2tCloud

Modern Workplace
Hands-on lab

AAD Premium, Intune, Office ProPlus

Microsoft 365 Enterprise

Lab Guide

Friday, May 17, 2019

Version 3.0

Prepared by

Gino van Essen
Gido Veekens
Stephan van de Kruis

Technical Cloud Consultants – Copaco Nederland

Document Revision

Change Record

Date	Author	Version	Change Reference
15-10-2018	Gino van Essen	0.1	Create document
16-10-2018	Stephan van de Kruis	0.2	Add new items
17-10-2018	Gino van Essen	1.0	Add new items and finalize document
4-2-2019	Stephan van de Kruis	1.1	Im
17-5-2019	Stephan van de Kruis	3.0	Revision

Name	Version Approved	Position	Date

Table of Contents

Introduction

The Microsoft 365 Modern Desktop Lab is designed to help you with the deployment of modern devices running Windows 10 Enterprise and Office 365 Pro Plus, managed by Enterprise Mobility + Security.

Estimated time to complete this lab

150 minutes

Objectives

- During this lab, you will learn how to use Azure Active Directory and Intune to:
- Create AAD group
- Configure Compliance policies
- Configure Configuration policies
- Configure Conditional Access
- Join Windows 10 clients to Azure Active Directory

Prerequisites

- Laptop/computer with Internet browser and wifi connected.
- Windows 10 Pro N version 1803 via Azure VM
- Windows 10 Enterprise version 1803 via Hyper-V manager or VMware workstation
- Microsoft 365 Enterprise E3 subscription

Student Materials

All student materials are available for download here:

https://github.com/Copaco/handsonlab

Activity 1: Getting Started

Objectives

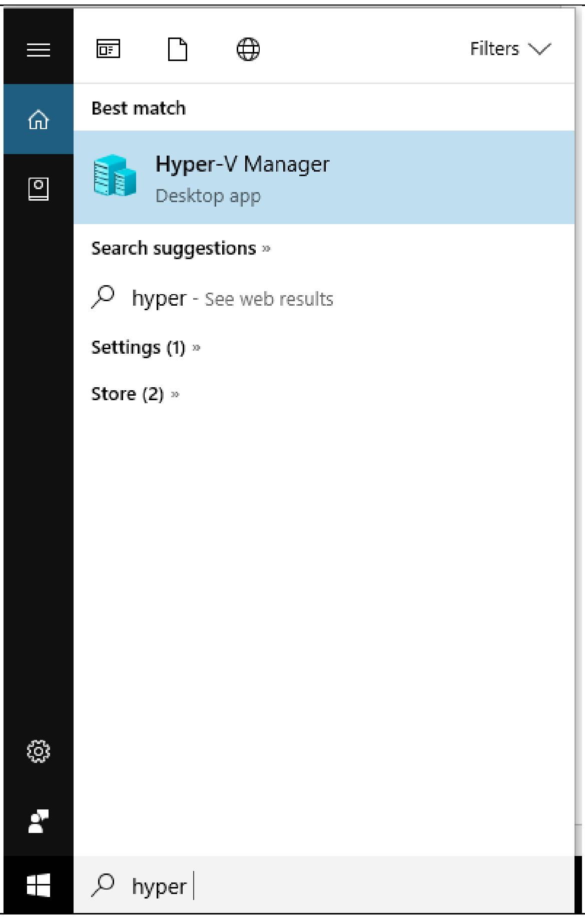
In this activity, you will configure the components necessary to perform this lab:

- Windows 10 Enterprise, version 1809 – Hyper-V

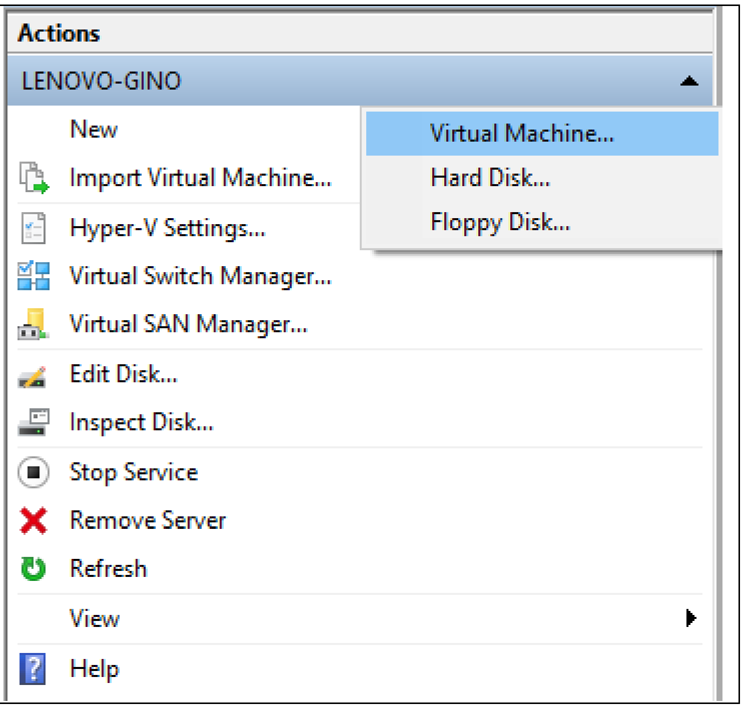
When Azure tenant \ subscription is not available

- ISO of Windows 10 Enterprise 1809 handed out by Copaco
- Hyper V Manager VM configuration

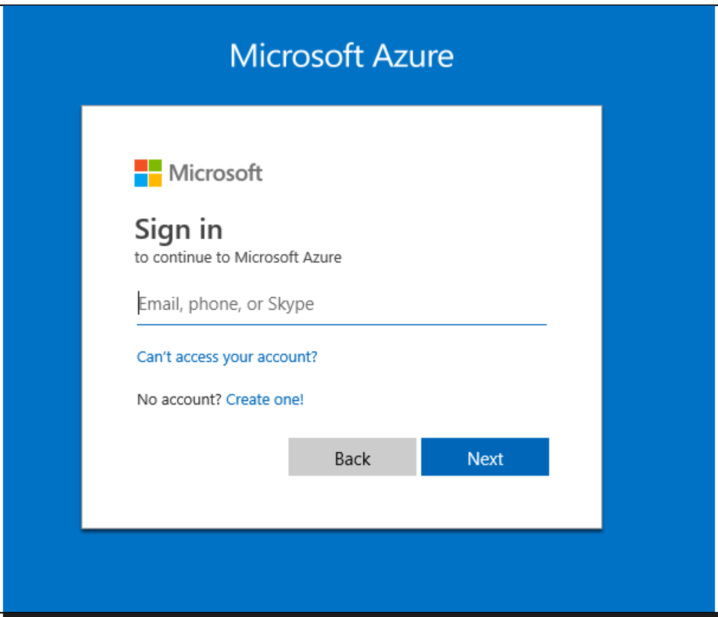
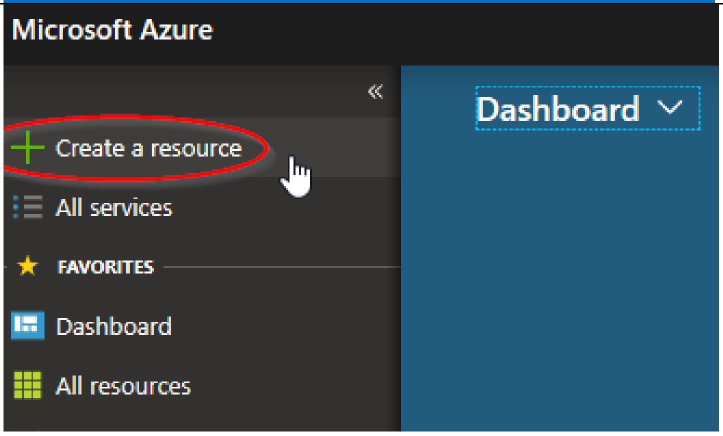
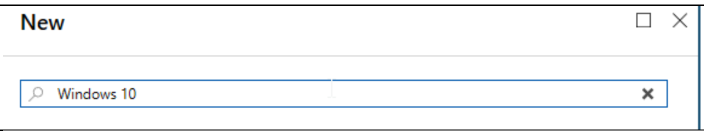
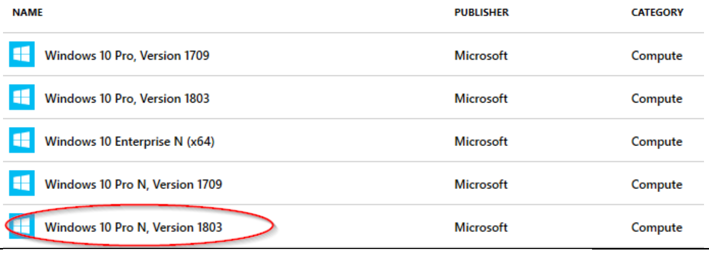
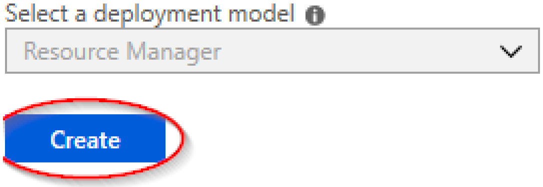
Exercise 1a: Create Windows 10 Enterprise VM

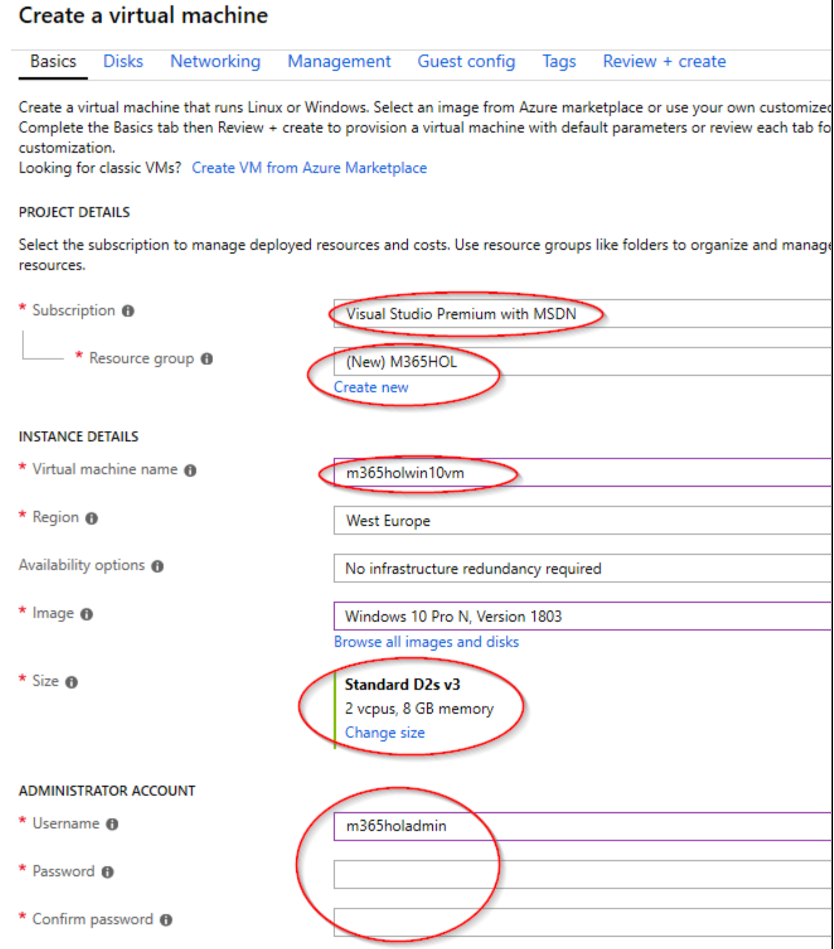
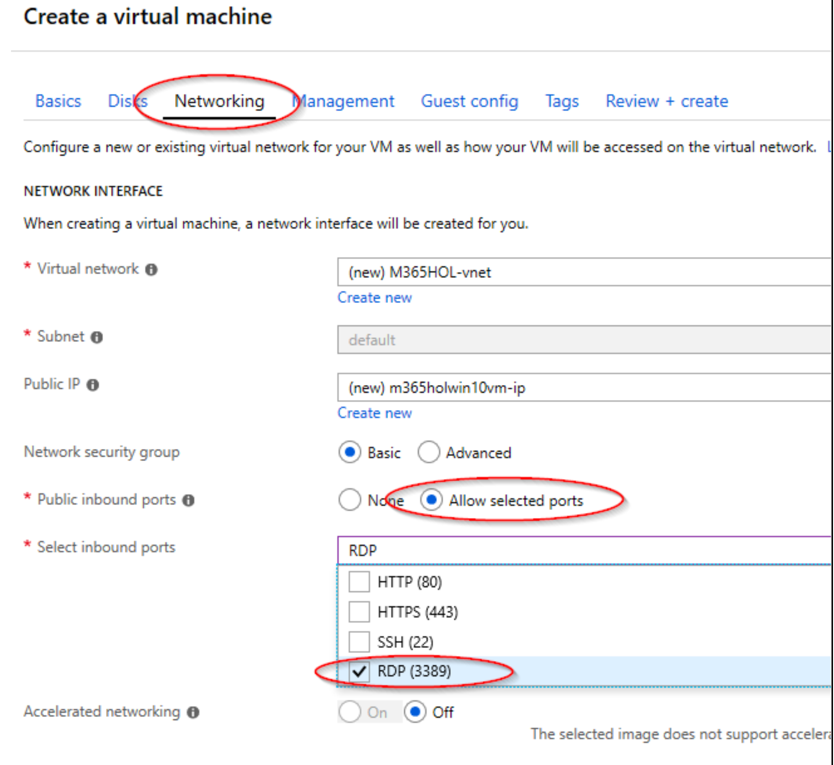
1. Open **Hyper-v Manager**	 Filters Best match Hyper-V Manager Desktop app Search suggestions » hyper - See web results Settings (1) » Store (2) » hyper

