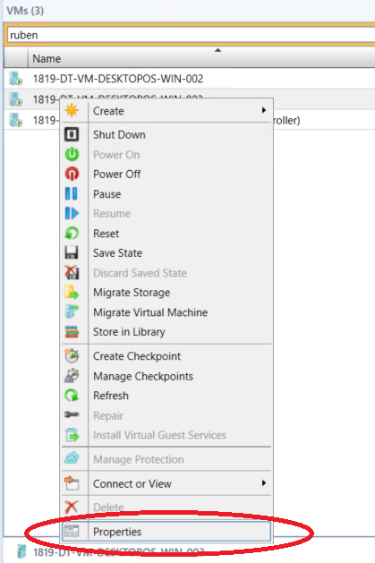
Windows Werkcollege 3

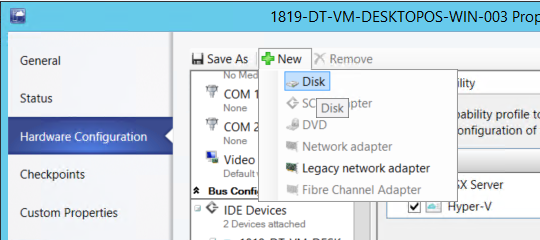
# Recovery & Backups

## Voorbereidende stap

Om te vermijden dat je werkstukken de dag voor indienen kapotgaan, of dat je Windows het plots begeeft, raden we je aan je gegevens te back-uppen. Om dit te doen hebben we een nieuwe fysieke schijf nodig voor onze VM. Je zal deze zelf moeten aanmaken door te connecteren met VMM en de properties window te openen van jouw Virtuele Machine.



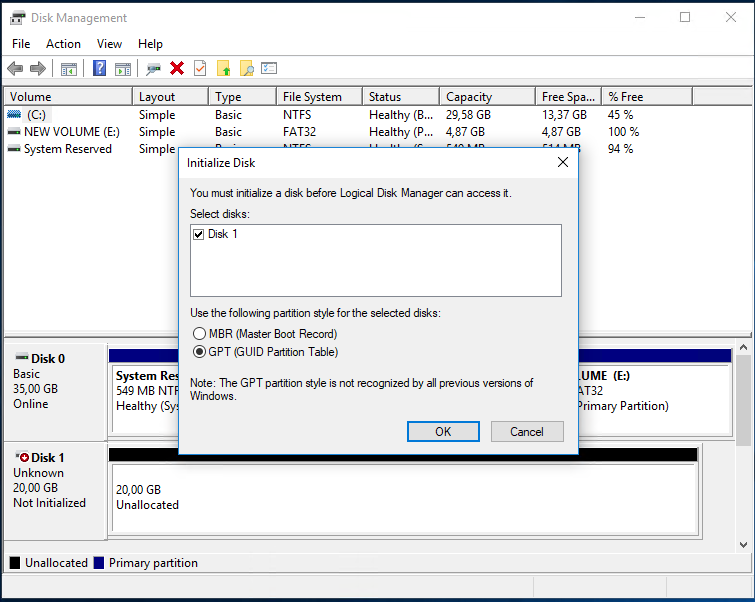
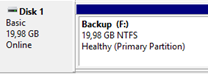
Selecteer daarna Hardware Configuration -> New -> Disk. En maak een nieuwe schijf aan met **30GB** ruimte. De andere instellingen staan al goed.



Connecteer nu met je VM (via rdp) en maak een nieuwe partitie aan op deze schijf (zie werkcollege 2).

Je zal bij het opstarten van de Disk Management-tool opmerken dat de schijf nog niet geïnitialiseerd is. Selecteer GPT en formateer de schijf daarna naar een NTFS formaat.

|  |
| --- |
| **Opdracht:**  Zoek op wat het verschil is tussen MBR (Master Boot Record) en GPT (GUID Partition Table) |

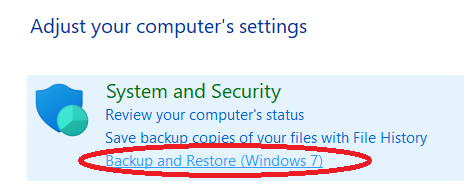


## System Image Recovery

Soms is het besturingssysteem zo zwaar beschadigd dat deze niet eens meer kan opstarten. Om dit op te lossen kan je gebruik maken van een systeemherstelschijf (System Image Recovery).

Om deze tool te kunnen uitvoeren hebben we wel eerst nood aan een ‘Image’ van het systeem die we moeten bij houden.

Om dit te verwezenlijken kan je gaan naar het Control Panel > System & Security > Backup and Restore (Windows 7) > Create a system image.

