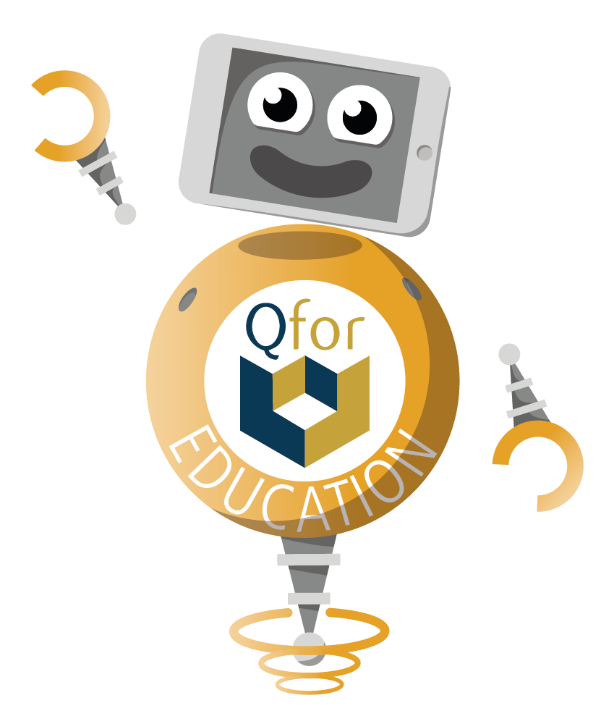
MEM Intune – Labs

Tuur Housiaux



Inhoudsopgave

[MEM Intune – Labs 1](#_Toc107227780)

[Inhoudsopgave 2](#_Toc107227781)

[Labo 01 – REGISTRATIE MEM INTUNE 3](#_Toc107227782)

[Labo 02 – Add Subscriptions 6](#_Toc107227783)

[Labo 03 – VPN + explore LAB 7](#_Toc107227784)

[Labo 04 – Create Users 9](#_Toc107227785)

[Labo 05 – Create Groups 11](#_Toc107227786)

[Labo 06 – Multifactor Authentication 13](#_Toc107227787)

[Labo 07 – Azure AD Self Service Password Reset 14](#_Toc107227788)

[Labo 08 – Corporate Branding 16](#_Toc107227789)

[Labo 09 – Device Join 19](#_Toc107227790)

[Labo 10 – Device Group 21](#_Toc107227791)

[Labo 11 – Compliancy rule 22](#_Toc107227792)

[Labo 12 – notifications 23](#_Toc107227793)

[Labo 13 – Add script 24](#_Toc107227794)

[Labo 14 – Conditional Access 26](#_Toc107227795)

[Labo 15 – Device profile - restrictions 28](#_Toc107227796)

[Labo 16 – Microsoft Store App 29](#_Toc107227797)

[Labo 17 – Microsoft 365 App 31](#_Toc107227798)

[Labo 18 – Win 32 App 32](#_Toc107227799)

[Labo 19 – Winget 34](#_Toc107227800)

[Labo 20 – Windows Update rings 37](#_Toc107227801)

[Labo 21 – Autopilot 38](#_Toc107227802)

[EXTRA 01 – BULK-USERS 41](#_Toc107227803)

[Extra 02 – Brand company portal 42](#_Toc107227804)

[Extra 03 – Change Domain Name (niet uit te voeren zonder extra kosten) 43](#_Toc107227805)

[Extra 04 – Azure AD connect 44](#_Toc107227806)

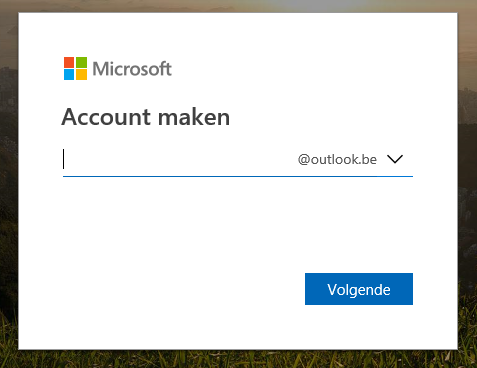
[Extra 05 – Chocolatey 45](#_Toc107227807)

[Extra 07 – Configuration Policies 46](#_Toc107227808)

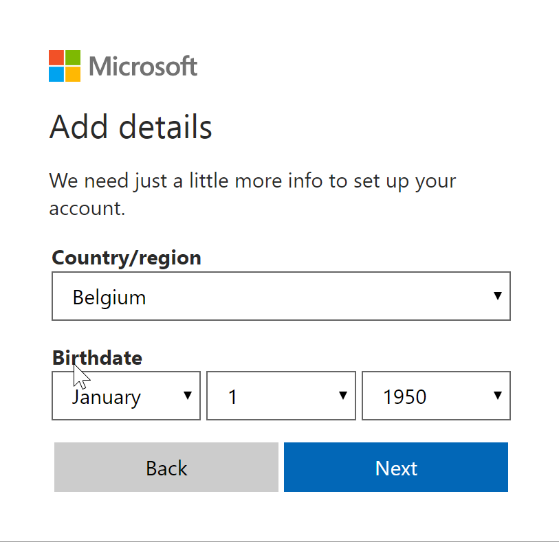
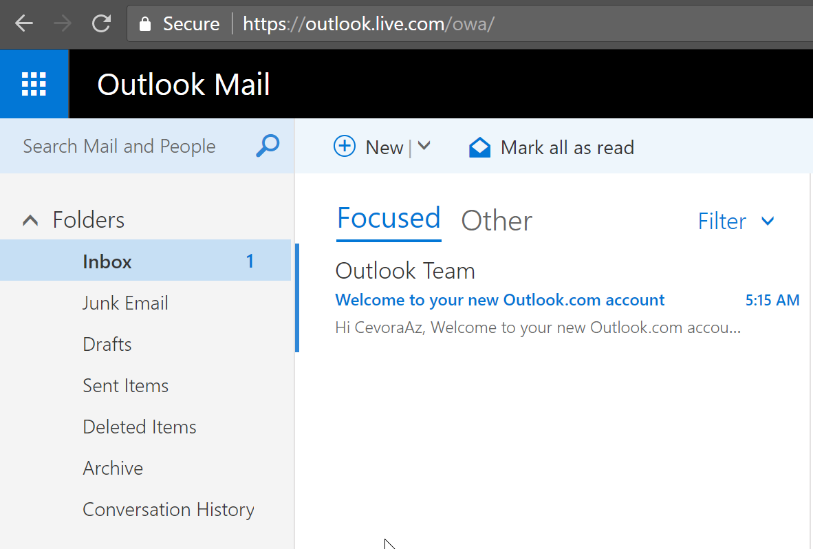
Labo 01 – REGISTRATIE MEM INTUNE

## DEELOPDRACHT 1: REGISTRATIE MAIL-ACCOUNT

* Gebruik een incognito sessie in je browser, ga naar <http://www.outlook.com>, maak een Microsoft Live ID (Microsoft Account).
* Selecteer Create Account \ gratis account maken

Graphical user interface, application

Description automatically generated

* Kies voor een uniek email adres en complex wachtwoord. Deze wordt later nog gebruikt vb.: [It11306tri@outlook.com](mailto:It11306tri@outlook.com).
  + Let op wachtwoorden kunnen gevraagd worden voor troubleshooting door de trainer. Kies dus niet voor een persoonlijk wachtwoord!
  + Vb.: Azerty01
* Vul First en Last name in. Dit mag fictief zijn.
* Geef een geboortedatum op (mag ook fictief zijn).  
  
* Voer de gevraagde verificatie-stappen uit.
* Geef de tijdzone mee en doorloop de wizard verder tot je in Outlook Web Mail zit.   
  

