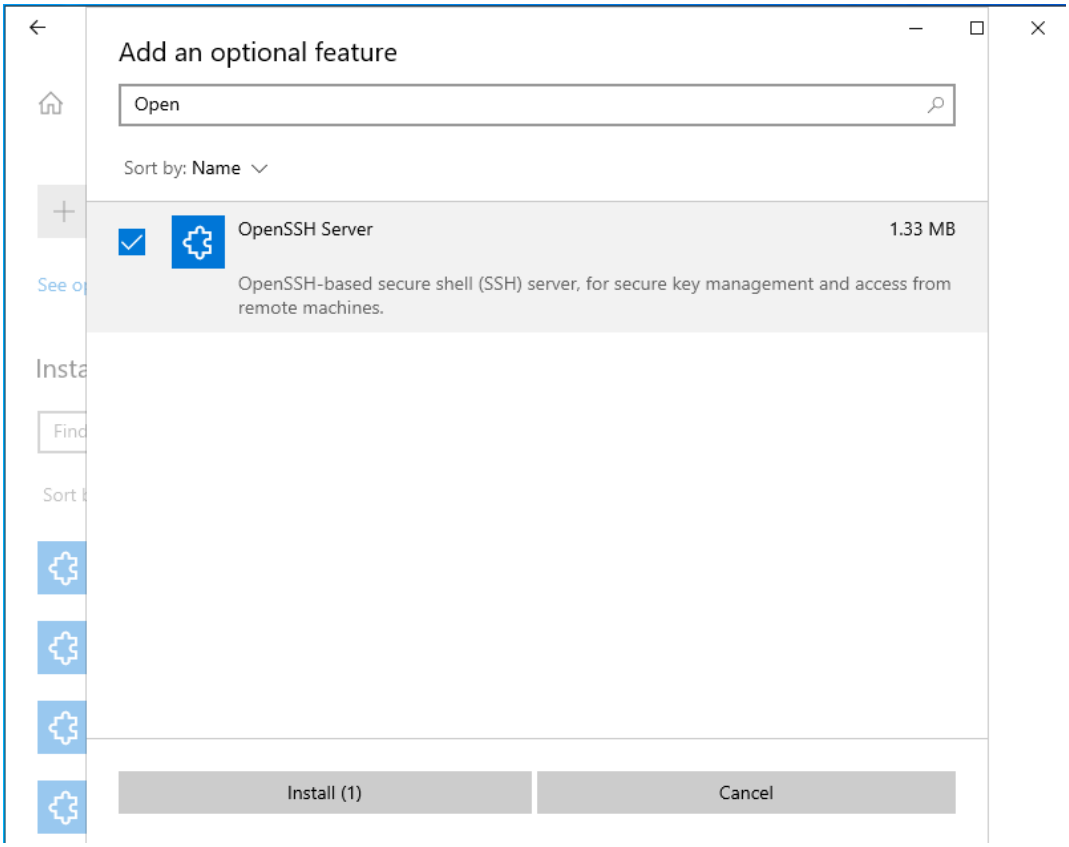


Our schedule is now created. This was completed on 02/11/22. Backups should be completed on a regular basis in line with the importance of data stored. For example, critical data could be backed up every hour whilst a user's program data could be backed up weekly.

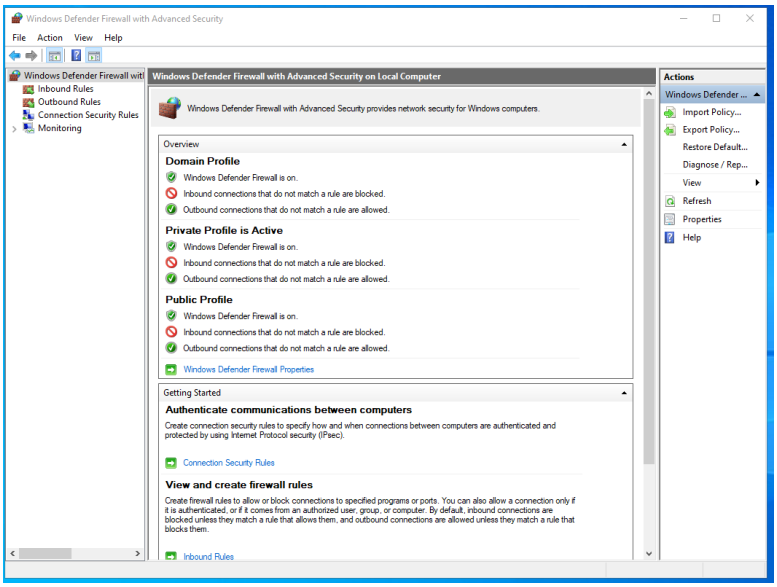
// Enabling SSH and configuring the firewall

To start, navigate to Settings, Apps, Optional Features.

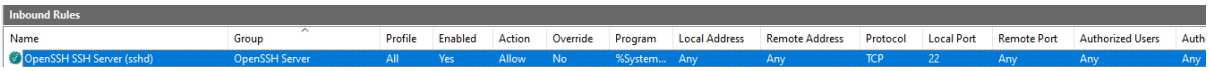
From there, select Add Feature and type in Open SSH and install the server.



OpenSSH automatically configures the firewall for us. Let's check it. We can access the firewall settings by typing wf.msc into the Window's Run dialogue.



After the snap-in opens, select Inbound Rules and search for OpenSSH SSH Server.



As we can see, this inbound rule is configured to allow traffic from port 22 over the TCP protocol allowing SSH to function.

This was completed on 02/11/22. This does not need to be repeated; however it is good practice to check your firewall every week to ensure all policies are recognised and correct.

// Network Security Policy

// Acceptable Usage Policy

Before using the network, all users should agree to a network acceptable usage policy (AUP). An AUP should contain what is and isn't allowed on the network. Typically, this contains not sharing your login details, following password complexity requirements, and not tampering with any computer or network settings. AUPs also outline the disciplinary action that will be taken if the policy is broken, such as verbal/written warnings or the blocking of your network access.

// Responsibilities

All network users are responsible for ensuring that they follow the appropriate training and best practices whilst using the network. For example, not clicking any suspicious links in e-mails or downloading files from an untrusted source.

// User Access Rights

Users of the network should only have access rights for what is required to complete their job. For example, people in the training department would not need access to the business' financial records. This is essentially important if an account is compromised, if the account has proper access rights set the damage will be minimised as they won't have access to everything within the network.

/ Timing for Reviews

User Access Rights should be reviewed every 3 months and should be reviewed when operating systems are updated to ensure no changes have been made and any new policies can be configured.

// Firewall Rules

With threats constantly evolving, it is important to keep an up-to-date firewall to ensure that nothing malicious can enter the network. Firewalls allows a network administrator to chose what is allowed in and out of their network based on port numbers, packet filtering and TCP connection and session observation.

/ Timing for Reviews

Firewalls should ideally be reviewed every month inline with current threat information to ensure any emerging threats and malware can be blocked before they have the chance to cause any damage.

// Security Audits

Security Audits are usually untaken by a third-party who check the network's security configuration to ensure the current security strategy is adequate, proper training is being delivered and if any vulnerabilities are present. Once the security audit is finished, a list of priorities if created for any issues found and the fixes should be implemented in that order. The results of the security audit should be shared with any pre-determined parties.

/ Penetration Testing

During security audits, a penetration tester will attempt to breach your network to identify any vulnerabilities that are yet to be patched. The tester will deliver a final report to the network administrator or security auditor with details of any vulnerabilities found and how they can be patched.

// Scope

The scope of the security policy should be staff and guests who use the network's IT equipment and services.