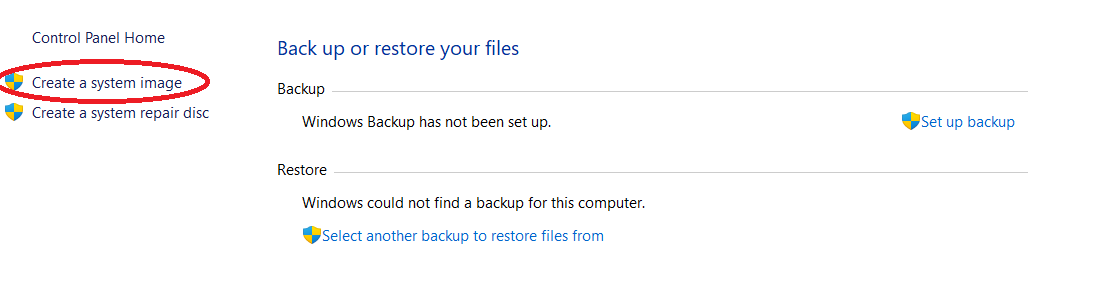


(Je kan ook gaan via Control Panel > System & Security > File History om daar System Image Backup te selecteren.)

Je kan de Control Panel openen door te zoeken in de windows search balk of run te openen (⊞ + r) en **control** in te geven.

A close-up of a computer screen

Description automatically generated



Je zal moeten ingeven waar je de back-up gaat bewaren. Een DVD, een aparte harde schijf of op een netwerklocatie.

Je kan in Windows 11 ook een bootable USB-stick maken om zo een systeemherstel te bewerken. Dan moet je wel gebruikmaken van de ‘Recovery Drive’ tool.

|  |
| --- |
| **Opdracht:**  Maak een herstelschijf aan op de door jou toegevoegde disk. |

### Windows Preinstallation Environment

WinPE is een minimalistisch besturingssysteem dat als doel heeft Windows te installeren, op te zetten en te herstellen.

Je kan WinPE plaatsen op een harde schijf of een usb-disk om vanuit de PE te booten en verschillende taken uit te voeren.

We raden je aan eens te kijken naar onderstaande link voor meer informatie. Merk ook op dat je kan leren om zelf je apps te schrijven voor WinPE.

<https://docs.microsoft.com/en-us/windows-hardware/manufacture/desktop/winpe-intro>

Er staat ook vermeld wat je kan doen via WinPE:

* Harde schijven instellen (voordat je Windows installeert)
* Een custom installatie van Windows maken door apps en scripts uit te voeren
* Windows images aanmaken en gebruiken
* Automatische herstelopties instellen
* Data van een niet opstartbare (unbootable) schijf halen
* Een eigen shell aanmaken of GUI voor deze taken te automatiseren
* …

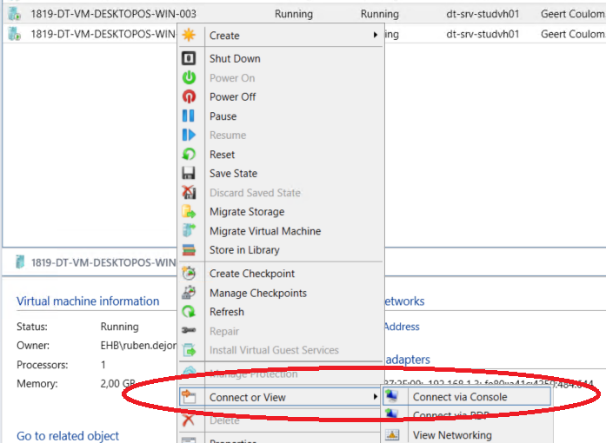
### WinRE (Windows Recovery Environment)

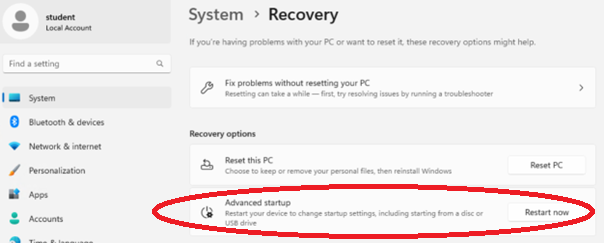
Bij een standaard Windows 11 desktop-installatie (en zelfs Windows server) wordt er een extra herstelomgeving (Operating System) mee geïnstalleerd. Deze omgeving wordt automatisch opgeroepen als je standaard Windows enkele malen weigert om op te starten en bevat enkele handige tools om je Windows terug aan de praat te krijgen. Dit is WinRE en is gebaseerd op WinPE.

Je kan op verschillende manieren in de WinRE geraken.

Eén manier is om te rechterklikken op de startknop, settings te kiezen, ‘Update & Security’ en daarna te klikken op recovery. Je kan daar de optie terugvinden om je PC te herstarten op een uitgebreide manier. Door deze te kiezen zal je booten in de WinRE.

Helaas zijn deze opties niet mogelijk via een rechtstreekse RDP-verbinding. Om dit te testen zal je via VMM moeten gaan. Connecteer met de Windows Server en open VMM.

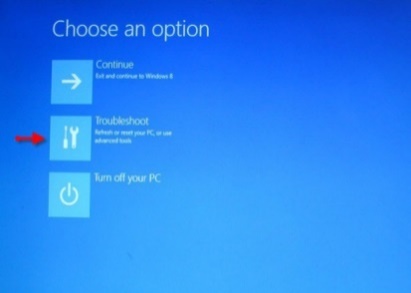
Connecteer daarna met je VM via Console en probeer daar de WinRE uit.