## DEELOPDRACHT 2: REGISTRATIE INTUNE SUBSCRIPTION

* Open een browser en surf naar [www.aka.ms/trial](http://www.aka.ms/trial)
* Doorloop alle stappen:
  + Bij Let’s get you started geef je het emailadres op dat je hebt aangemaakt in deelopdracht1.
  + Duw op next en dan op set up account
  + Bij het onderdeel “about you” geef je de volgende informatie en klik je op Next:

(Hier maken we eigenlijk een Microsoft Azure tenant aan)

* + - First Name: jouw voornaam
    - Last Name: jouw familienaam
    - Business email address: geef je emailadres uit deelopdracht 1 mee
    - Business phone number: geef je persoonlijk telefoonnummer op
    - Company name: “StudentXXX”-IT (bvb, Janssens-IT)
    - Size: 10-24
    - Country: Belgium
* Duw nu op next
* Bij het volgende scherm vraag je een bevestigingscode op voor het afronden van de registratie. Kies om een tekstbericht te krijgen. Wanneer je de code ontvangt, geef je de 6-cijferige code in.
* Bij het onderdeel “Sign in details” geef je de volgende informatie:
  + Enter a user name: eerste letter voornaam + . + familienaam (bvb, j.janssens)
  + Domainname: naar keuze (wel onthouden)
  + Password: paswoord naar keuze (gelieve te onthouden)
* Duw op Next en daarna op get started

Graphical user interface, text, application, email

Description automatically generated

Labo 02 – Add Subscriptions

## DEELOPDRACHT 1: ADD LICENCES

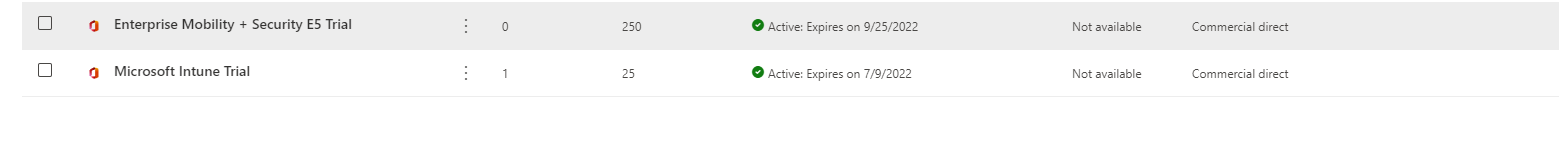
In deze oefening gaan we een extra licentie toevoegen aan onze MS365 omgeving

* Ga naar het admin center van Microsoft 365 = <https://admin.microsoft.com/>
* Browse naar “Billing” -> “Purchase services” en zoek voor “Microsoft 365 E5”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Kies voor manage trial
* Geef je telefoonnummer
  + Als je op problemen komt:
    - Druk op doorgaan om naar jouw facturatiegegevens te komen
    - Geef hier jouw adres op (geen BTW-nummer of andere zaken!)
* Geef de verificatiecode
* Klik op Start using Trial (nu uitproberen)
* Ga nu naar Billing\Your products
  + Hier zie je nu 2 producten staan



Labo 03 – Setup Intune

## DEELOPDRACHT 1: Device Enrollment inschakelen

We gaan device enrollement inschakelen zodat nieuwe devices kunnen gedetecteerd en beheerd worden door Intune

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices > Enroll devices
* Kies hier voor automatic enrollment
  + MDM user scope > All
  + MAM User scope > All

## EXTRA DEELOPDRACHT : Android Enrollment inschakelen

We gaan device enrollement inschakelen zodat nieuwe android devices kunnen gedetecteerd en beheerd worden door Intune

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices > Android
* Kies voor Android Enrollment
  + Managed google play
    - I accept
    - Start google to make connection

Maak een nieuw google-account aan. Doorloop alle stappen, vermijdt het toevoegen van je echt telefoonnumer, adres, etc buiten voor gsm-verificatie

* Na de connectie verkrijg je nu dit:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Kies voor de optie corporate-owned ,fully managed user devices
* Kies voor yes
* Je krijgt nu een QR-code te zien, deze kunnen eindgebruikers inscannen om hun device te enrollen

Labo 04 – Create Users

## DEELOPDRACHT 1: User Aanmaken

We gaan een user aanmaken via de admin portal en deze verwijderen

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar users en kies bij all users voor de optie “new user”

Graphical user interface, text, application, Word

Description automatically generated

* Geef volgende gegevens op:
  + Username: GuustFlater
  + Name: Guust Flater
  + First Name: Guust
  + Last Name: Flater
  + Wachtwoord: geef een wachtwoord mee
    - Noteer deze: …………………………
* Alle andere informatie laat je voor nu zo staan, duw op create

## DEELOPDRACHT 2: Delete User

We gaan een user volledig verwijderen

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar users
* Selecteer de user Guust en Click op “**Delete User”**
* Druk op **confirm Changes.**

De user bevindt zich nu in de “Deleted Users” Recycle bin. Controleer dit

## DEELOPDRACHT 3: Delete User permanent

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naardeleted users
* Selecteer de user Guust en Click op “**Delete permanently”**

## DEELOPDRACHT 4: Aanmaken users

Zorg ervoor dat volgende users zijn aangemaakt **of kies ervoor om de extra opdracht bulk users aan te maken**

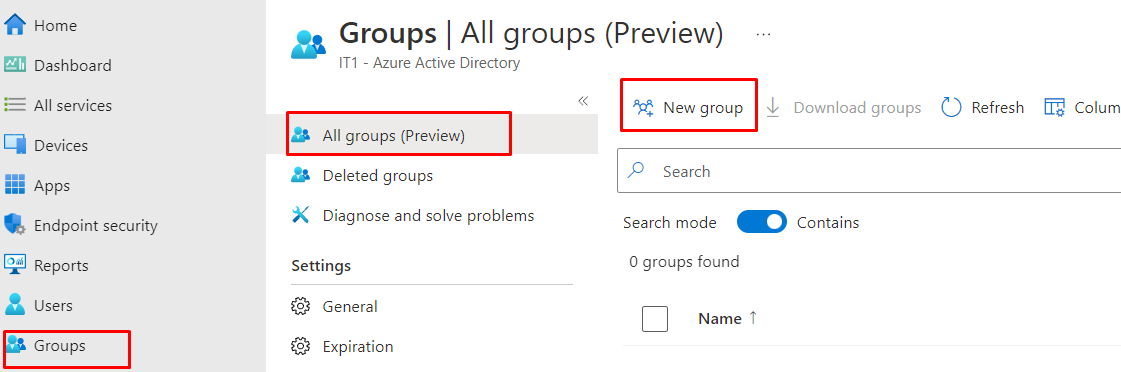
* Bas Schutte
* Sander Strauss
* Teunis Hake
* Lammert Homan
* Tom Ras
* Lammert Kess
* Mariska Cramp
* Marloes Van Rooy
* Paulien Tempel
* Willeke Drayer
* Paulien Goossen
* Paula Van Rooy

Labo 05 – Create Groups

## DEELOPDRACHT 1: Group Aanmaken

We gaan een group aanmaken via de admin portal

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar groups en kies bij all groups voor de optie “new group”



* Geef volgende gegevens op:
  + Group type: Security
  + Group Name: GS\_SALES
  + Group description: Sales users
  + Membership: Assigned
  + Members: Bas, Sander, Teunis
* Alle andere informatie laat je voor nu zo staan, duw op create

## DEELOPDRACHT 2: Edit user

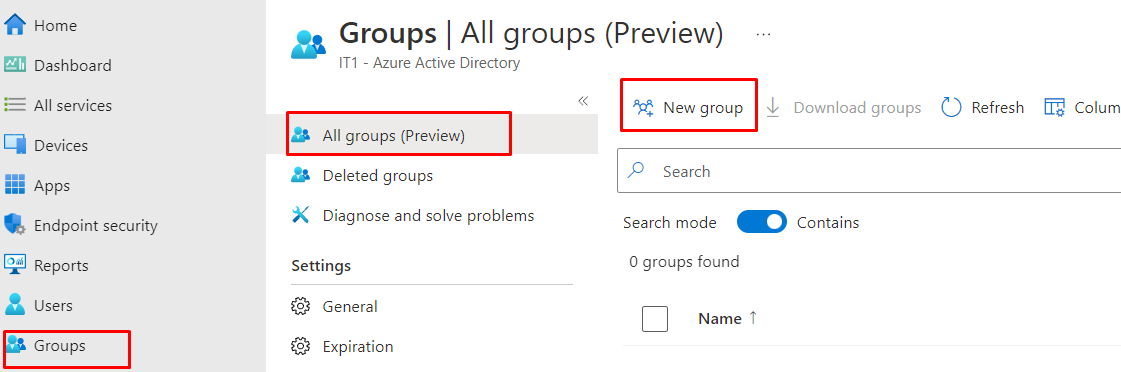
We de gebruikers aanpassen om te laten toevoegen via dynamic rules