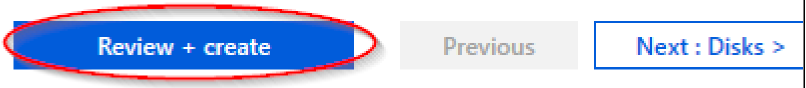
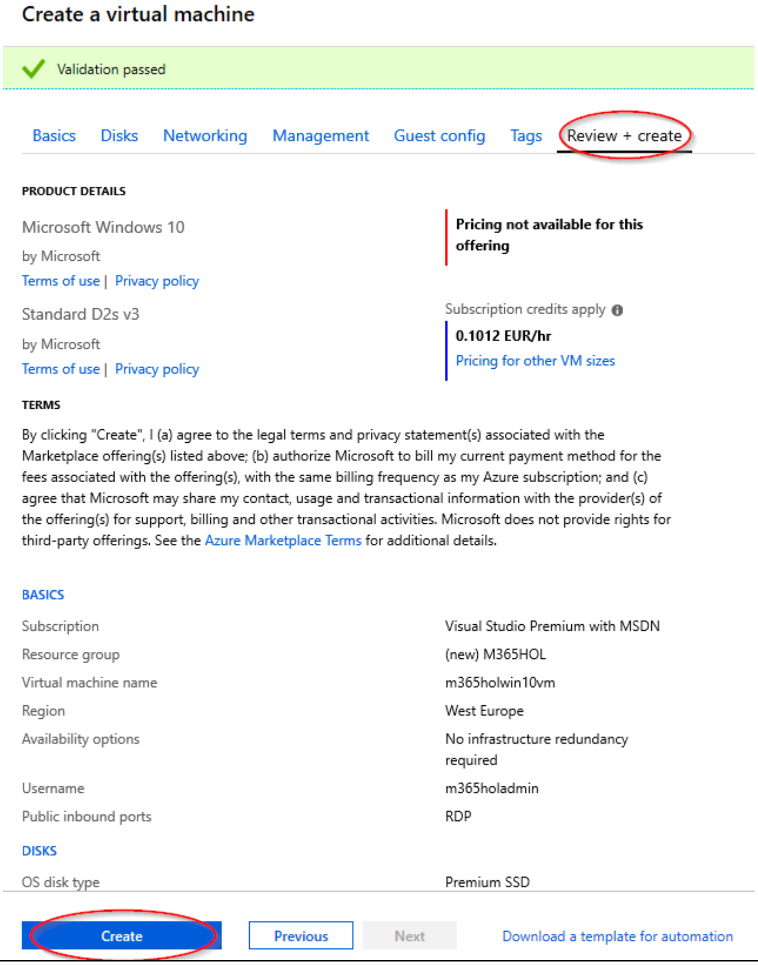
2. Create **New > virtual machine**
3. Name **WIN10ENT-1803**
4. Generation **Generation 2**
5. Assign Memory **4096 MB**
6. Configure Networking **Connection External**
7. Create VHD **Standard settings**
8. Installation Options **install an OS from a bootable CD/DVD**
9. Image file: “Win10.iso”
10. Finish / complete the configuration
11. **DO NOT START THE VM**

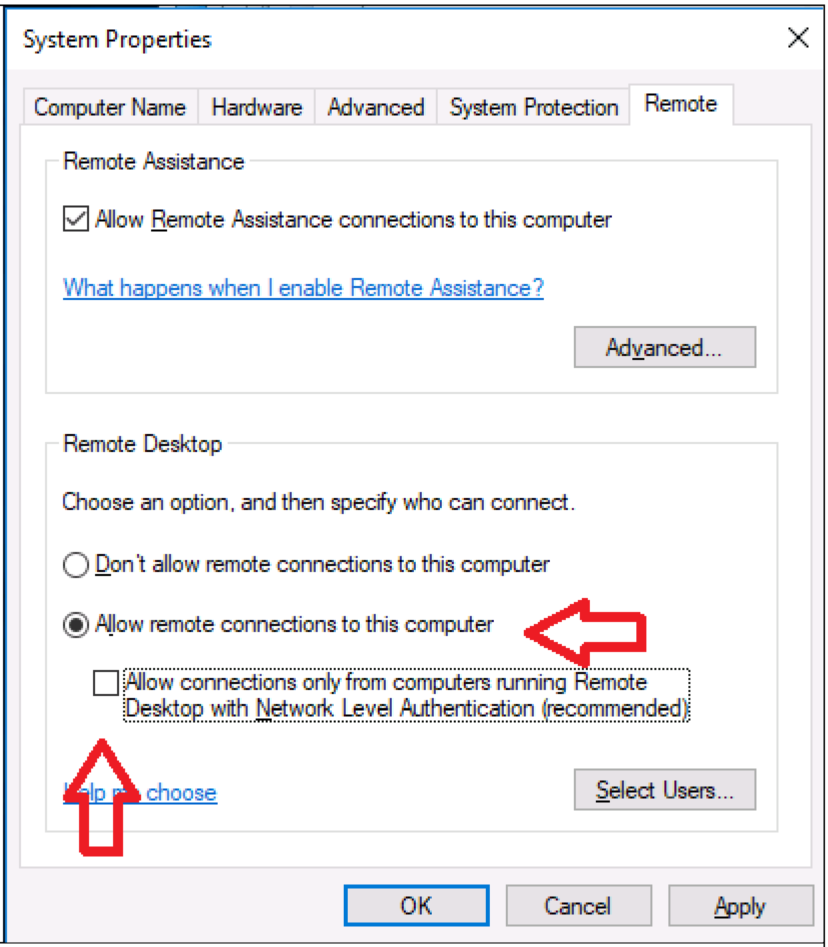


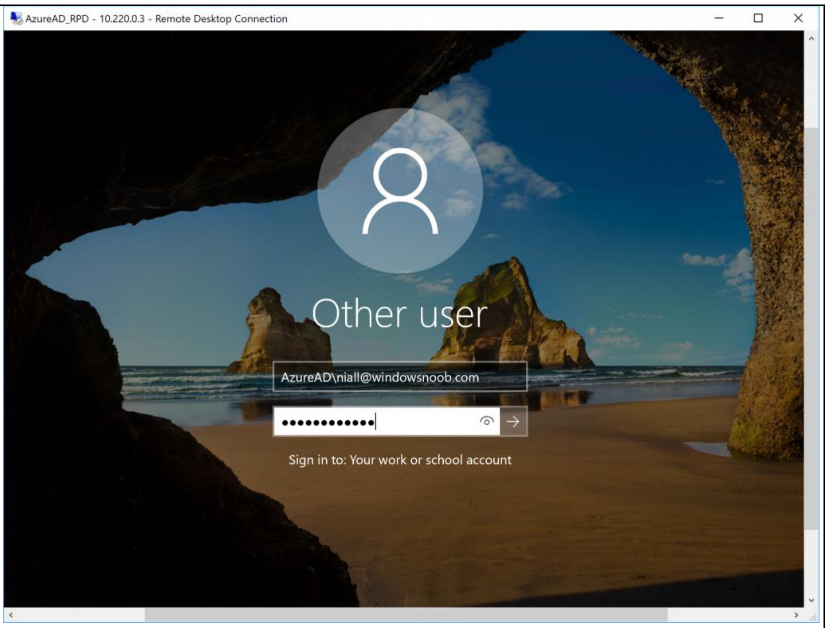
Exercise 1b **OPTIONAL: Create Windows 10 PRO VM in Azure**

12. Go to https://portal.azure.com and login with your Azure AD Work account"	 Microsoft Azure Microsoft Sign in to continue to Microsoft Azure Email, phone, or Skype Can't access your account? No account? Create one! Back Next
13. Create a resource	 Microsoft Azure Create a resource All services FAVORITES Dashboard All resources Dashboard
14. Search for "Windows 10"	 New Windows 10
15. Select "Windows 10 Pro N, Version 1803	 NAME PUBLISHER CATEGORY Windows 10 Pro, Version 1709 Microsoft Compute Windows 10 Pro, Version 1803 Microsoft Compute Windows 10 Enterprise N (x64) Microsoft Compute Windows 10 Pro N, Version 1709 Microsoft Compute Windows 10 Pro N, Version 1803 Microsoft Compute
16. Click "Create" (bottom of screen)	 Select a deployment model Resource Manager Create

17. Select Azure Subscription 18. Create resource group "M365HOL" 19. Enter VM name "M365holwin10vm" 20. Select VM Size "Standard D2s v3" 21. Enter username "m365holadmin" with Password "Test@m365hol2018"	 Create a virtual machine Basics Disks Networking Management Guest config Tags Review + create Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customizec Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab fo customization. Looking for classic VMs? Create VM from Azure Marketplace PROJECT DETAILS Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manag resources. * Subscription: Visual Studio Premium with MSDN * Resource group: (New) M365HOL Create new INSTANCE DETAILS * Virtual machine name: m365holwin10vm * Region: West Europe Availability options: No infrastructure redundancy required * Image: Windows 10 Pro N, Version 1803 Browse all images and disks * Size: Standard D2s v3 2 vcpus, 8 GB memory Change size ADMINISTRATOR ACCOUNT * Username: m365holadmin * Password * Confirm password
11. Go to tab "Networking" 12. Select "Allow selected ports" 13. Select Inbound ports "RDP (3389)	 Create a virtual machine Basics Disks Networking Management Guest config Tags Review + create Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. L NETWORK INTERFACE When creating a virtual machine, a network interface will be created for you. * Virtual network: (new) M365HOL-vnet Create new * Subnet: default Public IP: (new) m365holwin10vm-ip Create new Network security group: ● Basic ○ Advanced * Public inbound ports: ○ None ● Allow selected ports * Select inbound ports: RDP □ HTTP (80) □ HTTPS (443) □ SSH (22) ☑ RDP (3389) Accelerated networking: ○ On ● Off The selected image does not support accelera

14. Click “Review + create”	
15. Click “Create” 16. After 10 minutes (maximum) the VM creation is finished	Create a virtual machine ✓ Validation passed Basics Disks Networking Management Guest config Tags Review + create PRODUCT DETAILS Microsoft Windows 10 by Microsoft Terms of use | Privacy policy Pricing not available for this offering Standard D2s v3 by Microsoft Terms of use | Privacy policy Subscription credits apply 0.1012 EUR/hr Pricing for other VM sizes TERMS By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details. BASICS Subscription Visual Studio Premium with MSDN Resource group (new) M365HOL Virtual machine name m365holwin10vm Region West Europe Availability options No infrastructure redundancy required Username m365holadmin Public inbound ports RDP DISKS OS disk type Premium SSD Create Previous Next Download a template for automation

17. After the VM is ready log in to the VM 18. Set the Remote Desktop settings **to Allow Remote Connections to this computer** and remove the checkbox from **Allow connections only from computers running Remote Desktop with Network Level Authentication enabled**	 System Properties Computer Name Hardware Advanced System Protection Remote Remote Assistance ☑ Allow Remote Assistance connections to this computer What happens when I enable Remote Assistance? Remote Desktop Choose an option, and then specify who can connect. ○ Don't allow remote connections to this computer ● Allow remote connections to this computer □ Allow connections only from computers running Remote Desktop with Network Level Authentication (recommended) Help me choose
19. Log out of the VM 20. Download the RDP file and save the file on your desktop 21. Open the RDP file with Notepad.	
22. Add the following lines to the bottom 23. Save the file 24. Open to file to Remote desktop to the VM	enablecredsspsupport:i:0 authentication level:i:2

25. At the login screen you need to use the following format to log in: **AzureAD\<username@domain.com>**	 AzureAD_RPD - 10.220.0.3 - Remote Desktop Connection Other user AzureAD\niall@windowsnoob.com Sign in to: Your work or school account

Activity 2: Prepare Modern workplace with Intune

The most important components in this exercise are:

Azure Active Directory.

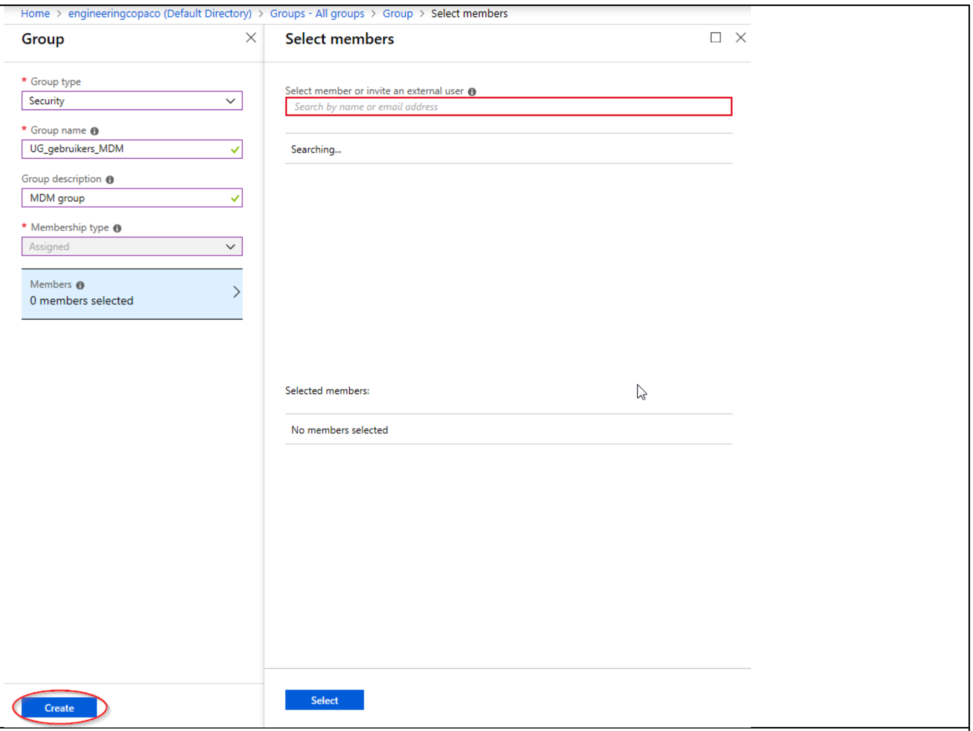
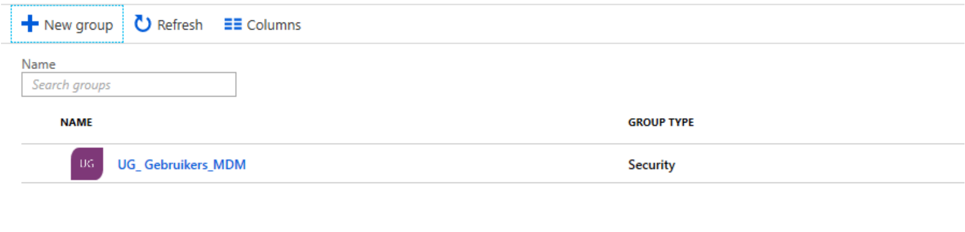
Users and Groups.