Een alternatieve manier is het volgende commando in cmd: **shutdown /r /o**

Voer volgende stappen uit eenmaal je opgestart bent in de WinRE.

* Kies Troubleshoot
* Kies Advanced Options
* Ga naar System Image Recovery

Eenmaal je dit hebt geselecteerd zal de wizard opgestart worden en zijn de volgende stappen vrij logisch te voltooien.

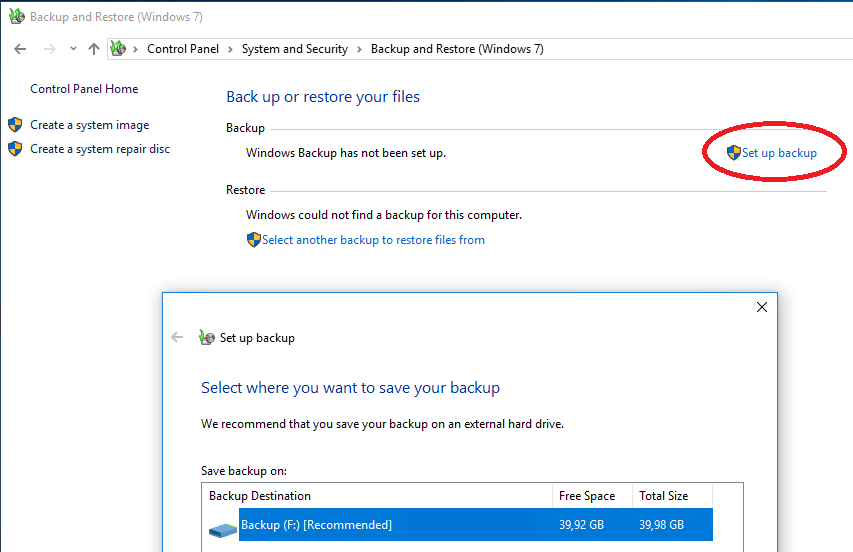
Als je een recovery image hebt gemaakt zou deze hierin moeten verschijnen.

|  |
| --- |
| **Opdracht:**  Verwijder enkele files en plaats daarna Windows terug naar zijn vorige status door gebruik te maken van een Recovery Image. Merk op dat de files terug zullen staan. |

Dit is nu geen mogelijkheid aangezien de VM’s UEFI niet ondersteunen, maar weet dat het handig is om via het ‘Troubleshoot’ menu te gaan naar je UEFI.

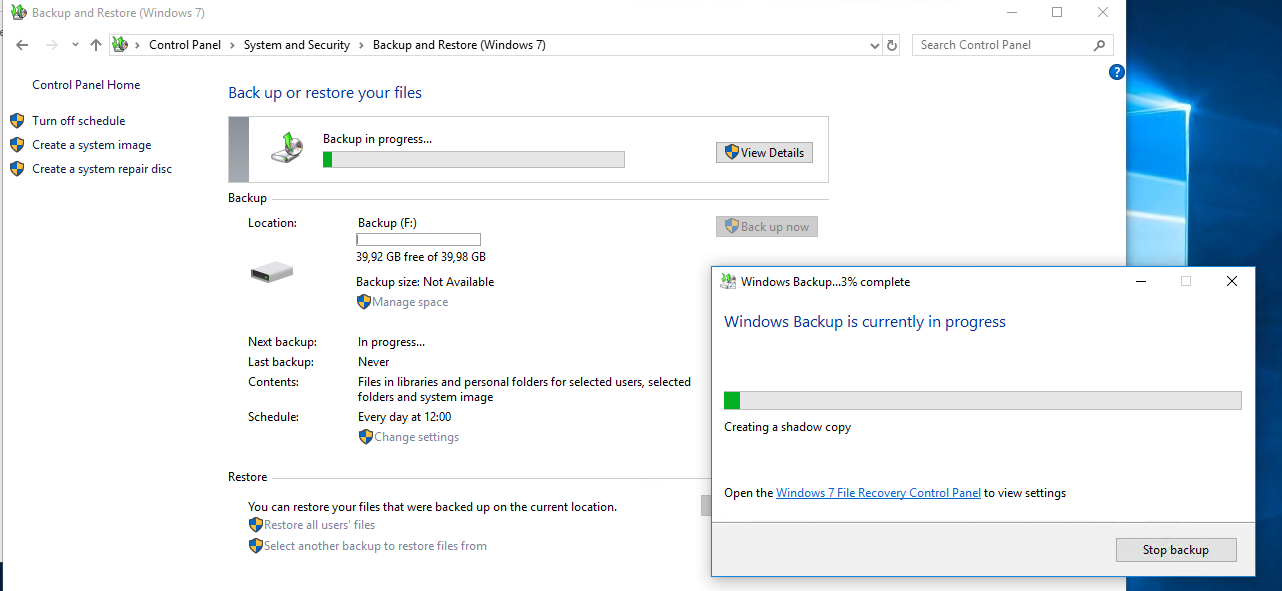
## Automatische File Backup

Je kan ook kiezen om een bepaalde schijf en bepaalde bestanden automatisch in een image te gaan bewaren. Dit kan je doen door te navigeren naar: Control Panel > System & Security > Backup and Restore (Windows 7) waar je ‘Set up backup’ kan selecteren.