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar users en slecteer bij all users de gebruiker Lammert H.
* Duw op edit
* Bij Job info geef je het departement Marketing mee
* Duw op save
* Doe hetzelfde voor Tom en de andere Lammert

## DEELOPDRACHT 3: Dynamic group Aanmaken

We gaan een dynamic group aanmaken via de admin portal en deze verwijderen

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar groups en kies bij all groups voor de optie “new group”



* Geef volgende gegevens op:
  + Group type: Security
  + Group Name: GS\_MARKETING
  + Group description: Marketing users
  + Membership: Dynamic User
  + Duw op de blauwe link: add dynamic rule
    - Bij property: Department
    - Operator: Equals
    - Value: Sales
    - Duw op Save
  + Duw op Create
* Maak van de sales groep ook een dynamische groep
* De volgende gebruikers behoren toe aan het departement Administratie, zorg dat deze ook lid zijn van de groep GS\_Administratie:
  + Mariska Cramp
  + Marloes Van Rooy
  + Paulien Tempel
  + Willeke Drayer
  + Paulien Goossen
  + Paula Van Rooy

Labo 06 – Add licence to group

## DEELOPDRACHT 1: Group Aanmaken

We gaan een licence toevoegen aan een groep

* Ga naar: <https://aad.portal.azure.com/>
* Klik op Azure Active Directory > Licenses
* Kies hier voor “All products”
* Selecteer Microsoft 365 E5

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Ga naar Licensed groups en duw op Assign
* Duw op add users and groups, voeg volgende groepen toe
  + GS\_Administratie
  + GS\_Marketing
  + GS\_Sales
* Zorg ook dat jouw account is toegevoegd
* Duw op review and assign
* Duw op assign

## DEELOPDRACHT 2: Controle

LET OP: voordat je deze stap kan uitvoeren moet je ongeveer 10 minuten wachten

* Ga naar: [admin.microsoft.com/](https://aad.portal.azure.com/)
* Onder users kies je voor active users
* Je zal merken dat alle accounts een licentie hebben

Labo 07 – Corporate Branding

## DEELOPDRACHT 1: Corporate Branding - login

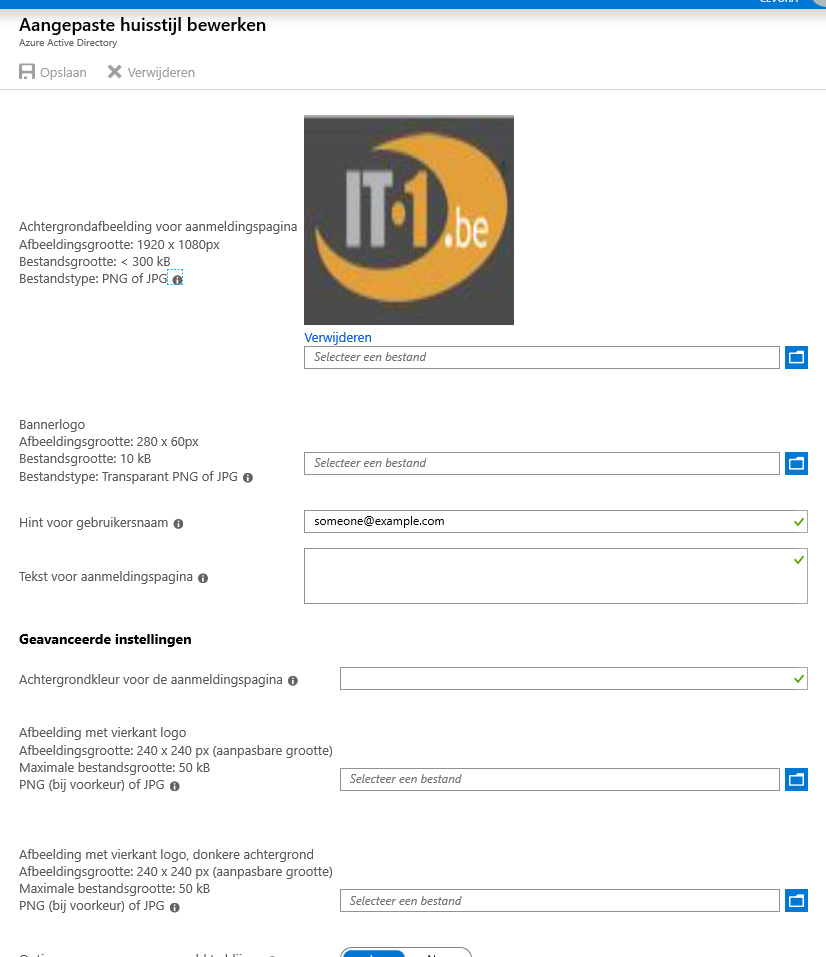
* Open een web-browser en open www.aad.portal.azure.com
* Open Azure Active Directory en ga naar “company branding”

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Klik op default
* Bij de achtergrondafbeelding kies je voor een foto naar keuze
* Bij banner-logo ook

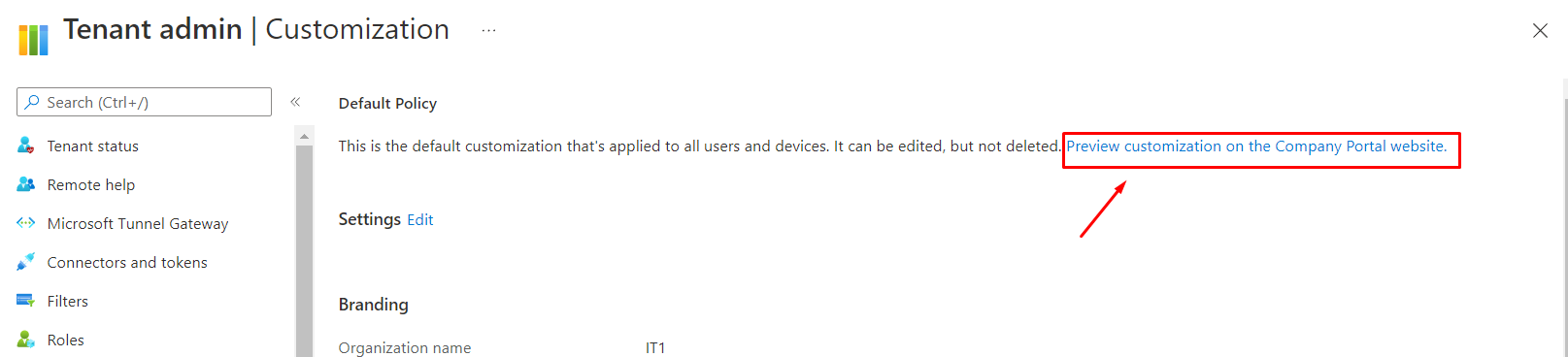
Kijk zelf naar de andere instellingen en pas dit eventueel zo goed mogelijk aan voor je eigen bedrijf



## DEELOPDRACHT 2: Corporate Branding - Intune

* Ga naar: <https://endpoint.microsoft.com/>
* Browse naar “tanant administration” > Customization
* Duw op edit
* Verander de instellingen naar keuze
* Duw op review + save
* Duw op save

Tip: je kan de policy testen door hierop te duwen:



Labo 08a – Windows device Prep

## DEELOPDRACHT 1: Create devices

* Ga naar <https://security.microsoft.com>
* Ga hier naar endpoint > Evaluation and labs
* Kies voor evaluation labs
  + Heb even geduld , 10-15 minuten
* Kies voor setup lab
  + 3 devices 72 hours each + Next
  + Bij simulators agent duw je op next
  + Bij summary duw je op setup lab
* Je krijgt nu volgend overzicht:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Ga naar devices en duw op add device
* Kies voor Windows 10
  + Sla pc-naam, username en password op!
* Heb geduld tot wanneer de virtuele machine is aangemaakt en probeer te connecteren hiernaar.
* **Maak ook een testmachine2 aan**

Labo 08b – Android device Prep

## DEELOPDRACHT 1: Download Android studio

* Open een web browser en geef de zoekterm android studio op
* Download dit programma en zorg dat deze geïnstalleerd is.
* Na de installatie kom je op dit scherm:

Afbeelding met tekst, schermafbeelding, mobiele telefoon

Automatisch gegenereerde beschrijving

* **Kies voor more actions en virtual device manager**
* **Duw op create device > Pixel 4, duw op next**
* **Kies bij R voor download en wacht tot alles is gedownload, duw op next**
* **Geef dit een naam: Android\_Clean**
* **Duw op finish**

Afbeelding met tekst, schermafbeelding, monitor, scherm

Automatisch gegenereerde beschrijving

* **Kies bij android\_clean voor duplicate**
* **Geef dit de naam Android\_1**
* **Start deze op**

Labo 09a – Device Join

## DEELOPDRACHT 1: Add Azure AD registered Device

* Connecteer naar testmachine1
* Login met de gegevens
* Ga naar Settings en dan naar accounts
* Kies voor Access Work or school
* Duw op connect
* Geef de gegevens op van een user met bijhorend wachtwoord (geen admin-rechten nodig)
* Doorloop alle stappen tot je dit ziet:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

## DEELOPDRACHT 2: Add Azure AD joined Device

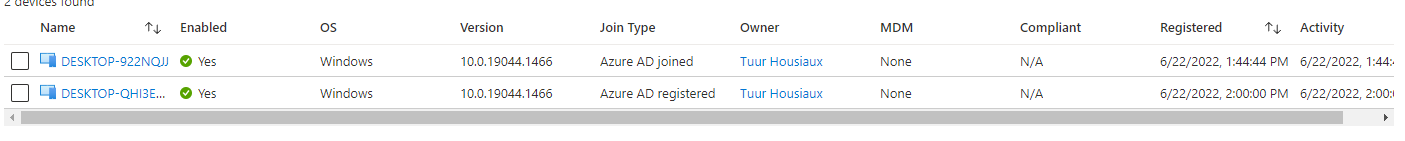
* Open de remote console manager en ga naar testmachine2
* Login met de gegevens
* Ga naar Settings en dan naar accounts
* Kies voor Access Work or school
* Duw op connect
* Kies hier voor “Join his device to Azure Active Directory”
* Geef de gegevens op van een user met bijhorend wachtwoord (geen admin-rechten nodig)
* Bij de popup “Make sure this is your organization” duw je op join”
* Doorloop alle stappen tot je dit ziet:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

## DEELOPDRACHT 3: Controle device join

* Login op <https://aad.portal.azure.com>
* Ga naar Azure Active Directory
* Ga naar devices>All devices
* Hier zie je dit (namen devices zijn anders)



* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar devices en kies bij all devices, ook hier moeten deze devices onder te vinden zijn. Dit kan echter even duren…

Labo 09b – Android device Join

## DEELOPDRACHT 1: personal device

* Connecteer naar Android\_1
* Open de google play store, log eventueel in met je gmail account dat je daarnet hebt aangemaakt.
* Download de app “company portal”
* Connecteer met jouw mailadres en doorloop alle stappen.
* Jouw device wordt nu geregistreerd als een persoonlijk device

Labo 10 – Device Group

## DEELOPDRACHT 1: Azure AD registered Device

Zorg dat je een extra testmachine maakt met os windows 11 en zorg dat dit een een Azure AD joined device wordt. Indien je dit niet meer goed weet, bekijk labo 8 en 9

## DEELOPDRACHT 2: Device group Windows 10

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar groups> All groups
* Kies voor new group
* Geef volgende info:
  + Type: Security
  + Name: Windows 10 devices
  + Description: Oplijsiting alle Windows 10 devices
  + Membership Type: Dynamic Device
* Duw op het blauwe “Add dynamic Query”
  + Property: Device OS version
  + Operator: Contains
  + Value: 10.0.1
  + Ga naar validate rules, voeg alle gevonden devices toe. Hier kan je valideren welke devices gevonden zijn.  
    Dit zijn er momenteel 2. Een AAD registered en AAD joined device
  + Ga terug naar configure rules
  + Duw op Add expression
    - Property: Management Type
    - Operator: Equals
    - Value MDM
  + Controleer hoeveel er nu gevonden zijn bij validate
  + Duw op save
* Duw op create

## DEELOPDRACHT 3: Device group Windows 11

* Maak ook een device groep voor alle Windows 11 AAD registered devices.
* Tip: Gebruik hiervoor de value 10.0.2 ipv 10.0.1

## EXTRA DEELOPDRACHT: Device group Personaly owned device

* Maak ook een device groep voor alle android personal devices
* Zorg voor volgende syntax:

(device.deviceOSType -contains "Android") and (device.deviceOwnership -eq "Personal")

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Labo 11a – Windows Compliancy rule

## DEELOPDRACHT 1: Compliancy rule

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> Compliance policies
* Kies hier voor “+create policy”
  + Platform: Windows 10 and later
* Duw op create
* Geef als naam: Bitlocker check
* Duw op next
* Ga hier naar device health en zet “require bitlocker” op require
* Duw op next
* Bij actions duwen we op next
* Bij Assignments geef je de Windows 11 groep mee
* Duw op next en create

## DEELOPDRACHT 2: Test compliancy rule

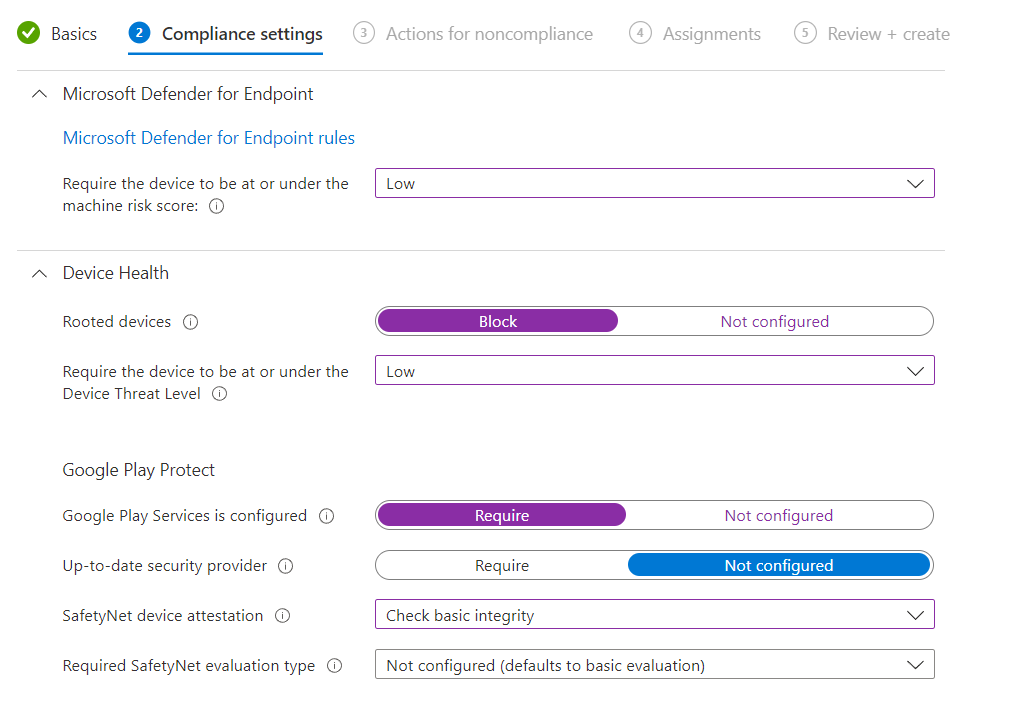
* Test of de windows 10 device compliant is of niet. Dit kan je doen door:
  + Ga naar: <https://endpoint.microsoft.com/>
  + Navigeer naar Devices> compliancy policies
  + Selecteer de aangemaakte policy
  + Ga naar device status
    - Hier zie je de status van je device

Als dit blijft staan op not applicable dan komt dit doordat deze PC’s (het zijn virtuele machines) geen bitlocker supporteren.