Intune.

Exersize 2: Create an AAD Group

1. Go to : http://portal.azure.com

Kenmerk	Waarde
Group type	Security
Group name	UG_gebruikers_MDM
Group description	MDM group
Membership type	Assigned

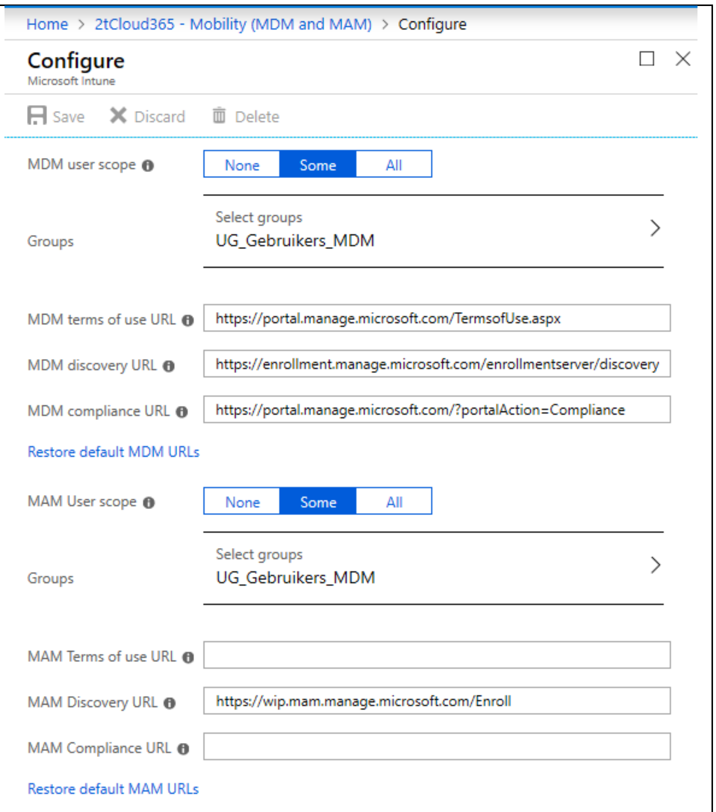
2. Go to: **Azure Active Directory->Manage->Groups** 3. Click **New Group** and create a group with the following settings 4. Add Admin account to group "**UG_Gebruikers_MDM**" 5. Click Create (bottom of screen)	 Home > engineeringcopaco (Default Directory) > Groups - All groups > Group > Select members Group * Group type: Security * Group name: UG_gebruikers_MDM Group description: MDM group * Membership type: Assigned Members: 0 members selected Select members Select member or invite an external user: Search by name or email address Searching... Selected members: No members selected
6. AAD Group "**UG_Gebruikers_MDM**" is created	 Name: Search groups NAME: UG_Gebruikers_MDM — GROUP TYPE: Security

Exercise 2a: Configure group-based Licensing

1. Go to: **Azure Active Directory → Licenses → All products** 2. Select **Microsoft 365 E3** 3. Select **Licensed groups** 4. Click the Assign button 5. At users and groups search for UG_gebruikers_MDM and select the group 6. At Assignment options make sure that On is selected and click OK 7. Click Assign	

Exercise 3: Configure MDM and MAM Intune settings

1. Go to **Azure Active Directory->Mobility (MDM and MAM)->Microsoft Intune.**



Home > 2tCloud365 - Mobility (MDM and MAM) > Configure

Configure
Microsoft Intune

Save Discard Delete

MDM user scope: None | **Some** | All

Groups: Select groups: UG_Gebruikers_MDM

MDM terms of use URL: https://portal.manage.microsoft.com/TermsofUse.aspx

MDM discovery URL: https://enrollment.manage.microsoft.com/enrollmentserver/discovery

MDM compliance URL: https://portal.manage.microsoft.com/?portalAction=Compliance

Restore default MDM URLs

MAM User scope: None | **Some** | All

Groups: Select groups: UG_Gebruikers_MDM

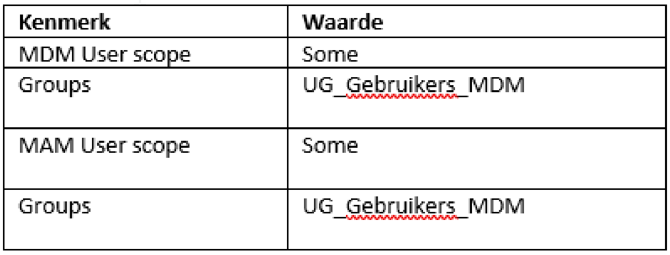
MAM Terms of use URL:

MAM Discovery URL: https://wip.mam.manage.microsoft.com/Enroll

MAM Compliance URL:

Restore default MAM URLs

2. Configure the settings ->

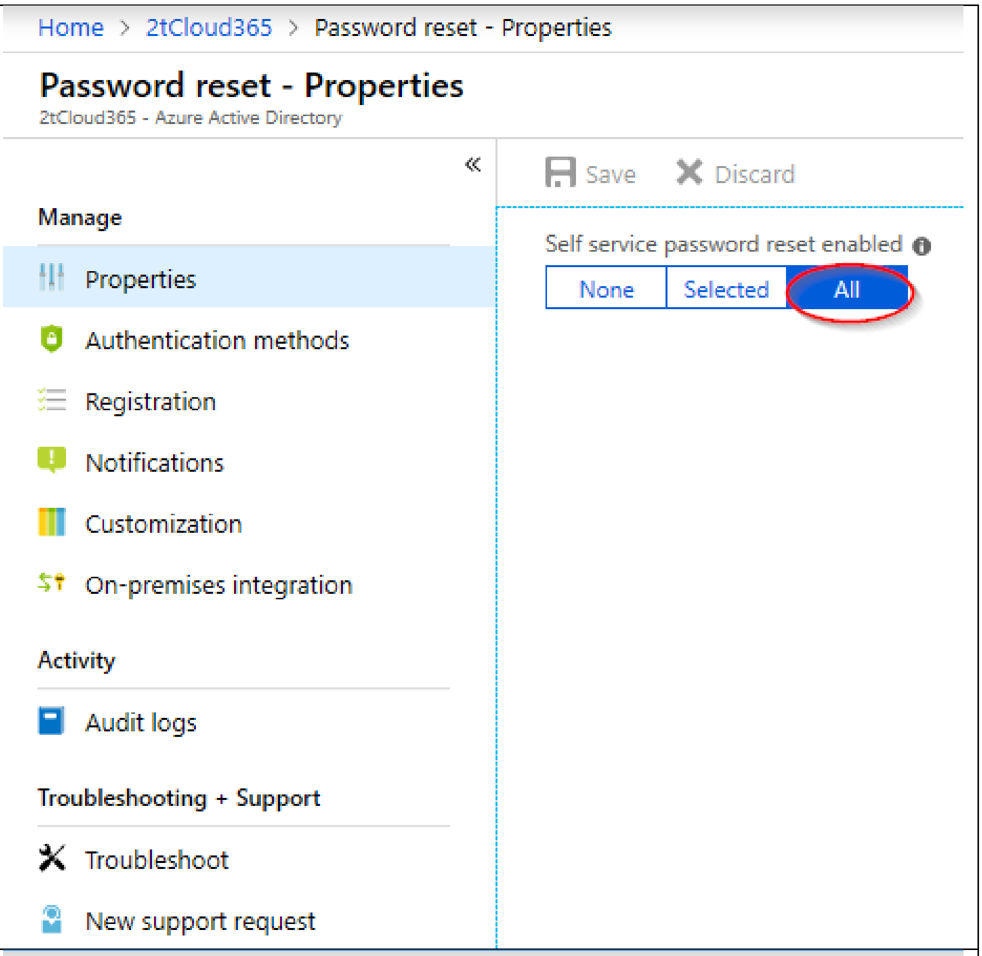


Kenmerk	**Waarde**
MDM User scope	Some
Groups	UG_Gebruikers_MDM
MAM User scope	Some
Groups	UG_Gebruikers_MDM

3. Click on **Save**

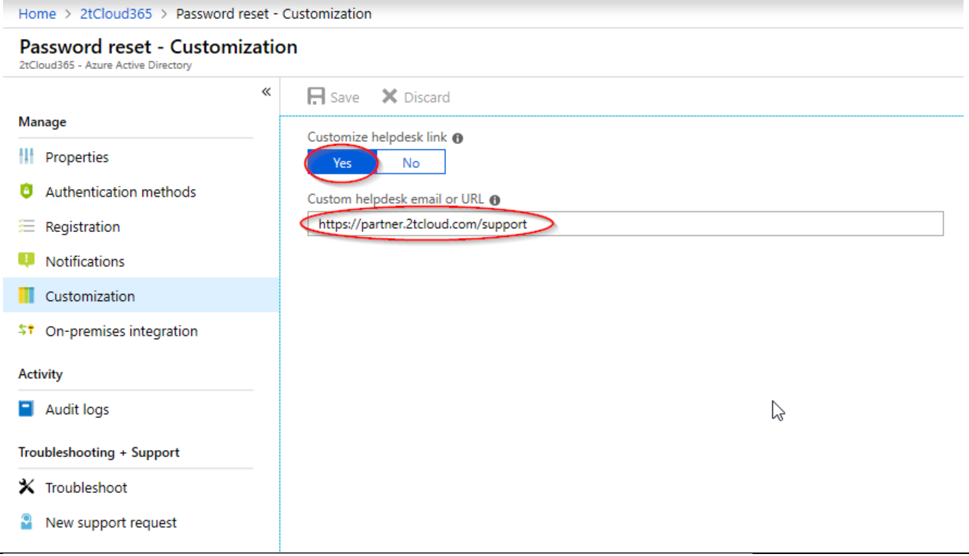
Exercise 4: Activate Self Service Password Reset

1. Go to **Azure Active Directory->Password reset->Properties**;
2. Set setting to: **All**
3. Click: **Save**



Self service password reset enabled: None Selected [✓ All]

4. Go to **Azure Active Directory-> Password reset-> Customization;**



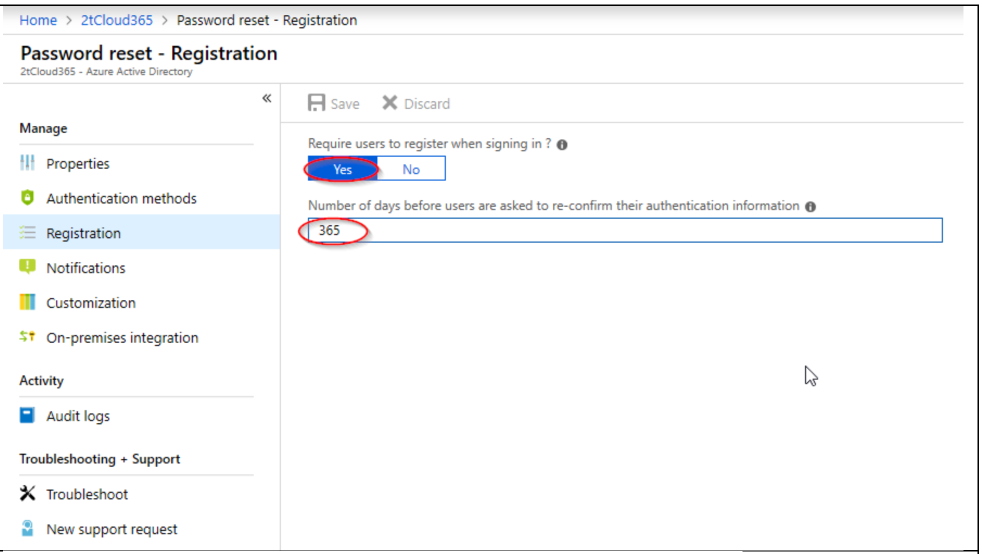
Customize helpdesk link: [✓ Yes] No

Custom helpdesk email or URL: https://partner.2tcloud.com/support

5. Configure the settings -> and click **Save**

Customize helpdesk link	Yes
Custom helpdesk email or URL	https://partner.2tcloud.com/support