|  |
| --- |
| Opdracht:  Kies je systeemfolder samen met een andere zelf te kiezen folder uit, en zorg dat deze elke dag om 12u00 wordt bewaard als image in de nieuwe partitie. |

Je zal merken dat hij nadien bezig zal zijn met een shadow copy aan te maken. Dit is een technologie die ervoor zorgt dat je bestanden kan kopiëren zelfs al zouden deze in gebruik zijn.



## System Restore Points

Soms is het niet nodig heel je besturingssysteem met inbegrip van je persoonlijke files terug te draaien naar een vorige versie. Soms is het voldoende om enkel je systeembestanden te veranderen zodat bepaalde “fouten” opgelost raken. Om dit op een eenvoudige manier te doen kan je gebruikmaken van Restore Points.

Pas op, System Restore Points kunnen niet gebruikt worden om persoonlijke data terug op te vragen.

Open je ‘Control Panel’ en pas de manier van weergeven aan naar “small icons”. Je zal merken dat er enkele opties bijkomen waaronder Recovery. Selecteer deze en kies daarna “Configure System Restore”

Graphical user interface, application

Description automatically generatedGraphical user interface, text, application, chat or text message

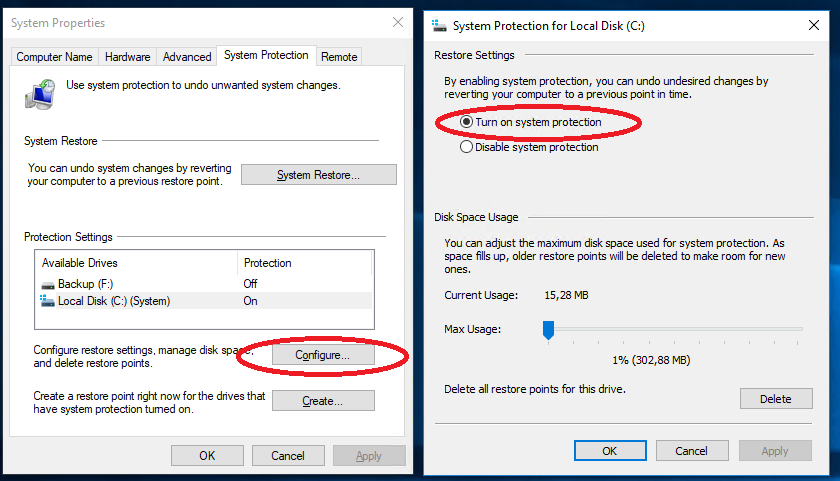
Description automatically generated

A picture containing shape

Description automatically generated

(Je kan er ook naar toe gaan door in de windows search “create a restore point” in te geven.

Hier kan je Restore points aanmaken, bepalen hoeveel ruimte op je schijf gebruikt wordt om deze punten bij te houden en of je dit al dan niet wil.



Als je problemen ondervindt, kan je, vanaf dat je eerste restore point aangemaakt is, de ‘Open System Restore’ optie selecteren om je systeem bestanden terug te zetten naar een vorige versie.

|  |
| --- |
| **Opdracht:**  Zet System Restore aan voor je c:/ schijf en maak een restore point aan (d.m.v. Create… )  Test het restore point uit door je register of systeemfiles / drivers aan te passen en terug te zetten. |

## File History

Maar je kan nog een stap verder gaan en een automatische back-up nemen en een ‘history’ (geschiedenis) opbouwen op individuele files die voor jou belangrijk zijn. Windows voorziet namelijk in een ingebouwd versioning systeem voor het bewaren van de files die te vinden zijn onder Libraries, Desktop, Contacts en Favorites. (Libraries bevat onder andere Documents en Pictures). Je kan zelf folders toevoegen aan Libraries door te rechtermuisklikken te kiezen voor “Show more Options” en daarna onder “Include in library” te kiezen voor Create new library.

A screenshot of a computer

Description automatically generatedA screenshot of a computer

Description automatically generated

**Opdracht:**

• Zoek de betekenis en het nut van ‘versioning’ op.

Je kan bij de “small icons” in het Control palen (zie 1.4) de optie File History terugvinden.



Kies er voor File history aan te zetten de schijf die je wilt gebruiken om je geschiedenisbestanden te bewaren.

|  |
| --- |
| **Opdracht:**   * Stel, door gebruik te maken van advanced settings, in dat je elke dag een back up wil die 9 maanden moeten blijven staan. * Maak een nieuwe folder onder je c:/ en voeg daarna de folder toe aan Libraries en zorg dat deze geback-upt wordt. |

Je kan nu door de properties van deze folders of bestanden op te vragen via windows explorer, selecteren om naar een vorige versie te gaan.