Labo 11b – Android Compliancy rule

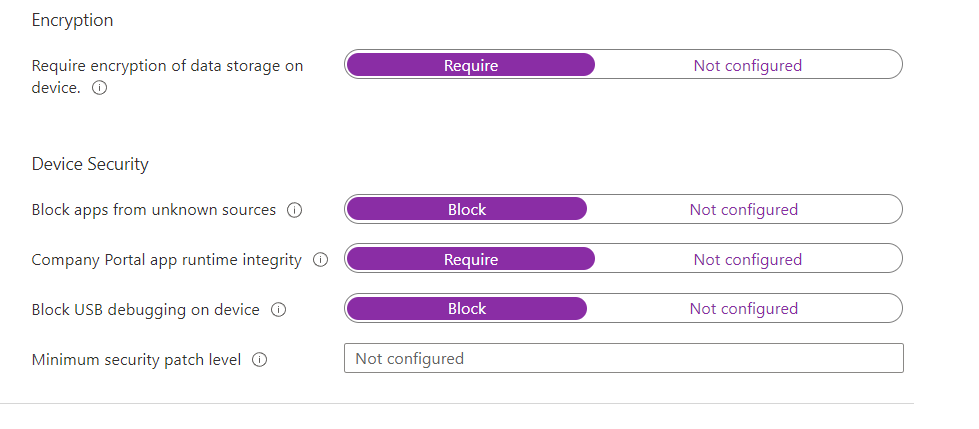
## DEELOPDRACHT 1: Compliancy rule

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> Android
* Compliancy policies
* Kies hier voor “+create policy”
  + Platform: Android enterprise
  + Type: Personally owned
* Duw op create
* Geef als naam: Personally owned android
* Duw op next
* Zorg voor volgende settings



Afbeelding met tekst

Automatisch gegenereerde beschrijving



* Duw op next
* Bij actions duwen we op next
* Bij Assignments geef je de personal android devices groep mee
* Duw op next en create

Labo 12 – notifications

## DEELOPDRACHT 1: Aanmaken notificatie

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> Compliance policies
* Kies hier links voor notifications
* Duw op “+ create notification”
* Geef als naam: Bitlocker warning op
* Duw op create
* Geef als naam: Bitlocker notification
* Duw op next
* Geef volgende gegevens op:
  + Locale: Dutch
  + Subject: Waarschuwing bitlocker
  + Message: “Let op jouw computer is momenteel niet geëncrypteerd en dus een gevaar wanneer deze wordt gestolen”
  + Is default = aangevinkt
* Duw op next
* Duw op create

## DEELOPDRACHT 2: Linken aan bestaande compliance rule

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> Compliance policies
* Selecteer « bitlocker check »
* Ga naar properties
* Bij « actions for non compliance » duw je op edit
* Voeg een actie toe door volgende gegevens door te geven:
  + Action: Send email to end users
  + Schedule: 30 dagen
  + Message template: bitlocker warning
  + Duw op review + save

Labo 13 – Add script

## DEELOPDRACHT 1: Aanmaken Powershell script

* Open een editor (notepad, notepad++, Powershell ISE) en kopieer het volgende:

net stop w32time

w32tm /config /syncfromflags:manual /manualpeerlist:"0.be.pool.ntp.org 1.be.pool.ntp.org 2.be.pool.ntp.org 3.be.pool.ntp.org"

net start w32time

w32tm /config /update

w32tm /resync /rediscover

tzutil /s "Romance Standard Time"

* Bewaar dit script als time.ps1

## DEELOPDRACHT 2: Adding script in Intune

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> scripts
* Kies hier voor “+Add”
  + Windows 10 and later
* Name: time script
* Script settings: laad time.ps1 op, de rest lat je default staan. Duw op next
* Bij assignment geef je alle devices op. Duw op next.
* Duw op add

## DEELOPDRACHT 3: Test script

* Login op testclient1 met jouw azure AD user
* Open powershell en voer volgende commando uit:
  + w32tm /query /configuration
* Na enige tijd zal je dit verkrijgen (indien niet, log uit en terug in)

Afbeelding met tekst

Automatisch gegenereerde beschrijving

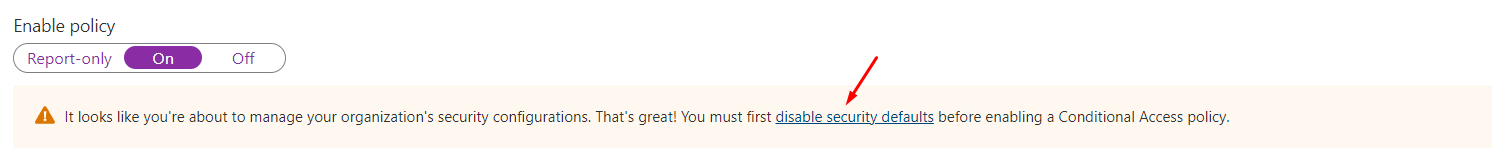
Labo 14 – Conditional Access

## DEELOPDRACHT 1: Opvragen IP-gegevens

* Type in google what’s my ip
* Kopieer het ip-adres zodat je deze later kan gebruiken
* Zorg ook dat je de netmask kan terugvinden (dit ziet eruit als /13 of /17))

## DEELOPDRACHT 2: Aanmaken conditional access

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> conditional access
* Ga naar named locations
* Selecteer « +IP ranges location »
  + Name : Hoofdkantoor
  + Markeer als trusted
  + Duw op het +-icoon en voeg daar het ip-adres in van “what’s my ip” samen met de netmask
  + Duw op create
* Ga nu naar policies en kies voor “new policy”
  + Name: MFA Hoofdkantoor
  + Users: All users
  + Conditions: location
    - Configure: yes
    - Exclude
    - Selected locations: hoofdkantoor
    - Duw op select
  + Conditions: device platform
    - All devices
  + Grant: require MFA
  + Enable policy: on
  + Je ziet ook dit staan:



* + Duw op disable security defaults
    - Zet dit op No, my company is using conditional access
    - save
  + Duw op create

## DEELOPDRACHT 3: Testen conditional access

* Log uit en log terug in op endpoint.microsoft.com
* Is er terug achter MFA gevraagd?
  + Let op: dit wordt voor administrators aanschouwt als een security risico en zal dus vaak automatisch teruggezet worden voor administrators. Gebruik voor testen een andere users.
  + Let op: Bij eerste keer inloggen kan hij wel steeds vragen om extra verificiatiemogelijkheden toe te voegen. Dit heeft evenwel niets met MFA te maken.  
    Je kan dit testen door hierna eens terug uit en in te loggen

Labo 15 – Device profile - restrictions

## DEELOPDRACHT 1: Aanmaken device profile

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar Devices> « configuration policies »
* Duw op create profile
  + Platform : Windows 10 and later
  + Type : templates
  + Template name : device restrictions
  + Duw op create
* Geef de naam « background company” op en duw op next
* Bij de settings navigeer je naar personalization
* Geef de URL op van de gewenste afbeelding
* Duw op next
* Zorg dat het toegepast wordt op alle devices, duw op next
* Bij rules geef je op dat hij moet toegepast worden als de OS editie Windows 10/11 is.
* Duw op create