6. Go to **Azure Active Directory-> Password reset-> Registration;**



Home > 2tCloud365 > Password reset - Registration

Password reset - Registration

2tCloud365 - Azure Active Directory

Require users to register when signing in ? Yes No

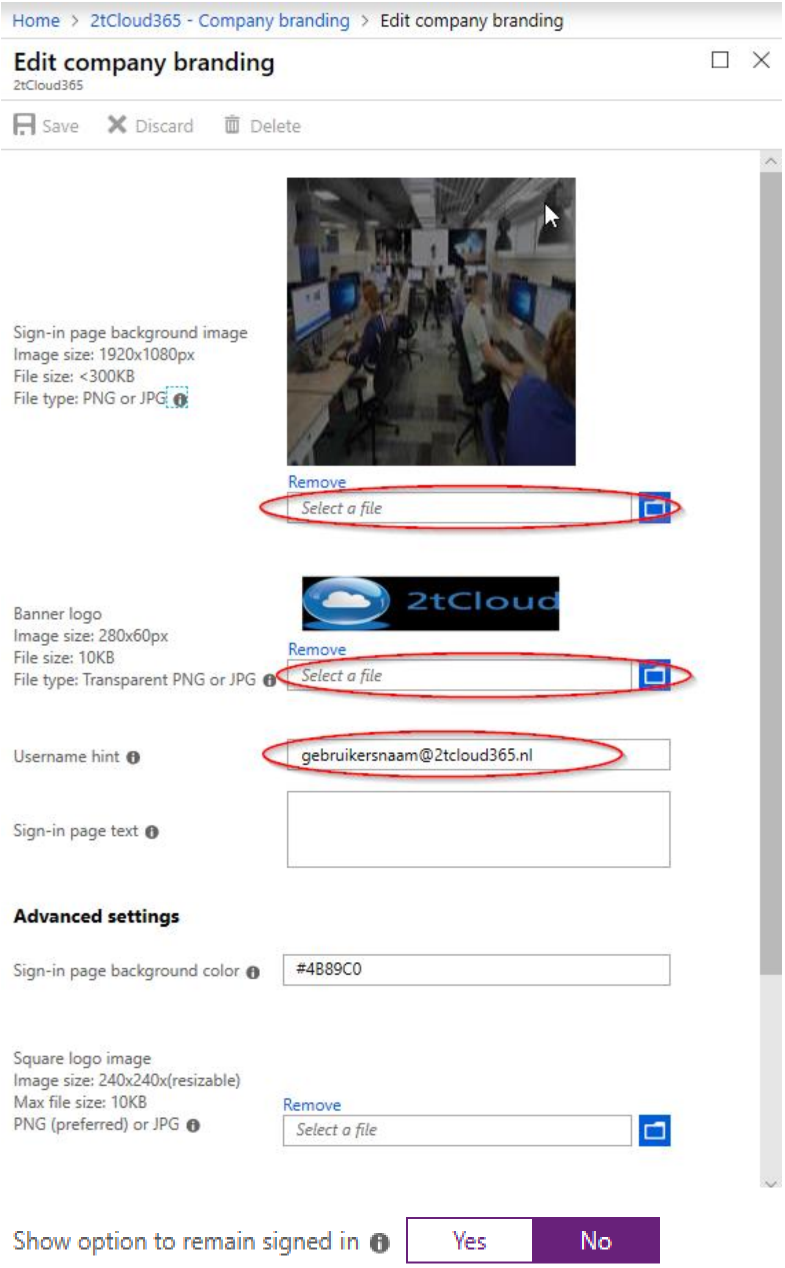
Number of days before users are asked to re-confirm their authentication information: 365

7. Configure the settings -> and click **Save**

Require Users to register when Signing in?	Yes
Number of days	365

Exercise 5: Company branding

1. Go to **Azure Active Directory->Company Branding->Edit company branding;**



Home > 2tCloud365 - Company branding > Edit company branding

Edit company branding

2tCloud365

Save Discard Delete

Sign-in page background image
Image size: 1920x1080px
File size: <300KB
File type: PNG or JPG

Remove

Select a file

Banner logo
Image size: 280x60px
File size: 10KB
File type: Transparent PNG or JPG

Remove

Select a file

Username hint: gebruikersnaam@2tcloud365.nl

Sign-in page text:

Advanced settings

Sign-in page background color: #4B89C0

Square logo image
Image size: 240x240(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

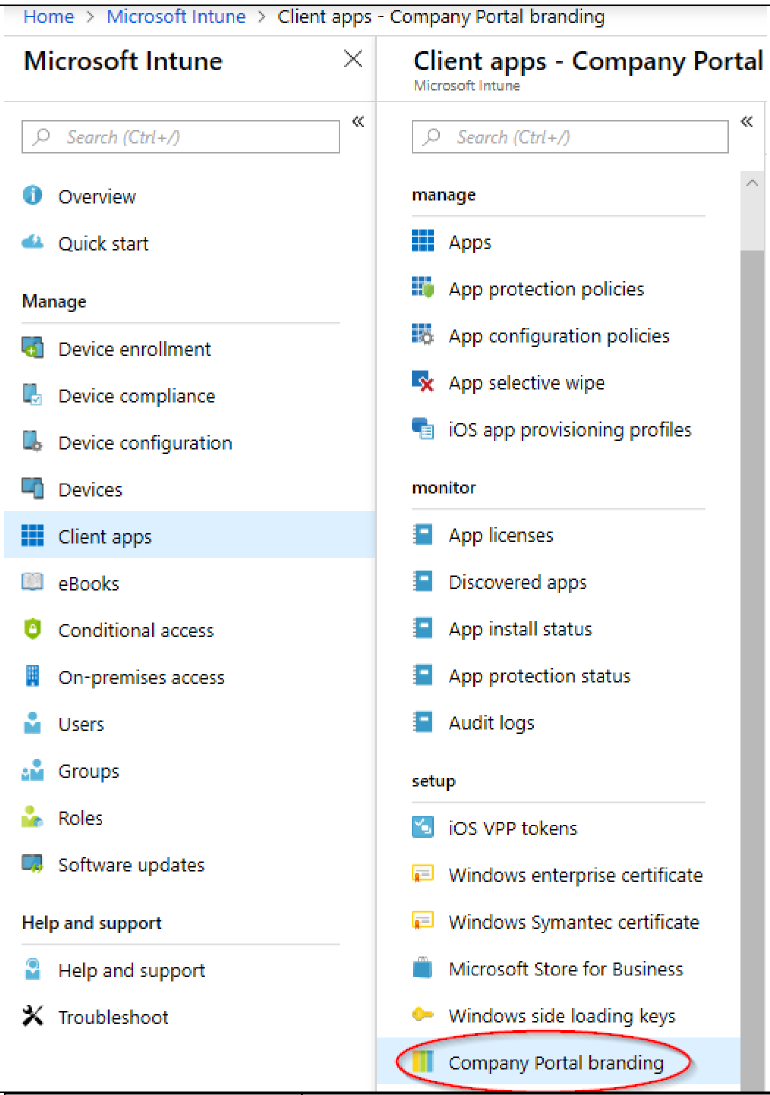
Select a file

Show option to remain signed in: Yes [✓ No]

2. Configure the settings -> Click **Save**

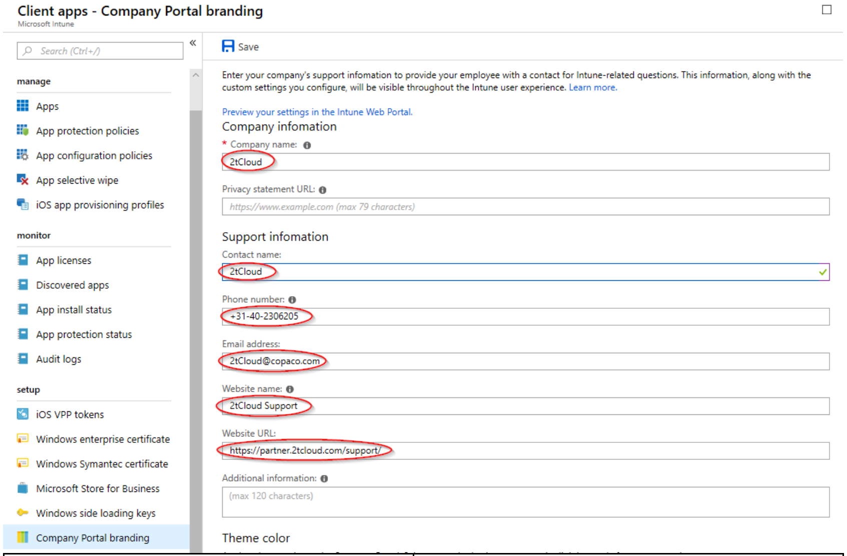
Sign-in page image	Add image
Banner image	Add image
User name hint	gebruikersnaam@2tcloud365.nl
Show option to remain signed in	No

3. Go to **Intune -> Client apps -> Company Portal Branding**



4. Configure the settings -> Save

Company Name	2tCloud or your own company
Contact name	2tCloud or your own company
Phone number	Add picture
E-mail adress	2tcloud@copaco.com or gebruikersnaam@x.onmicrosoft.com
Support website name	2tCloud Support or your own company
Support Website URL	https://partner.2tcloud.com/support/ or your own



Client apps - Company Portal branding

Microsoft Intune

Enter your company's support infomation to provide your employee with a contact for Intune-related questions. This information, along with the custom settings you configure, will be visible throughout the Intune user experience. Learn more.

Preview your settings in the Intune Web Portal.

Company infomation

* Company name: 2tCloud

Privacy statement URL: https://www.example.com (max 79 characters)

Support infomation

Contact name: 2tCloud

Phone number: +31-40-2306205

Email address: 2tCloud@copaco.com

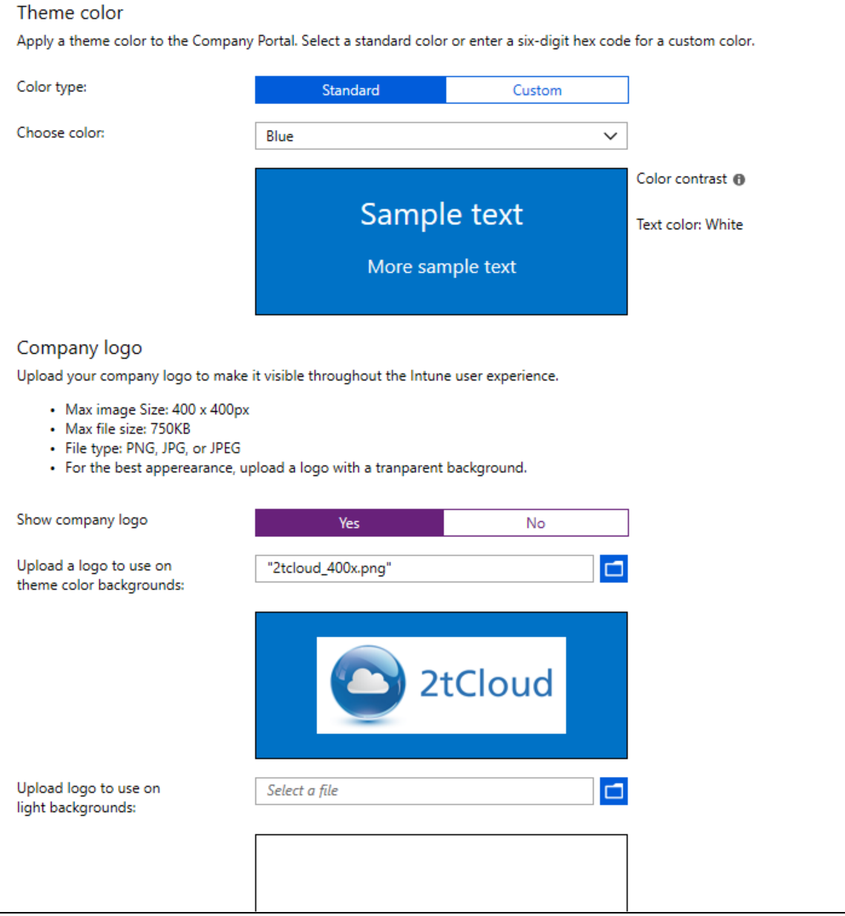
Website name: 2tCloud Support

Website URL: https://partner.2tcloud.com/support/

Additional information: (max 120 characters)

Theme color

Show company logo	Yes
Company logo	Add logo



Theme color

Apply a theme color to the Company Portal. Select a standard color or enter a six-digit hex code for a custom color.

Color type: Standard | Custom

Choose color: Blue

Color contrast

Text color: White

Company logo

Upload your company logo to make it visible throughout the Intune user experience.

- Max image Size: 400 x 400px
- Max file size: 750KB
- File type: PNG, JPG, or JPEG
- For the best apperearance, upload a logo with a tranparent background.