A screenshot of a computer

Description automatically generated

Je kan in Windows ook zoeken naar ‘Restore your files with File History’ om zo een tool te openen die je toelaat de geschiedenis van een hele folder stap per stap te bekijken.

## One Drive

Helaas hebben studenten in het verleden al voorgehad dat files net voor een deadline verloren gaan doordat de hardeschijf crashed. In zo een situatie heb je meestal niet de tijd om allerhande tools te gebruiken om de data van de hardeschijf terug te krijgen. Om je file veilig te kunnen bewaren raden we daarom aan om een betrouwbare cloudstorage te gebruiken. Microsoft biedt dit aan en via jullie Office365 van de school uit hebben jullie 1T online opslag. Microsoft OneDrive werkt standaard met Files On-Demand, wat wil zeggen dat hij deze enkel download wanneer je ze opent of gebruikt.

Graphical user interface, application, email

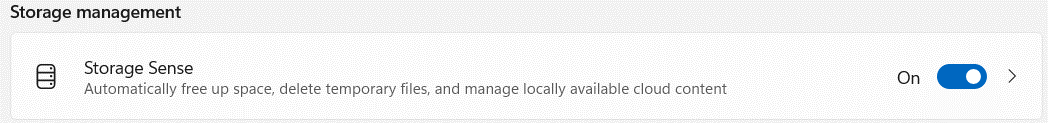
Description automatically generated

|  |
| --- |
| **Opdracht:**   * Start de OneDrive app op, login en selecteer de folder die je wil gebruiken om de bestanden bij te houden. * Open de Settings van de App. * Ga naar Manage Backup en stel in dat hij je Documenten moet beheren om automatisch te synchroniseren. * Bewaar via Windows Explorer enkele Files in de folder en controleer online via <https://ehb-my.sharepoint.com/> of deze toegekomen zijn. * Rechtermuisklik één van jouw OneDrive Folders in File Explorer en kies de optie Share. Kies iemand uit om deze folder mee te delen en probeer om met elkaar files uit te wisselen.   Graphical user interface, text, application, chat or text message  Description automatically generated   * Vergeet niet om je OneDrive account op je VM te ontkoppelen na dit werkcollege. |

#### Good to know (Niet te kennen leerstof)

Storage Sense is een tool van Windows die je helpt om wat opslagruimte automatisch vrij te maken.

Rechterklik op het startmenu, selecteer Settings, System en navigeer naar Storage.



Je zal merken dat je daar de opties hebt om Storage sense aan te zetten en te bepalen hoe dat deze ingevuld wordt.

|  |
| --- |
| **Opdracht:**   * Ga naar de opties van Storage Sense (door op het Storage Sense te klikken) * Zorg ervoor dat Storage Sense elke week onnodige files opspoort en verwijdert. * Zorg er ook voor dat hij elke 30 dagen de recycle bin (de Prullenbak) en de Downloads folder leegmaakt. * Kies voor ‘Run Storage Sence Now’. |

Storage sense zoekt standaard naar verschillende soorten files die weg mogen.

Denk aan:

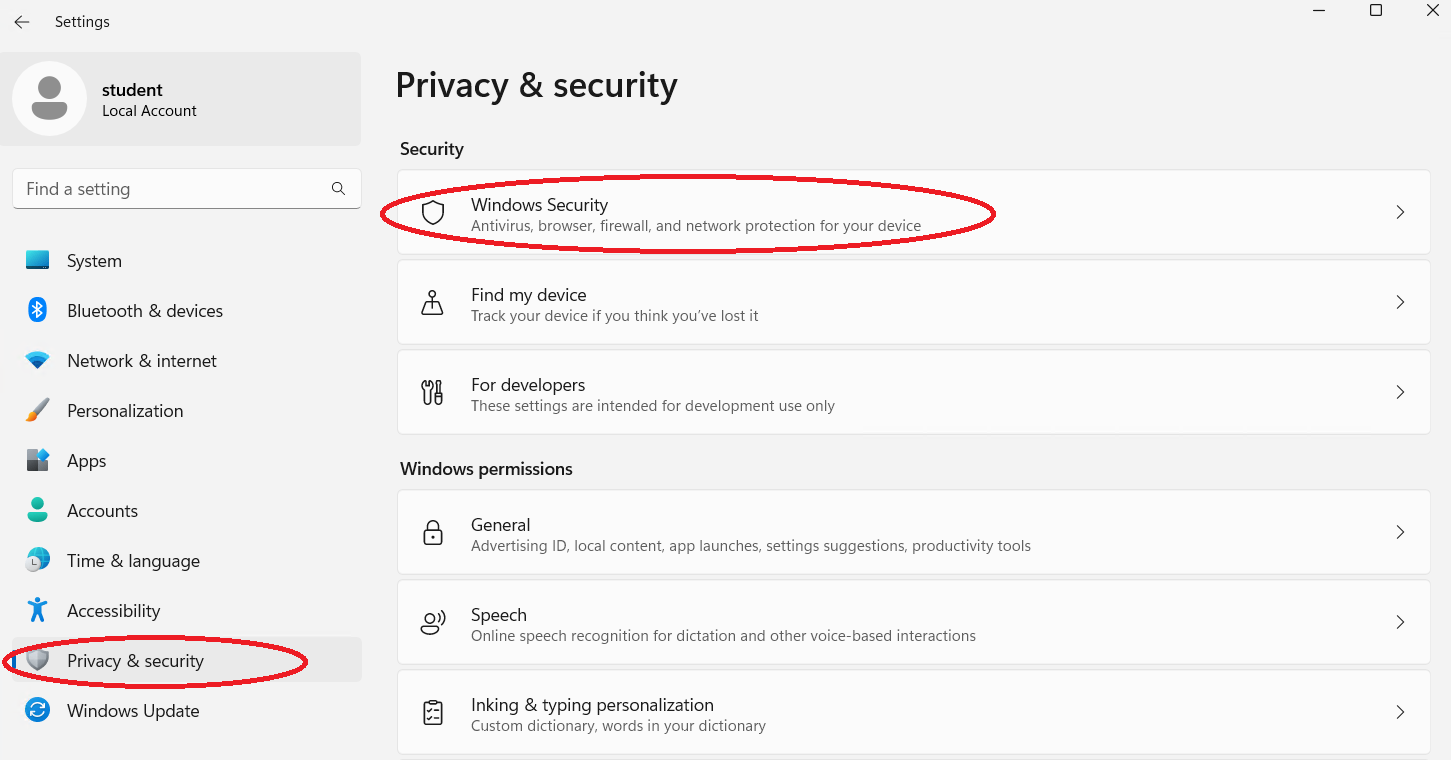
* Tijdelijke setup files
* Systeem cache files
* Internet Cache files
* Device Driver Packages
* Systeemlogs, memory dump files
* Tijdelijke Systeem bestanden
* Windows update bestanden
* …

# Windows Security

## Windows Virus & Threat protection en Firewall

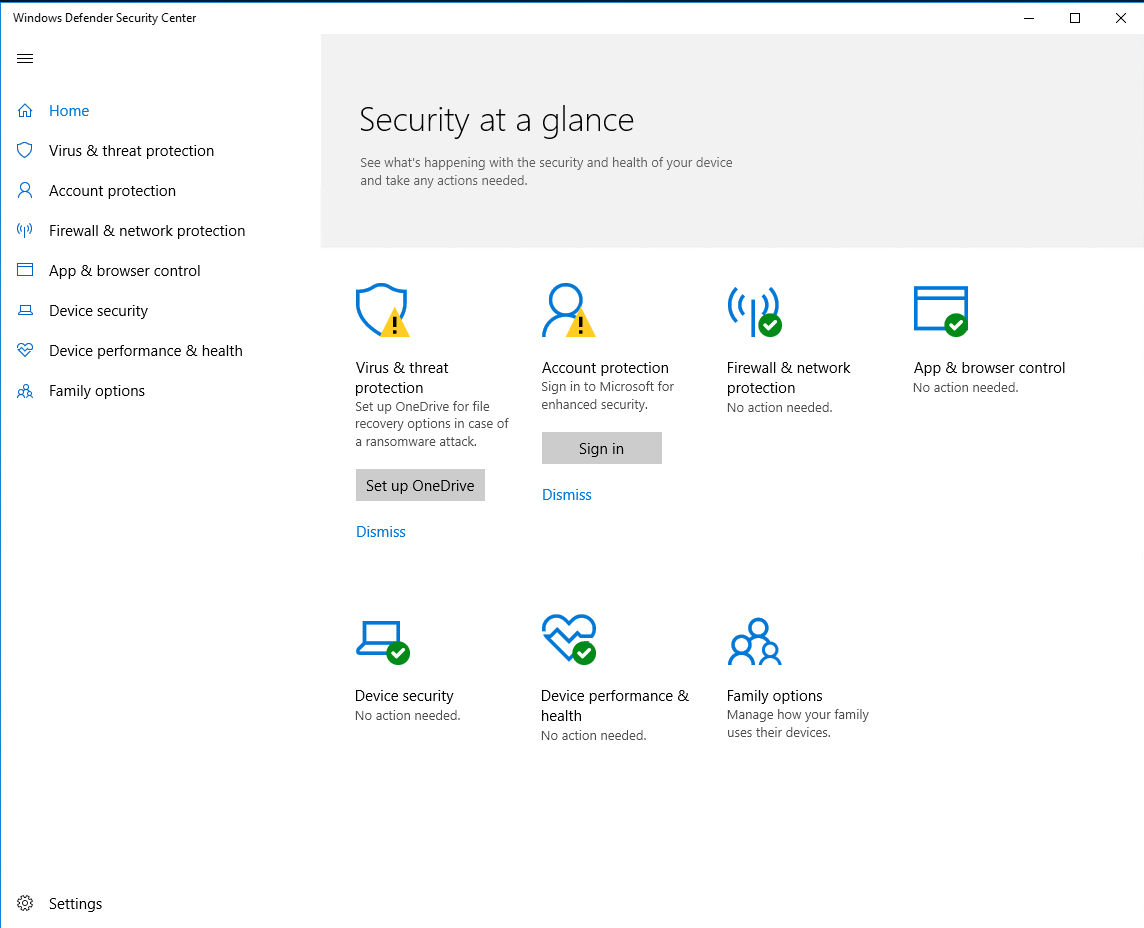
Windows 11 enkele tools die je helpen je bij het realtime beveiligen van je PC tegen virussen, spyware en andere kwaadaardige software.