## DEELOPDRACHT 2: Test background

* Login op CL01 met jouw azure AD user
* Na enige tijd zal je jouw achtergrond verkrijgen (indien niet, log uit en terug in)
  + Dit heeft tijdens de testfase langer dan 15 minuten geduurd

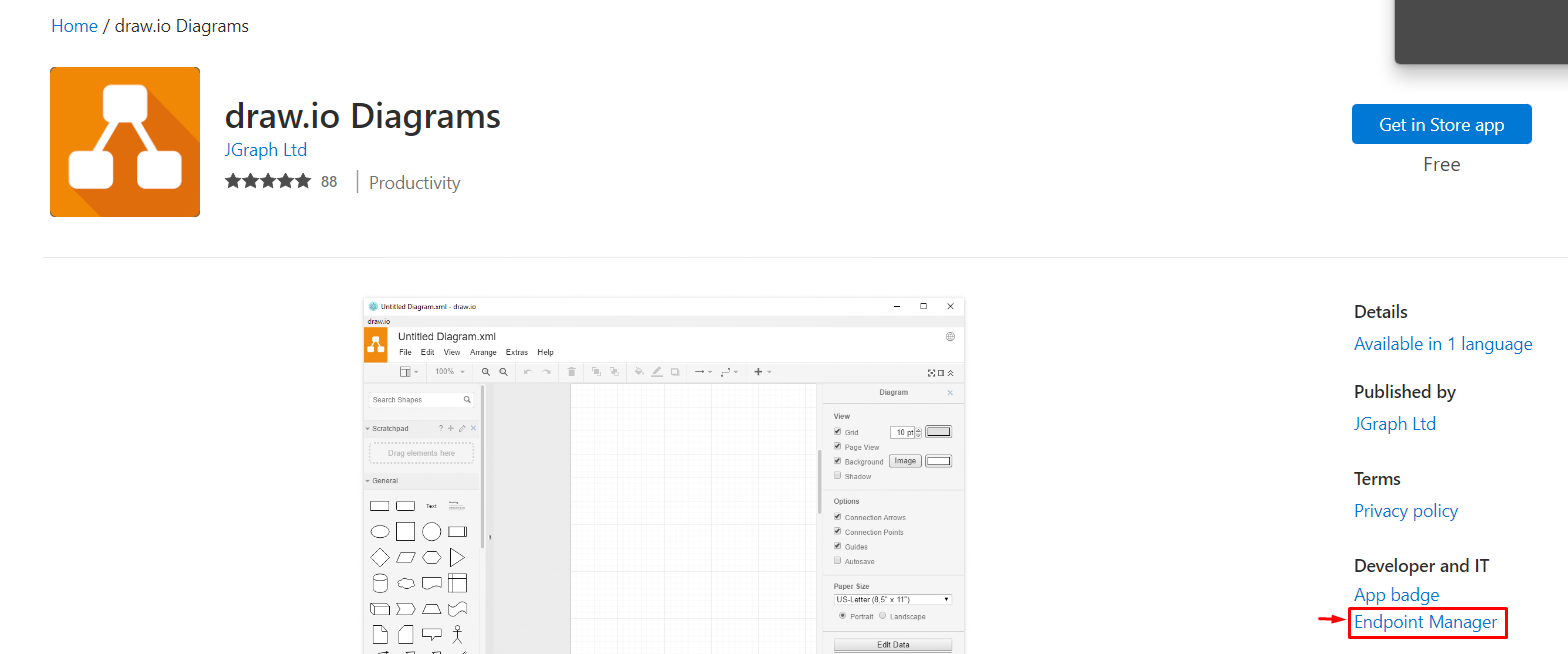
Labo 16 – Microsoft Store App

## DEELOPDRACHT 1: Install company Portal

* Login op CL01 met jouw Azure AAD user
* Open de Microsoft store en zoek naar de app company portal
* Installeer deze.
* Vanaf dat deze is geïnstalleerd, open je de app
* Bij home zie je staan “This device hasn’t been set up…”, klik hierop
* Duw op Next en dan op connect, je zal merken dat jouw mailadres automatisch wordt gevonden maar dat je je nog moet authenticeren.
* Geef je wachtwoord op en duw op next tot je terug in je company portal bent.

## DEELOPDRACHT 2: Add Microsoft store App

* Open de web-browser en ga naar <https://apps.microsoft.com/store>
* Zoek hier voor de app genaamd “Draw.io”
* Kies voor de link naar endpoint manager



* Kopieer de URL en zorg dat je deze bewaard, deze hebben we later nodig
* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar apps > All Apps
* Kies hier voor Add
* Bij het type kies je voor een Microsoft Store App, duw op select
* Geef volgende gegevens mee:
  + Name: Draw Diagrams
  + Description: Hier kan flowcharts mee maken
  + Publisher: Jgraps Ltd
  + Appstore URL: (je gekopieerde URL)
  + Catergory: Productivity
  + Show this feature…= Yes
  + De rest laat je zo staan
* Duw op next
* Bij Assignments duw je op add all users, duw op next
* Bij review en create duw je op create.

## DEELOPDRACHT 3: Test Microsoft store App

* Login op CL01 met jouw azure AD user
* Open de company portal
* Bekijk of je Draw.io kan terugvinden onder apps. Indien niet:
  + Ga naar settings en duw sync.
  + Dit kan echter even duren.

Labo 17 – Microsoft 365 App

## DEELOPDRACHT 1: Add Microsoft store App

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar apps > All Apps
* Kies hier voor Add
* Bij het type kies je voor een Microsoft 365 Apps > Windows 10 and later. Duw op select.
* Geef volgende gegevens mee:
  + Suite Name: Word en Outlook
  + Description: Microsoft 365 Word en Outlook
  + Zorg dat deze zichtbaar is in het company portaal
  + De rest laat je zo staan
* Duw op next
* Geef volgende gegevens mee:
  + Select Office Apps: Word en Outlook
  + Update Channel: Monthly
  + Languages: Engels, Nederlands en Frans
  + De rest laat je default staan
* Duw op Next
* Bij Assignments duw je onder Required voor All devices

## DEELOPDRACHT 2: Test Microsoft 365 App

* Login op CL01 met jouw azure AD user
* Open de company portal
* Bekijk of je de app kan terugvinden onder apps. Indien niet:
  + Ga naar settings en duw sync.
  + Dit kan echter even duren.

Normaal moet de installatie automatisch gebeuren, dit kan echter even duren

**Soms kan het zijn dat de app al geïnstalleerd is voordat hij in het portaal verschijnt!**

Labo 18 – Win 32 App

## DEELOPDRACHT 1: Download Intune prep tool & msi Google chrome

* Ga naar: <https://github.com/Microsoft/Microsoft-Win32-Content-Prep-Tool>
  + Of zoek op google naar “win 32 content prep tool”
  + Zoek naar de github verwijzing
* Download deze tool, dit doe je door op code te duwen en dan op download zip

Afbeelding met tekst, monitor, schermafbeelding, scherm

Automatisch gegenereerde beschrijving

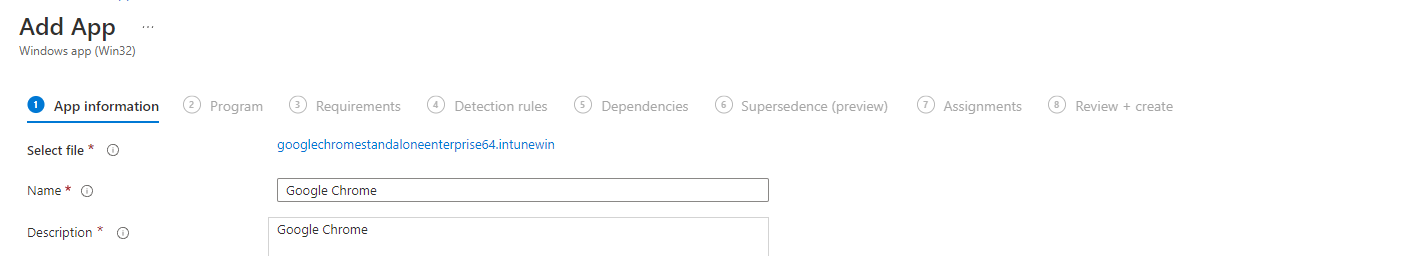
* Extract: “IntuneWinAppUtil.exe” uit deze zip. Deze gaan we nodig hebben.
* We gaan ook de msi van chrome downloaden.
  + Goodle > google chrome msi
  + Open de verwijzing naar de google site. <https://Chromeenterprise.google>
  + Bij file type selecteer je msi en download deze file.
  + Accept and download
  + Verplaats dit bestand naar een (zelfgemaakte folder) C:\Software\Googlechrome