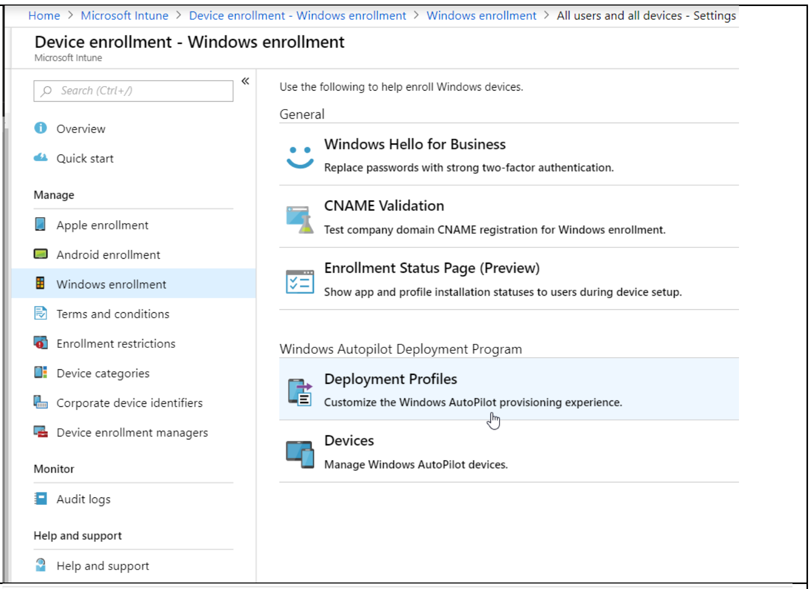
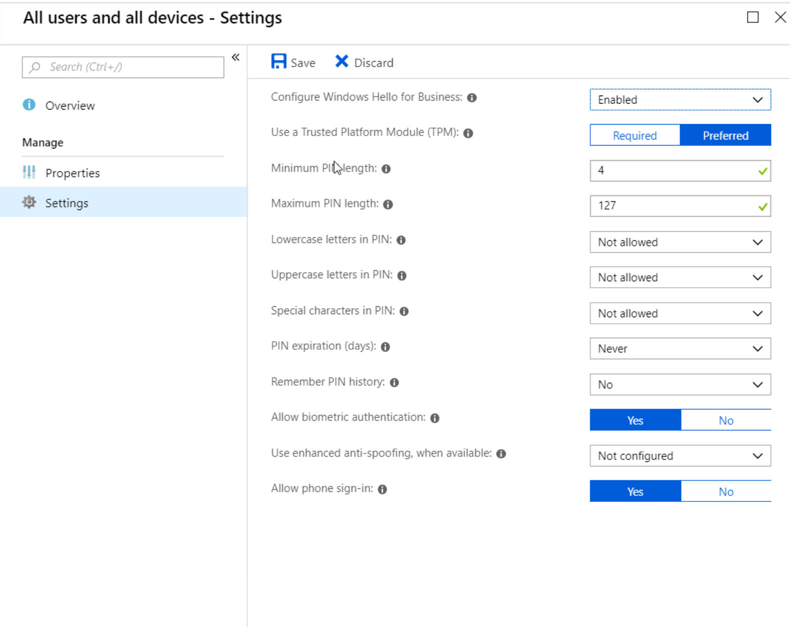
Show company logo: Yes | No

Upload a logo to use on theme color backgrounds: "2tcloud_400x.png"

Upload logo to use on light backgrounds: Select a file

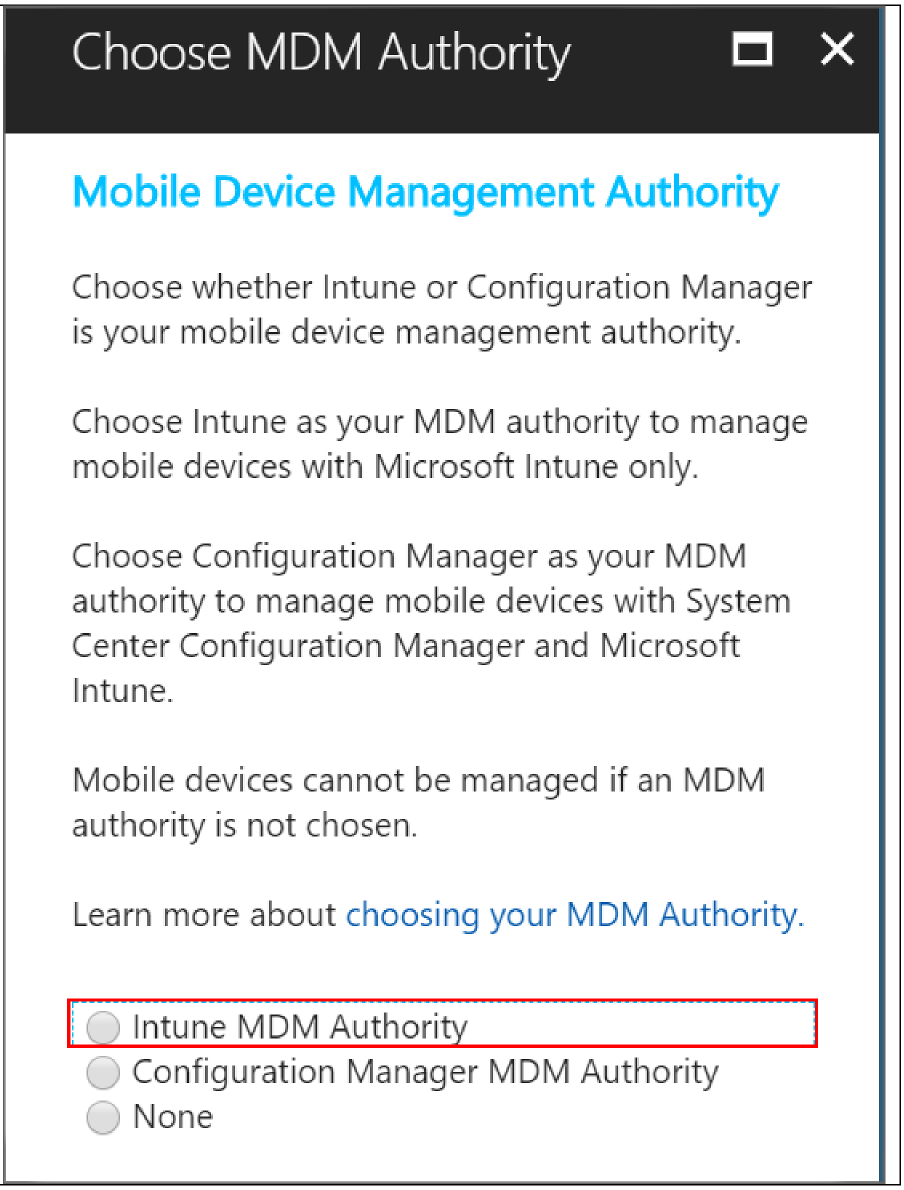
Exercise 6: Windows Hello

With Windows Hello you can allow user to access their devices using a gesture, such as biometric authentication, or a PIN.

Go to portal.azure.com and select Microsoft Intune. Then select Device Enrollment → Windows enrollment. There you can select Windows Hello For Business	 Home > Microsoft Intune > Device enrollment - Windows enrollment > Windows enrollment > All users and all devices - Settings Search (Ctrl+/) Overview Quick start Manage Apple enrollment Android enrollment Windows enrollment Terms and conditions Enrollment restrictions Device categories Corporate device identifiers Device enrollment managers Monitor Audit logs Help and support Help and support Device enrollment - Windows enrollment Microsoft Intune Use the following to help enroll Windows devices. General Windows Hello for Business Replace passwords with strong two-factor authentication. CNAME Validation Test company domain CNAME registration for Windows enrollment. Enrollment Status Page (Preview) Show app and profile installation statuses to users during device setup. Windows Autopilot Deployment Program Deployment Profiles Customize the Windows AutoPilot provisioning experience. Devices Manage Windows AutoPilot devices.
1. Select settings 2. At Configure Windows for Business select Enabled. 3. You can leave the default settings 4. And select Save	 All users and all devices - Settings Search (Ctrl+/) Overview Manage Properties Settings Save Discard Configure Windows Hello for Business: Enabled Use a Trusted Platform Module (TPM): Required [✓ Preferred] Minimum PIN length: 4 Maximum PIN length: 127 Lowercase letters in PIN: Not allowed Uppercase letters in PIN: Not allowed Special characters in PIN: Not allowed PIN expiration (days): Never Remember PIN history: No Allow biometric authentication: [✓ Yes] No Use enhanced anti-spoofing, when available: Not configured Allow phone sign-in: [✓ Yes] No

Exercise 7 Set MDM authority to Intune

1. From the Azure Portal go to All Services → Intune
2. select the orange banner to open the Mobile Device Management Authority setting. The orange banner is only displayed if you haven't yet set the MDM authority.
3. Under Mobile Device Management Authority, choose Intune as your MDM authority



Choose MDM Authority

Mobile Device Management Authority

Choose whether Intune or Configuration Manager is your mobile device management authority.

Choose Intune as your MDM authority to manage mobile devices with Microsoft Intune only.

Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

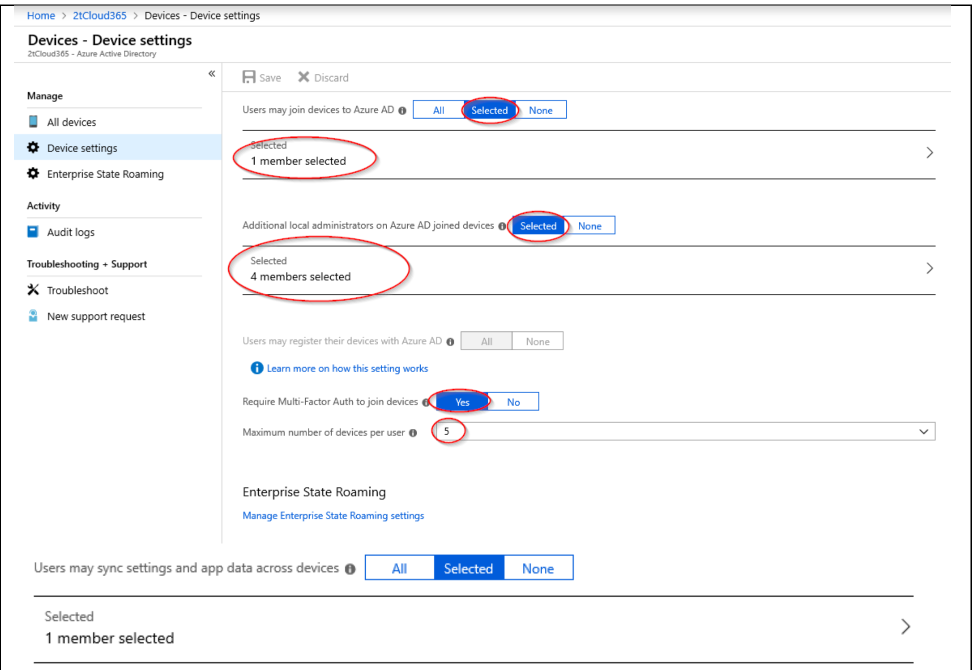
Mobile devices cannot be managed if an MDM authority is not chosen.

Learn more about choosing your MDM Authority.

○ Intune MDM Authority
○ Configuration Manager MDM Authority
○ None

Exercise 8: Device Settings

<table>
<tr>
<td>1. Go to <b>Azure Active Directory ->Users and groups -> Device Settings;</b></td>
<td>



Home > 2tCloud365 > Devices - Device settings

Devices - Device settings
2tCloud365 - Azure Active Directory

Users may join devices to Azure AD: All / [✓ Selected] / None
Selected: 1 member selected

Additional local administrators on Azure AD joined devices: [✓ Selected] / None
Selected: 4 members selected

Users may register their devices with Azure AD: All / None
Learn more on how this setting works

Require Multi-Factor Auth to join devices: [✓ Yes] / No

Maximum number of devices per user: 5

Enterprise State Roaming
Manage Enterprise State Roaming settings

Users may sync settings and app data across devices: All / [✓ Selected] / None
Selected: 1 member selected

</td>
</tr>
<tr>
<td>2. Configure the settings --&gt; Click <b>Save</b></td>
<td>
<table>
<tr><td>Users may join devices to Azure AD</td><td>UG_Gebruikers_MDM</td></tr>
<tr><td>Additional local administrators on Azure AD Joined Devices</td><td>Selected -&gt; Admin</td></tr>
<tr><td>Require Multi-Factor Auth to join devices</td><td>Yes</td></tr>
<tr><td>Maximum number of devices per user</td><td>5</td></tr>
<tr><td>Users may sync settings and enterprise app data</td><td>UG_Gebruikers_MDM</td></tr>
</table>
</td>
</tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
<tr><td></td><td></td></tr>
</table>