Je kan deze openen en bekijken via Windows Security. Windows Security kan je openen door er naar te zoeken in de Windows zoekbalk, of te gaan via Settings -> Privacy & security -> Windows Security -> Open Windows Security.



A screenshot of a computer

Description automatically generated



|  |  |  |
| --- | --- | --- |
| **Microsoft Defender Antivirus** | **Windows Firewall** | **Windows SmartScreen** |

### Microsoft Defender Antivirus

Wanneer Microsoft Defender een verdachte toepassing of andere onbekende software detecteert, wordt in een Microsoft-database gecontroleerd of deze potentieel schadelijk is. Microsoft Defender volgt automatisch bekende malware maar je kunt ook bijgewerkte lijsten krijgen wanneer je maar wilt.

Deze definities worden automatisch bijgewerkt zodra je ‘Virus & threat protection updates’ selecteert en dan op ‘Check for updates’ klikt.

Microsoft Defender wordt op de achtergrond uitgevoerd en je krijgt alleen een melding als er specifieke handelingen moeten worden verricht. Je kunt ook een eigen scan laten uitvoeren wanneer je maar wilt. Als je pc niet goed werkt of als je van iemand een e-mail hebt gekregen die er verdacht uitziet, gebruik je best Microsoft Defender om te controleren of je niet onbedoeld malware hebt gedownload.

Om je defender te testen kan je gebruik maken van de volgende site:

<https://demo.wd.microsoft.com/>

|  |
| --- |
| **Opdracht:**  Probeer de Cloud-delivered Protection uit. Download de unsafe file en zorg dat je antivirus de threat detecteert. Bekijk the threat en verwijder via de antivirus het bestand. |

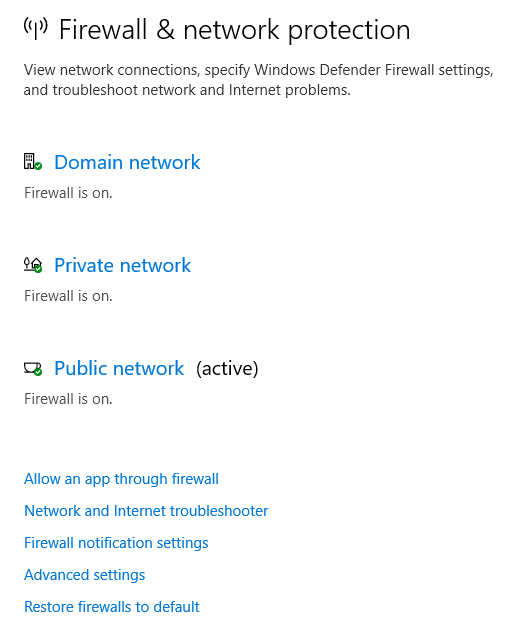
De tool gebruikt groene, gele en rode kleurcodes om de beveiligingsstatus van je pc weer te geven.

Make sure your PC doesn’t turn into something obscene, and keep it green! https://static-cdn.jtvnw.net/jtv_user_pictures/chansub-global-emoticon-2cde79cfe74c6169-24x18.png

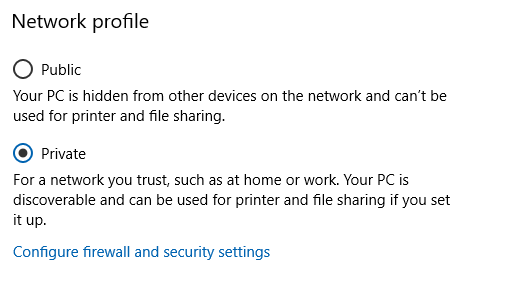


### Windows Firewall

Wanneer je de Firewall settings opent zal je direct merken dat er een verschil wordt gemaakt tussen Domain, Private en Public Network.

Men spreekt over een **domein netwerk** wanneer de computer geconnecteerd is met een Domain Controller en verbonden is met dat bepaalde netwerk.

Tussen Publiek en Private kan de gebruiker zelf kiezen. Dit doe je in de netwerkinstellingen.

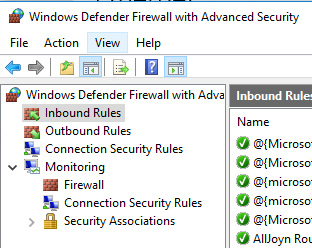


Een **privé netwerk** is voor een netwerk dat je vertrouwt, waarbij andere PC’s jou makkelijk kunnen en mogen detecteren.