## DEELOPDRACHT 2: Create IntuneWin file

* Open IntuneWinAppUtil.exe
* Je zal een CMD-venster krijgen met enkele vragen:
  + Source folder: C:\Software\Googlechrome
  + Setup file: googlechromestandaloneenterprise64.msi
  + Output Folder: C:\Software\Googlechrome
  + Catalog folder: N
* Het CMD-venster sluit automatisch af
* Ga naar de folder: C:\Software\Googlechrome, je zal hier een INTUNEWIN file zien. Deze gaan we uploaden naar intune en deployen naar de devices.

## DEELOPDRACHT 3: Add win32 App

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar apps > All Apps
* Kies hier voor Add
* Bij het type kies je voor een Other > Windows app. Duw op select.
* Bij select file, browse je naar je intunewin file, open deze en zorg dat deze is ingeladen in Intune. Je verkrijgt dan volgend scherm:



* Bij Publisher geef je nog Google Corporation mee. Zorg ook dat deze app zichtbaar is in het company portaal.
  + Category en Logo mogen ingevuld worden.
* Duw op Next
* Bij Program staat alles juist (dit is het voordeel van een msi)
* Geef volgende requirements mee:
  + OS architecture: 64-bit
  + OS versie: Windows 10 1909
* Duw op next
* Bij detection rules:
  + Manually configure detection rules
  + Duw op Add
    - Kies voor MSi en laat de rest default staan.
    - Duw op OK
  + Duw op Next
* Bij dependencies duw je op next
* Supersedence rules duw je op next
* Assignments: required en All devices. Duw op Next
* Duw op create

## DEELOPDRACHT 4: Test Windows 32 App

* Login op CL01 met jouw azure AD user
* Bekijk of je de app kan terugvinden onder geïnstalleerde apps. Indien niet:
  + Log uit en terug in

Normaal moet de installatie automatisch gebeuren, dit kan echter even duren

Labo 19 – Winget

## DEELOPDRACHT 1: Create ps1 scripts

* Login op CL01 met jouw azure AD user
* Open Powershell en geef volgende CMD-Let in:
  + winget search keeper

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Kopieer de ID van keeper password manager (niet het cijfer)
* Open notepad en type het volgende:
  + winget install --id "JouwID" --exact --accept-package-agreements --accept-source-agreements
* Bewaar dit als InstallKeeper.ps1 onder de folder c:\software\keeper
* Open terug notepad en type het volgende:
  + winget install --id "JouwID"
* Bewaar dit als UnInstallKeeper.ps1 onder de folder c:\software\keeper

## DEELOPDRACHT 2: Create intunewin file

* Zorg dat je deze 2 scripts wrapped naar een intunewin file zoals in labo 10

## DEELOPDRACHT 3: Add win32 App

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar apps > All Apps
* Kies hier voor Add
* Bij het type kies je voor een Other > Windows app. Duw op select.
* Bij select file, browse je naar je intunewin file, open deze en zorg dat deze is ingeladen in Intune. Je verkrijgt dan volgend scherm:

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Volgende informatie geef je op:
  + Name: Keeper
  + Description: Keeper install
  + Publisher: Keeper Security Inc.
  + Company portal: Yes
  + Category en Logo mogen ingevuld worden.
* Duw op Next
* Bij Program geef je het volgende op:
  + Install: powershell.exe -executionpolicy Bypass -file .\installkeeper.ps1
  + Uninstall: powershell.exe -executionpolicy Bypass -file .\Uninstallkeeper.ps1
  + **Zorg dat het user-based install is.**
* Duw op next
* Geef volgende requirements mee:
  + OS architecture: 64-bit
  + OS versie: Windows 10 1909
* Duw op next
* Bij detection rules:
  + Kies voor custom
    - Vraag het detection script aan de trainer
    - Verander het software programma naar de opgegeven ID

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Laad dit aangepast script op
  + Duw op Next
* Bij dependencies duw je op next
* Supersedence rules duw je op next
* Assignments: required en All devices. Duw op Next
* Duw op create

Labo 20 – Windows Update rings

## DEELOPDRACHT 1: Create User groups

* Maak 3 user groups aan:
  + Test update users:
    - Voeg jezelf toe
  + Acceptation users
    - Voeg van elk departement 1 user toe

## DEELOPDRACHT 2: Create update rings

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar devices > update rings for windows 10
* Kies hier voor create profile.
  + Name: Test update ring
  + Duw op next
  + Controleer volgende gegevens
    - updates voor microsoft producten en drivers worden geüpdate
    - Quality update defferal period: 0
    - Feature update defferal: 0
    - De rest laat je default staan
  + Duw op next
  + Assigned aan de groep: Test update users. Duw op next
  + Duw op create
* Zorg dat ook volgende profiles worden aangemaakt:
  + Acceptation ring
    - Quality update defferal period: 15
    - Feature update defferal: 90
  + Production ring
    - Quality update defferal period: 30
    - Feature update defferal: 180
    - Group: All users (exclude test update users en acceptance users)

Labo 21 – Autopilot

## DEELOPDRACHT 1: Capture hardware ID

* Login op de laptop
* Open Powershell als admin en geef volgende CMD-Let in:
  + (Je kan dit script ook vinden door in google: “manually register device in intune” op te zoeken)

md c:\HWID

Set-Location c:\HWID

Set-ExecutionPolicy -Scope Process -ExecutionPolicy Unrestricted -Force

Install-Script -Name Get-WindowsAutopilotInfo -Force

$env:Path += ";C:\Program Files\WindowsPowerShell\Scripts"

Get-WindowsAutopilotInfo.ps1 -OutputFile AutopilotHWID.csv

* Bij vragen over nuget repository geef “Y” op.
* Kopieer de CSV zodat je deze kan inladen (C:\HWD)

## DEELOPDRACHT 2: import CSV

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar devices> enroll devices
* Kies hier voor de optie “devices”
* Kies voor import en importeer hier je CSV
* Geef het even tijd om te importeren. Je kan wel al verder werken aan de volgende deelopdrachten

## DEELOPDRACHT 3: Maak autopilot device group

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar groups> All groups
* Kies voor new group
* Geef volgende info:
  + Type: Security
  + Name: Autopilot devices
  + Description: Oplijsting van alle autopilot devices
  + Membership Type: Dynamic Device
* Duw op het blauwe “Add dynamic Query”
* Duw bij rule syntax op de knop edit

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* Geef volgende info mee
  + (device.devicePhysicalIDs -any (\_ -contains "[ZTDID]"))
  + Duw op OK
* Duw op save
* Duw op create

## DEELOPDRACHT 4: Maak autopilot profile aan

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar devices> enroll devices
* Kies hier voor de optie “deployment profiles”
* Maak een nieuw profiel aan door op “+create profile” te kiezen
  + Windows PC
* Eerste stap:
  + Name: autopilot profile
  + Description: profiel voor autopilot
  + Convert all… : No
  + Duw op Next
* Stap 2:
  + Verander keyboard naar no
  + Verander device name template naar yes:
    - AP-%RAND:6%
  + Duw op next
* Stap 3:
  + Voeg de groep autopilot devices mee
  + Duw op next
* Duw op create

## DEELOPDRACHT 5: Maak enrollment status page

* Ga naar: <https://endpoint.microsoft.com/>
* Navigeer naar devices> enroll devices
* Kies hier voor de optie “Enrollment status page”
* Kies voor create
* Stap 1:
  + Name: Autopilot status
  + Description: Status van autopilot deployment
  + Duw op next
* Stap 2:
  + Show app and profile configuration: yes
  + Laat alles default staan
  + Duw op next
* Stap 3:
  + Voeg alle users toe
  + Duw op next
* Stap 4:
  + Duw op next
* Stap5:
  + Duw op create

## DEELOPDRACHT 4: Test autopilot

* Login op CL01 met jouw azure AD user
* Ga naar settings > Update en security
* Kies voor recovery
* Bij reset PC kies je voor “Get started”
* Doorloop de stappen om je PC te resetten
  + Alle bestanden mogen verwijderd worden
  + Kies voor local reinstall
* Dit kan even duren.