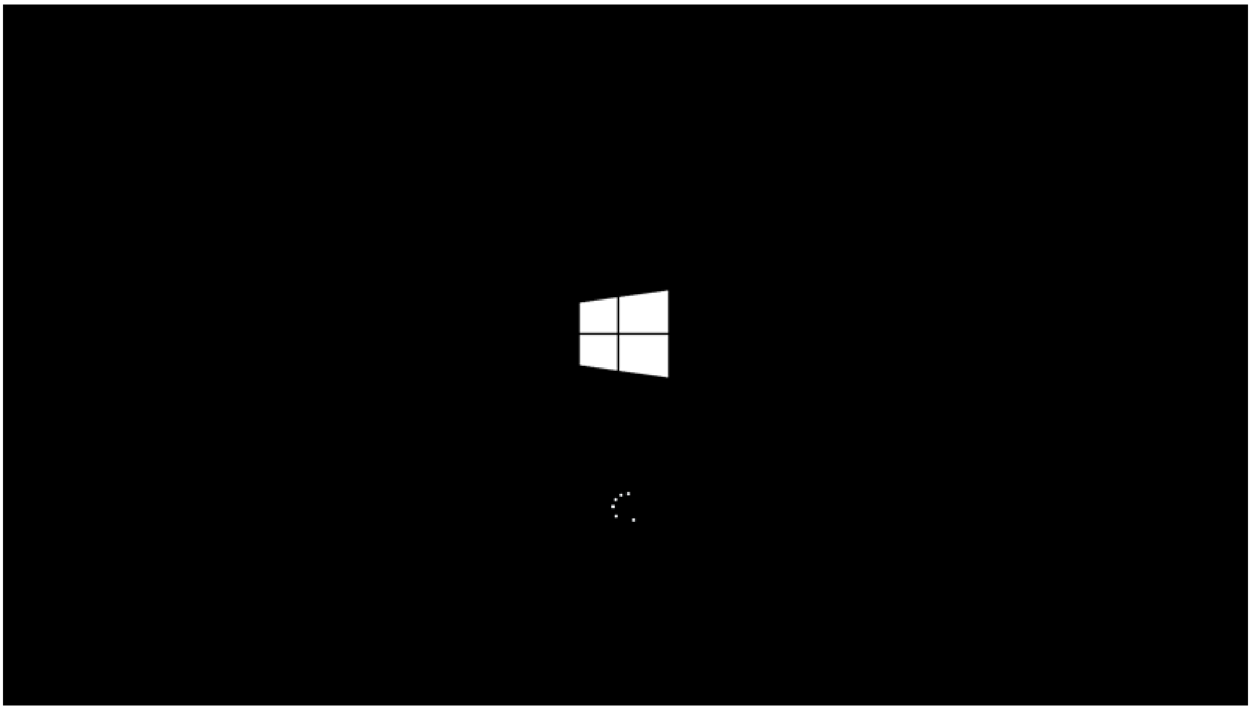
Activity 3: Add Windows to MDM

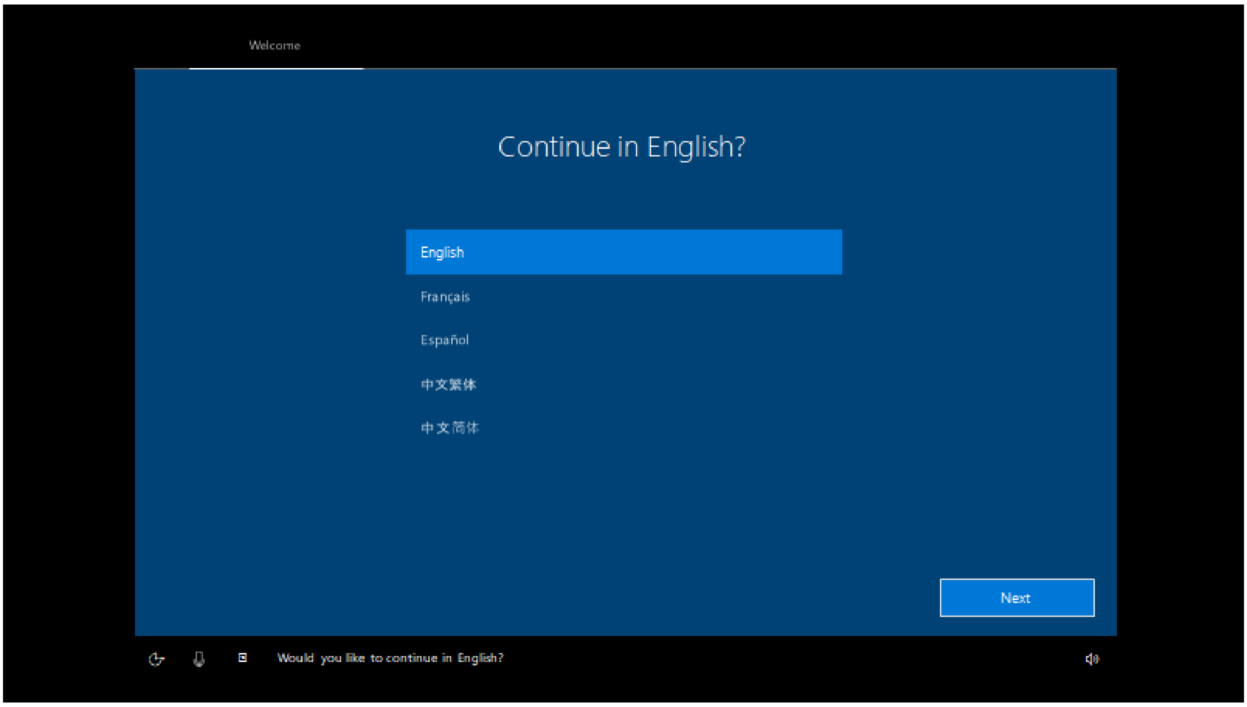
Exercise 9: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)

Go to the Win10 VM (Azure or Hyper-V Manager)

Exersize 9b (Optional) – Hyper V Win10 VM

Start the setup of the Windows 10 Enterprise OS, and sign in with your test account





Welcome

Continue in English?

English

Français

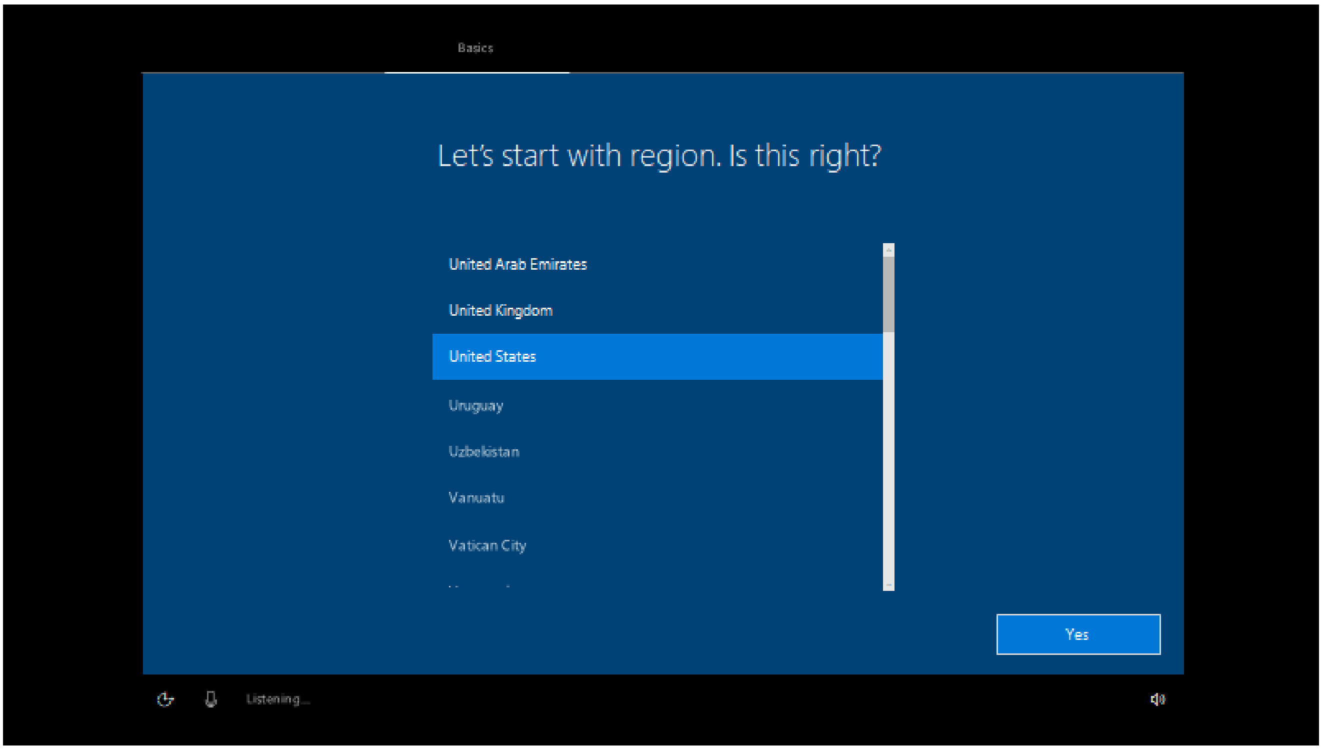
Español

中文繁体

中文简体

Next

Would you like to continue in English?



Basics

Let's start with region. Is this right?

United Arab Emirates

United Kingdom

United States

Uruguay

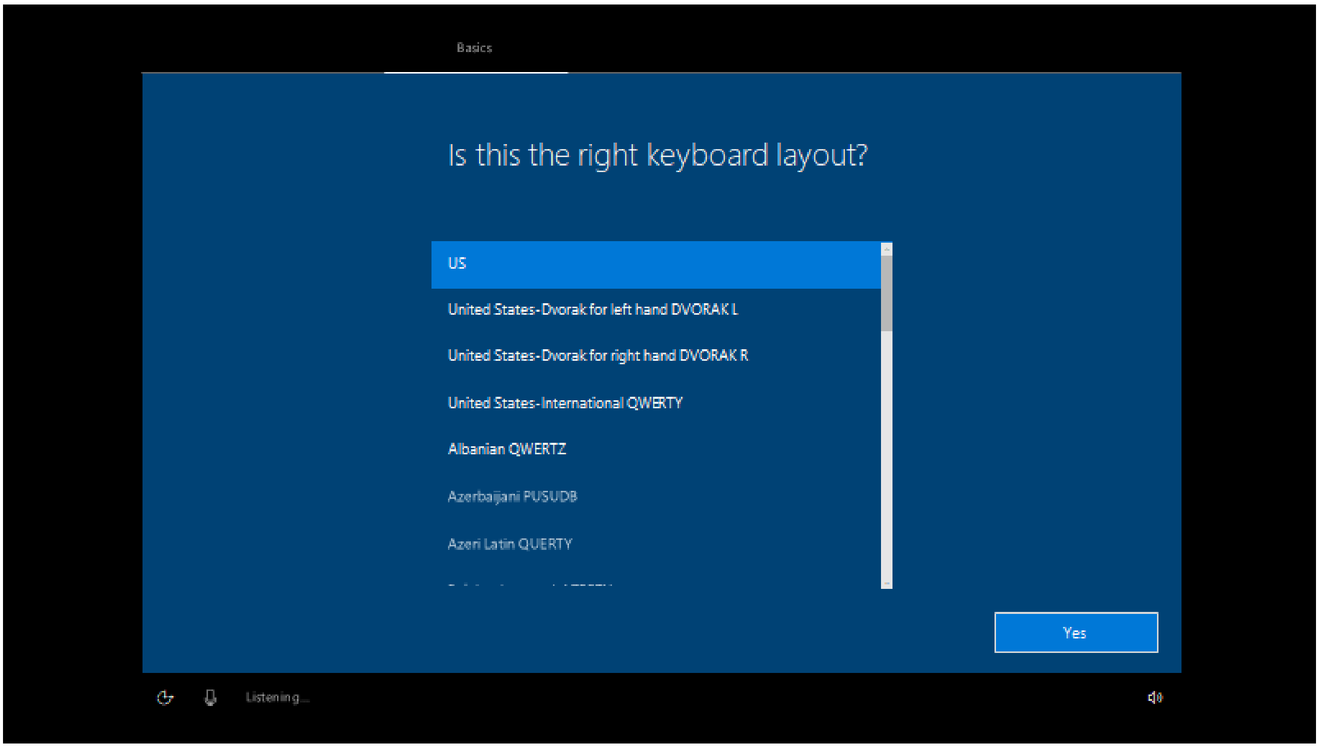
Uzbekistan

Vanuatu

Vatican City

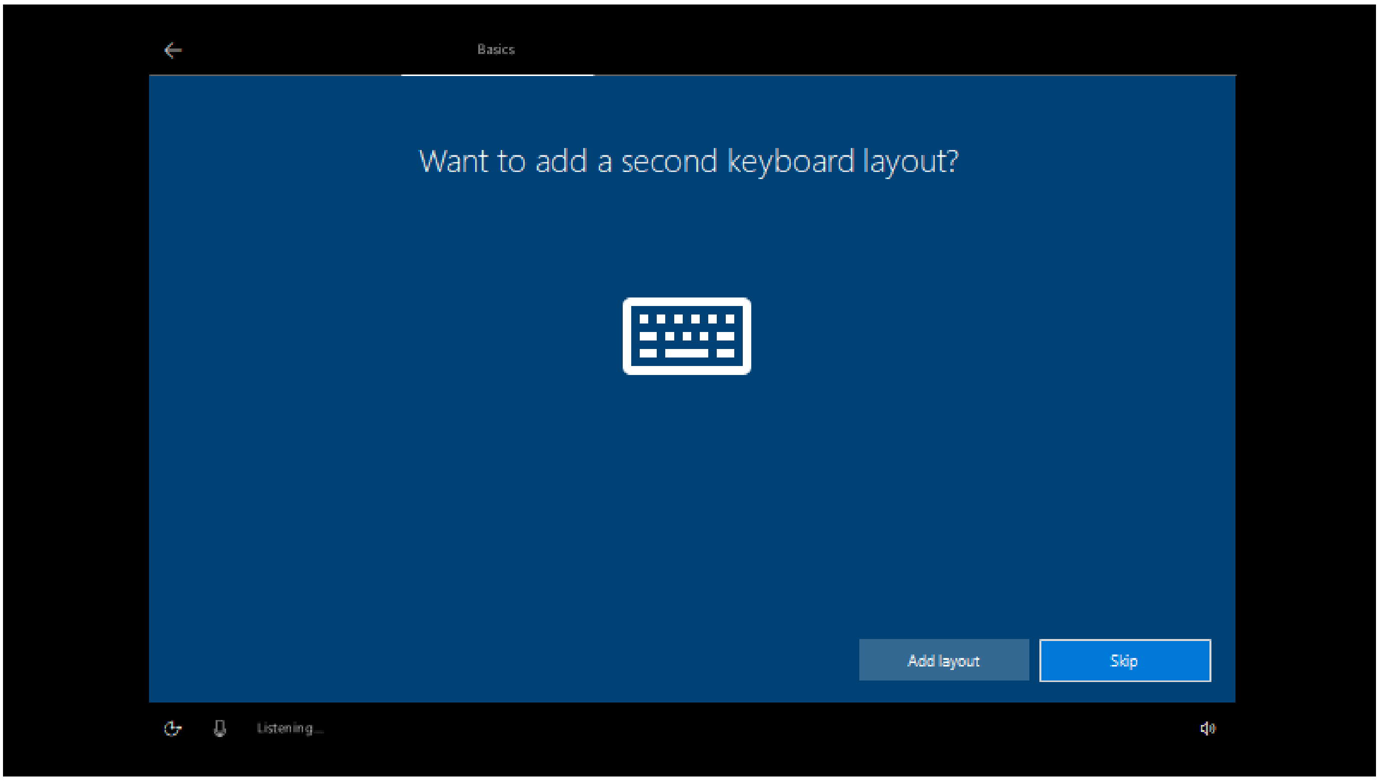
Yes

Listening...