Een **publiek netwerk** is kort gezegd voor al de rest. Denk aan de school (indien je niet bent geconnecteerd met de domain controller), een internetcafé, ziekenhuis, etc…

Natuurlijk willen wij onze firewall zelf kunnen instellen door bepaalde toegang te verlenen of te weigeren. Een makkelijke manier is om je applicaties rechten te geven of te ontnemen door de ‘Allow an app through firewall’ optie te kiezen. Je zal merken dat de aangeboden opties vrij beperkt zijn. Zo kan je bv. niet kiezen welke poorten je al dan niet wenst toe te laten. Om dit te doen zal je moeten kiezen voor de ‘Advanced Settings’ optie.

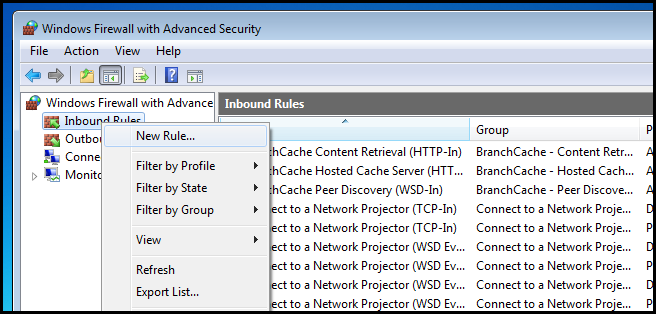
Je zal merken dat je drie soorten rules (beveiligingsregels) kunt instellen.



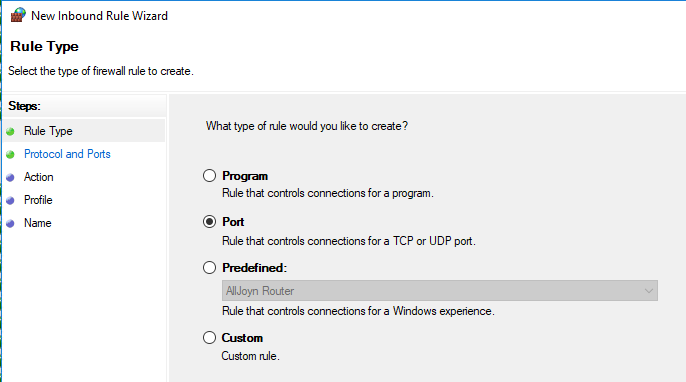
**Inbound:** Binnenkomende requests van het netwerk naar jouw PC.

**Outbound:** Uitgaande trafiek (afkomstig van jouw applicaties).

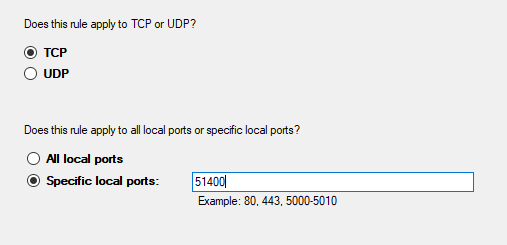
**Connection Security Rules:** Regels om PC’s te verbinden via IPsec. Hiermee kan je instellen dat een Computer moet geauthentiseerd zijn of dat de connectie wordt geweigerd.

Je kan een nieuwe regel aanmaken door te rechterklikken op Inbound rules en ‘New Rule…’ te selecteren.

Je kan zelf experimenteren, maar maak voorlopig een regel aan die een poort open zal zetten.



Kies voor TCP protocol en kies poort 51400



En laat deze toe op alle netwerken.

|  |
| --- |
| **Opdracht:**   * Zeg aan de docenten dat je klaar bent om je poort te testen en geef hen je ip-adres. Zij zullen vanaf dan pakketjes naar jouw PC sturen (naar poort 51400). * Ga naar <https://eternallybored.org/misc/netcat/> en download netcat 1.12 * Windows defender zal dit aanzien als een hacking tool. Je zal de tool dus moeten whitelisten (toelaten) * Gebruik volgende commando in cmd om te luisteren naar de poort   **nc -L -p 51400**   * Indien je tekst ziet verschijnen staat je poort open. * Sluit deze poort (via de firewall) en kijk of de berichten stoppen. * Je kan netcat ook gebruiken om berichten te versturen naar een bepaalde poort. Zoek dit op en test uit.   (Op de site <https://packetsender.com> kan je een handig grafisch tooltje vinden om packages te versturen naar een bepaalde poort) |

|  |
| --- |
| **Opdracht:**   * Ping wil niet werken tussen de VM’s onderling indien deze niet op het domein zitten. Om dit op te lossen kan je de firewall instellen zodat een medestudent je wel mag pingen. * Pas de ‘Inbound Rules’ aan. Zorg ervoor dat File and Printer Sharing (Echo Request – ICMPv4-In) op enabled staat voor alle profielen (domain, private, public). Zodat deze de trafiek toelaat. * Test dit uit met een andere student en zorg dat hij/zij antwoord krijgt wanneer hij/zij naar jou pingt. |