EXTRA 01 – BULK-USERS

## DEELOPDRACHT 1: BULK IMPORT USERS

* Open een browser en surf naar de URL https://endpoint.microsoft.com
* Navigeer naar users> All users
* Kies hier voor Bulk operations > Bulk create
* Klik op het Add Multiple users icoon.
* Download CSV template, open deze met notepad (geen excel)
* Pas het volgende aan:
  + Verwijder alles na Last name

Afbeelding met tekst

Automatisch gegenereerde beschrijving

* + Maak nieuwe users aan als volgt:
    - Bv.:   
      Bas Schutte,B.Schutte@intunetest062022.onmicrosoft.com,Azerty01, No,Bas,Schutte
    - Zorg dat het gedeelte voor .onmicrosoft.com aangepast is naar jouw omgeving
* Bewaar het CSV bestand en keer terug naar je webbrowser
* Bij het onderdeel upload your csv file browse je naar de opgeslagen csv-file en klik je op sumbit.
* Ga nu naar admin.microsoft.com
* Navigeer naar users > Active users
* Open een user en zorg dat deze de juiste licenties bevat

EXTRA 02 – USERS Script

## DEELOPDRACHT 1: Add users with script

* Open een browser en surf naar de URL <https://github.com/TuurHousiaux/TrainingIntune>
* Download het script: “Users MS365.ps1”, dit voert het volgende uit:
  + Openen powershell als admin
  + Installeren module Msonline (indien nog niet geïnstalleerd)
  + Aanmaken users met departementen

Extra 03 – Multifactor Authentication

## DEELOPDRACHT 1: Multifactor Authentication

In deze oefening gaan we multifactor authentication uitvoeren voor de omgeving

* Ga naar: <https://endpoint.microsoft.com/>
* Browse naar “Users” en kies voor “per user multifactor authentication”

Graphical user interface, text, application

Description automatically generated

* Selecteer de global administrator
* Kies voor enable
* Bij de popup duw je op enable multifactor auth
* Selecteer daarna terug de administrator en kies voor enforce
* Bij de popup duw je op enforce

## DEELOPDRACHT 2: Multifactor Authentication testen

* Log uit en terug in op <https://portal.office.com>
  + Als er gevraagd wordt voor multifactor auhtentication:
    - Installeer Microsoft Authenticator op jouw smartphone
    - Duw op next
    - Scan de QR-code vanuit de authenticator app (add account > work/school account)
    - Duw next en aansluitend approve op je smartphone
  + Voor de 2e authenticatie
    - Geef jouw gsm-nummer op
    - Duw next
    - Geef de verificatie-code op
    - Next
    - Geef bij App Password een naam op
    - Duw op done

Extra 04 – Azure AD Self Service Password Reset

## DEELOPDRACHT 1: Azure AD SSPR inschakelen

We gaan Azure AD SSPR inschakelen

* Ga naar: <https://endpoint.microsoft.com/>
* Browse naar “Users” > Password reset

Graphical user interface, text, application

Description automatically generated

* Geef volgende configuratie mee (vergeet niet elke keer op save te duwen!):

Graphical user interface, application, Teams

Description automatically generated

* + Properties:
    - Self service password reset enabled: All
  + Authentication methods
    - Number: 2
    - Methods:
      * Email
      * Mobile App
      * SMS
  + Registration:
    - Default laten staan
  + Notifications:
    - Both yes
  + De rest gewoon default

## DEELOPDRACHT 2: Azure AD SSPR testen

We gaan Azure AD SSPR testen

* Open een andere browser in-private
* Ga naar portal.office.com
* Geef jouw mail-adres van de admin mee
* Duw next en zeg dan forgot password
* Volg de stapjes om jouw wachtwoord te resetten.

Extra 03 – Brand company portal

## DEELOPDRACHT 1: Corporate Branding - Theme

* Open een web-browser en open [www.portal.office.com](http://www.portal.office.com)
* Open het admin center
* Ga naar settings \ organization settings
* Kies voor organization profile
* Kies hier voor Custom themes
* Pas volgende settings aan:
  + Use a custom logo image
  + Make the logo clickable (naar een website naar keuze)
  + Kies voor een background image
  + Bekijk eventueel de andere settings
* Druk op save

Afbeelding met tekst

Automatisch gegenereerde beschrijving

Extra 04 – Change Domain Name (niet uit te voeren zonder extra kosten)

## DEELOPDRACHT 1: Change domain name

* Ga naar portal.office.com en lo gin
* Open de admin center
* Ga naar Settings \Domains
* Druk op Add Domain
* Geef de naam van het gewenste domein en duw op use this domain
* Bij domain verification zorg je dat “add a txt record …” aanstaat en druk op continue
* Kopieer de txt-value en ga naar je DNS-provider (in de demo gebruik ik nomeo, maar je kan ook vele andere gebruiken)
* Druk op verify, let op dit kan even duren voordat het juiste record wordt herkend!
* Zorg dat alle records voor Office 365 worden aangemaakt, de meeste providers kunnen dit aan de hand van een wizard.
* Druk op verify. Indien alles goed is kan je je domein toevegen.
* Hij staat reeds op default.
* We veranderen nu al onze users van .onmicrosoft.com naar het nieuwe domein

Extra 05 – Azure AD connect

## DEELOPDRACHT 1: Installeer Azure AD connect

* Ga naar een server op jouw domein en login met de domain admin
* Download het product Azure AD Sync (download van het internet)

## DEELOPDRACHT 2: Change UPN

* Enkel nodig als jouw UPN van de lokale AD niet hetzelfde is als deze van de O365-omgeving.
* Ga naar Active directory domains and trusts, rechtermuisklik op Active directory domains and trusts
* Voeg jouw azure AD domein toe
* Sluit Active directory domains and trusts
* Zorg dat alle gebruikers een andere UPN-sufix hebben

## DEELOPDRACHT 2: Azure AD Connect

* Installaeer Azure AD connect.
* Bij de vraag om je Azure AD te koppelen geef je de global admin op van je M365-tenant
* Bij de vraag voor de enterprise admin van jouw domein geef je deze op.
* Daarna krijg je de melding dat niet alle UPN-sufixen zijn gekoppeld. Vink aan dat dit ok is en duw op next.
* Bij de review duw je op finish, na de installatie gaat hij automatisch beginnen syncen.
* Wacht enige tijd en de users worden aangemaakt

Extra 06 – Chocolatey

Volg de stappen op deze link voor chocolatey apps

<https://semiadmin.nl/2021/09/02/automating-chocolatey-with-intune/>

Extra 07 – Configuration Policies

## DEELOPDRACHT 1: Configuration policies

Leren werken met deze policies is vooral uitzoeken en testen (op eventueel testgroepen)  
Probeer zeker volgende settings ook eens te configureren!

Windows 10

* Device restriction:
  + Locked screen background
* Administrative templates
  + Onedrive settings
    - Like: silently move, silent sign-in, prevent users etc.
* Identity Protection
  + Set up profile (only allow PIN)

EDGE

* Device restrictions profile
  + Choose a custom home page
  + Choose some settings
* Administrative templates
  + Push Adblocker Plus & Adblocker for Youtube