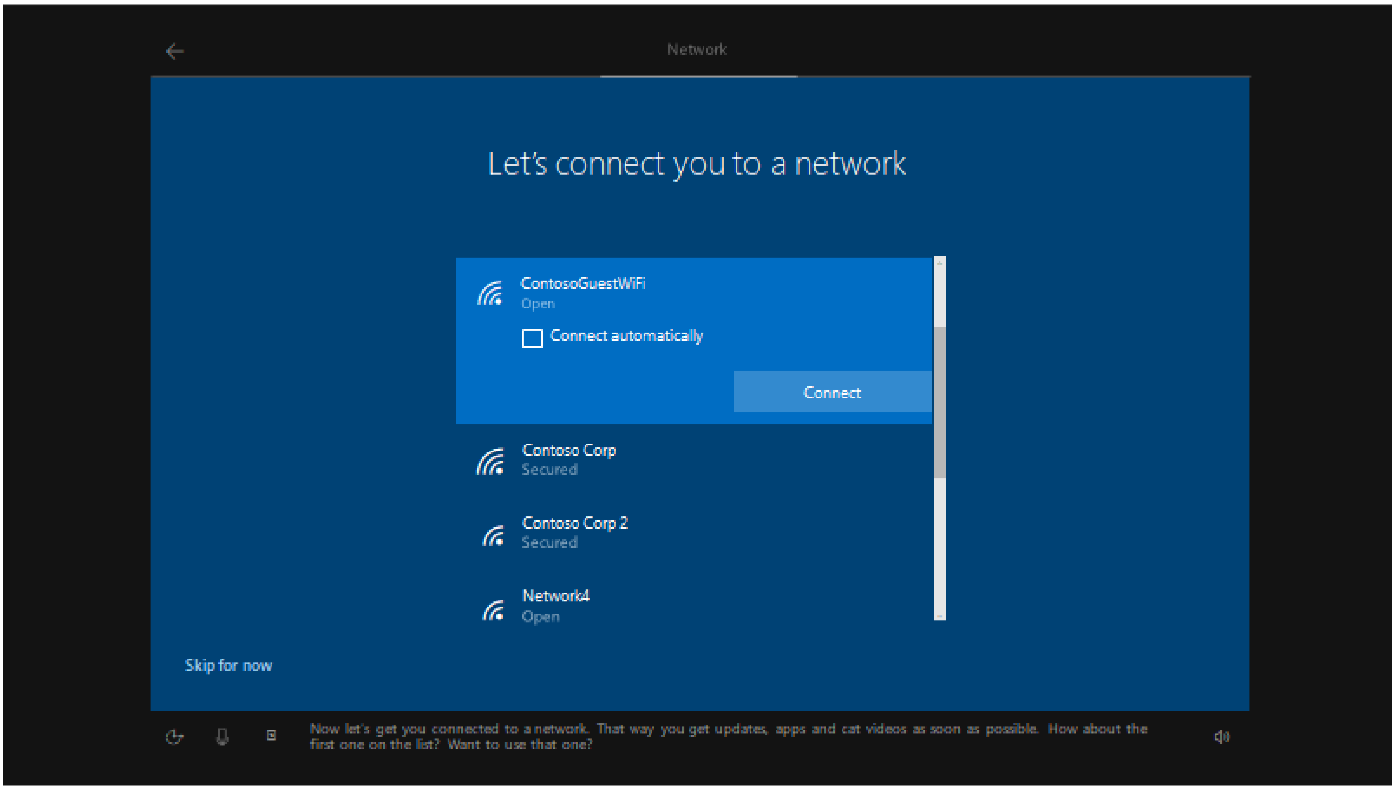


Is this the right keyboard layout?

Basics
US
United States-Dvorak for left hand DVORAK L
United States-Dvorak for right hand DVORAK R
United States-International QWERTY
Albanian QWERTZ
Azerbaijani PUSUDB
Azeri Latin QUERTY
Yes
Listening...



Want to add a second keyboard layout?



Let's connect you to a network

ContosoGuestWiFi
Open

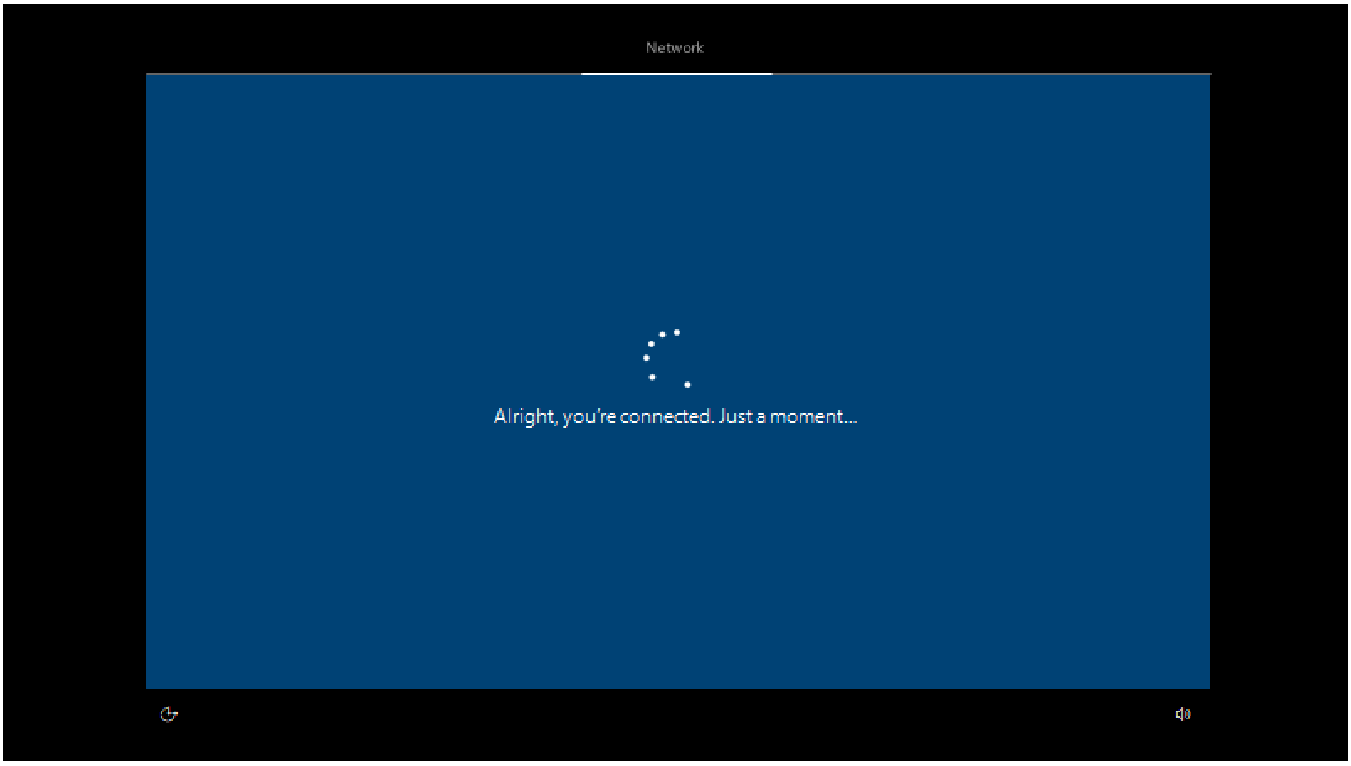
□ Connect automatically

Contoso Corp
Secured

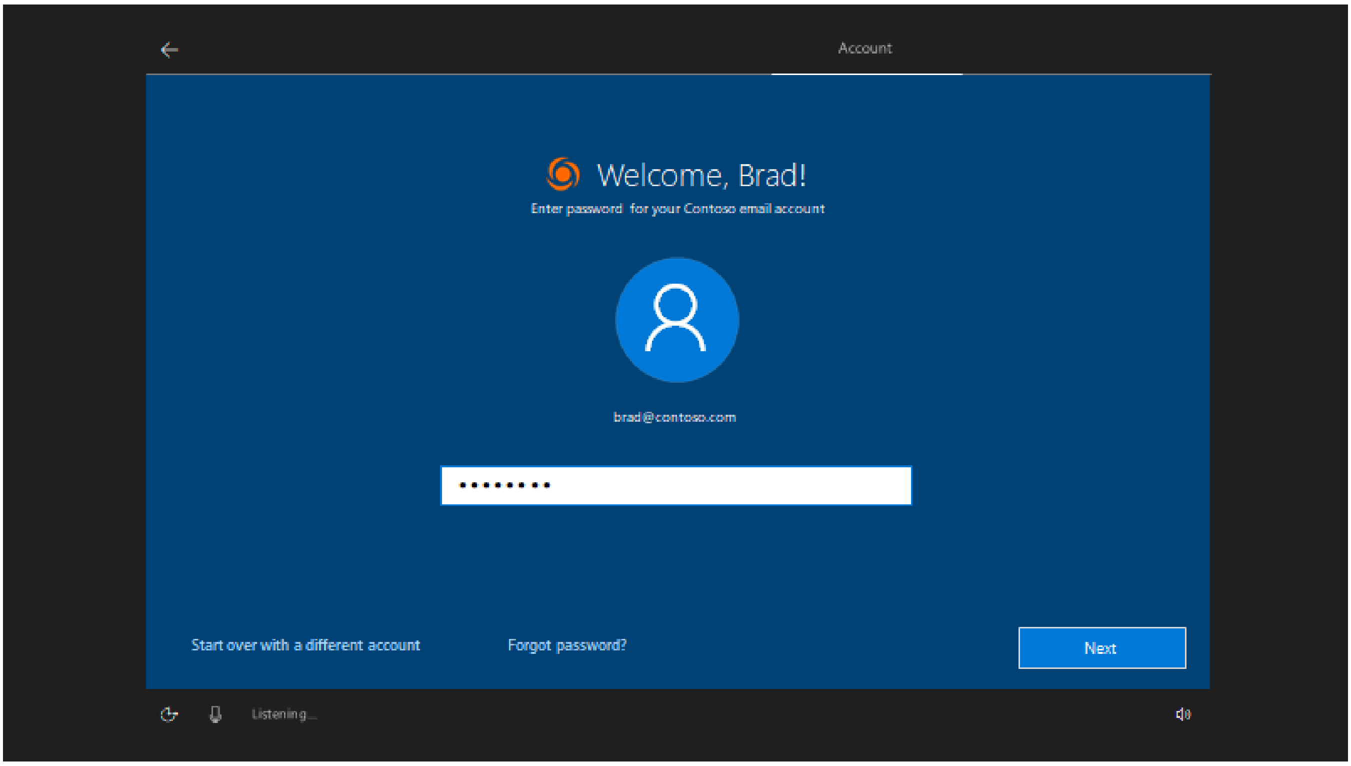
Contoso Corp 2
Secured

Network4
Open

Now let's get you connected to a network. That way you get updates, apps and cat videos as soon as possible. How about the first one on the list? Want to use that one?



Alright, you're connected. Just a moment...

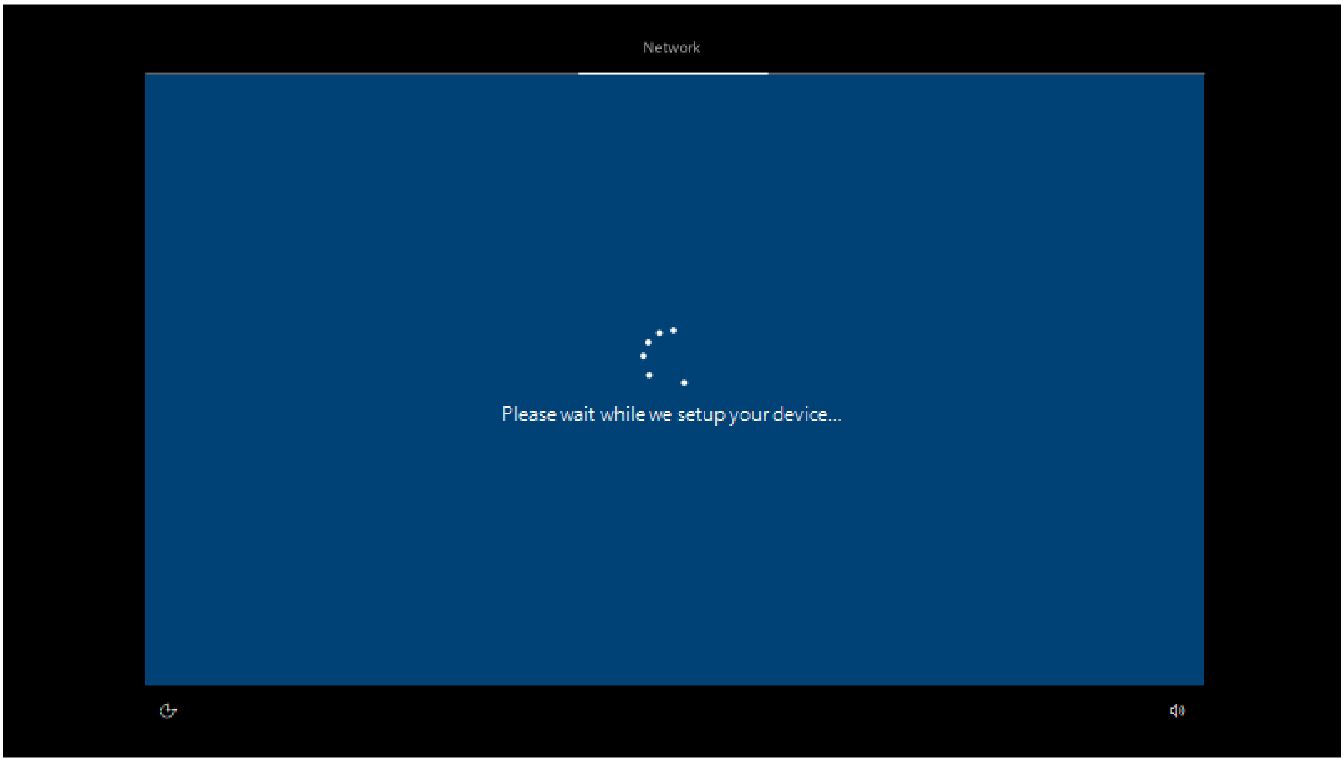


Welcome, Brad!

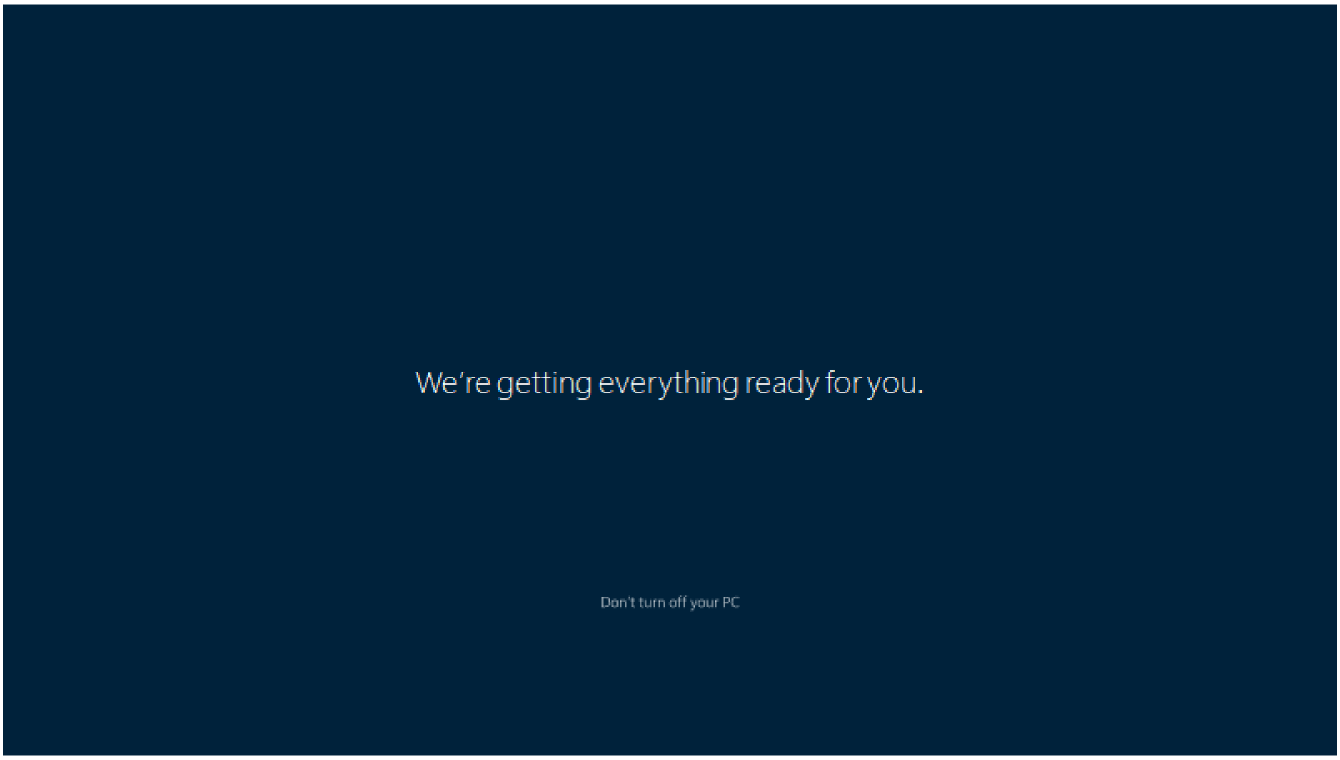
Enter password for your Contoso email account

brad@contoso.com

••••••••

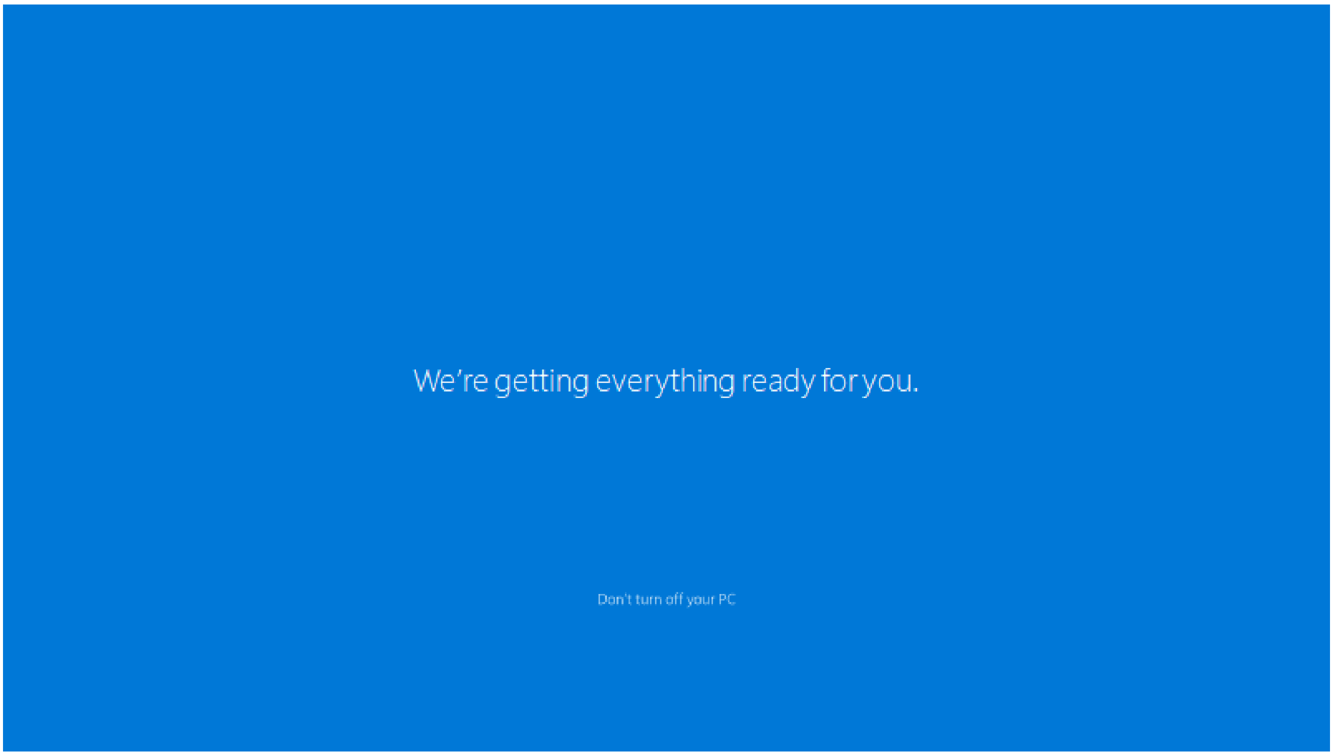


Please wait while we setup your device...



We're getting everything ready for you.

Don't turn off your PC



We're getting everything ready for you.

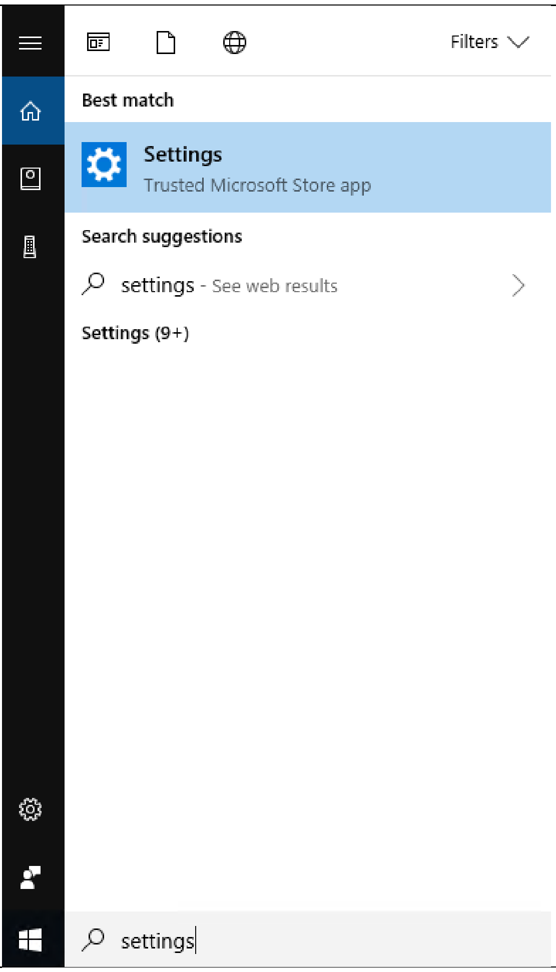
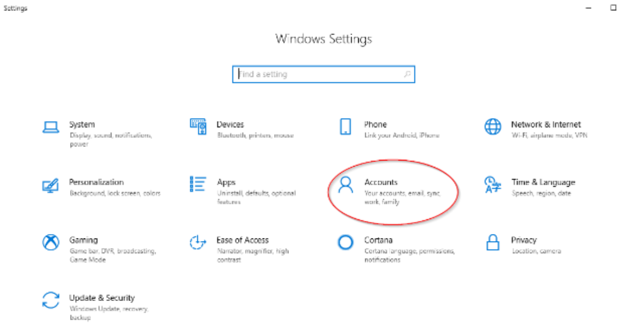
Don't turn off your PC

Exersize 9c (Optional) - Azure steps OPTIONAL

1. Open the RDP file you created in Excersize 1b.
2. Sign in the device

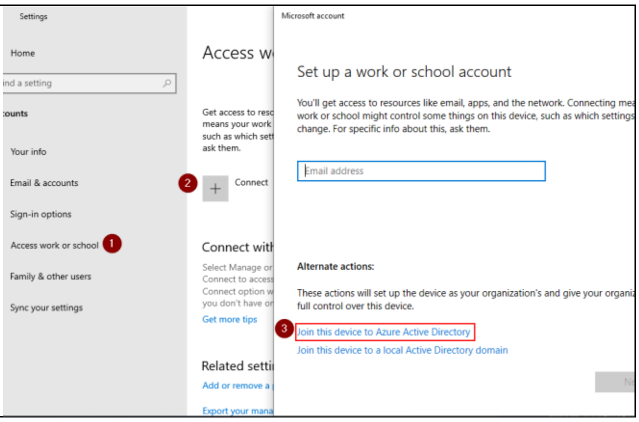
This section outlines how to enroll a Windows 10 device into Microsoft Intune for MDM.

Complete these steps on the M365holwin10vm virtual machine.

Enroll a Windows 10 Device in Intune 1. Login to the virtual machine and go to **Start > Settings**.	
2. In the **Settings** app, browse to **Accounts > Access work or school**.	

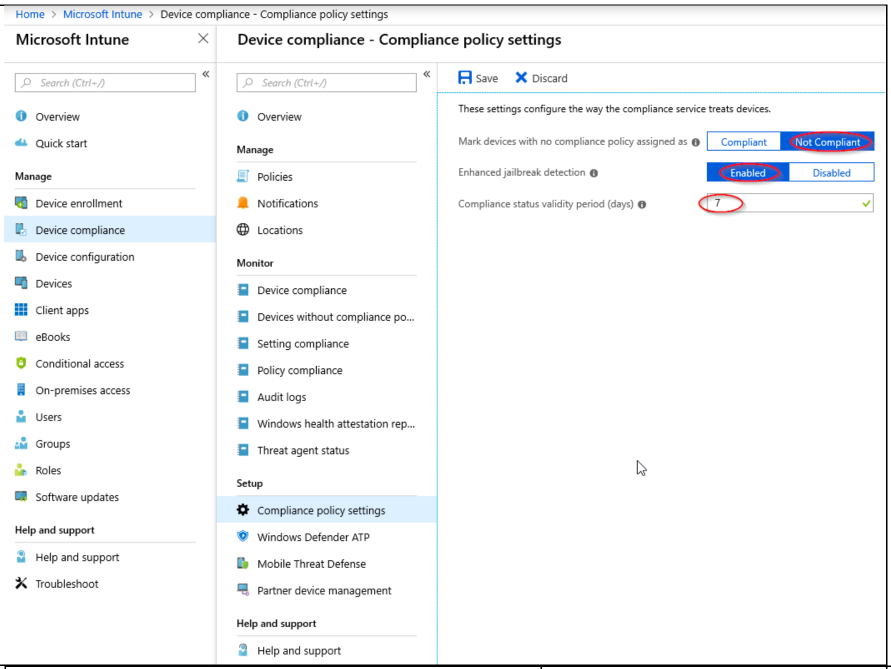
Filters
Best match
Settings
Trusted Microsoft Store app
Search suggestions
settings - See web results
Settings (9+)
settings

Settings
Windows Settings
Find a setting
System
Display, sound, notifications, power
Devices
Bluetooth, printers, mouse
Phone
Link your Android, iPhone
Network & Internet
Wi-Fi, airplane mode, VPN
Personalization
Background, lock screen, colors
Apps
Uninstall, defaults, optional features
Accounts
Your accounts, email, sync, work, family
Time & Language
Speech, region, date
Gaming
Game bar, DVR, broadcasting, Game Mode
Ease of Access
Narrator, magnifier, high contrast
Cortana
Cortana language, permissions, notifications
Privacy
Location, camera
Update & Security
Windows Update, recovery, backup

3. Click **Connect**. 4. The **Setup a work or school account** dialog box will show, asking for your account to enroll the device. 5. Select **Join this device to Azure Active Directory.** 6. Provide the **Azure AD** account and click **Next**. 7. In the **Microsoft Intune Enrollment** page, enter the **password** then click **Sign in**. Click **Got it**. 8. In the **Settings** app, you should see that the device is now connected to the corporate MDM. Click **Sync** and confirm that the sync was **successful**.	 Settings Home ind a setting counts Your info Email & accounts Sign-in options Access work or school 1 Family & other users Sync your settings Access w Get access to reso means your work such as which sett ask them. 2 Connect Connect with Select Manage or Connect to access Connect option w you don't have or Get more tips Related setti Add or remove a Export your mana Microsoft account Set up a work or school account You'll get access to resources like email, apps, and the network. Connecting mea work or school might control some things on this device, such as which settings change. For specific info about this, ask them. Email address Alternate actions: These actions will set up the device as your organization's and give your organiz full control over this device. 3 Join this device to Azure Active Directory Join this device to a local Active Directory domain N

Activity 4: Configuration Intune

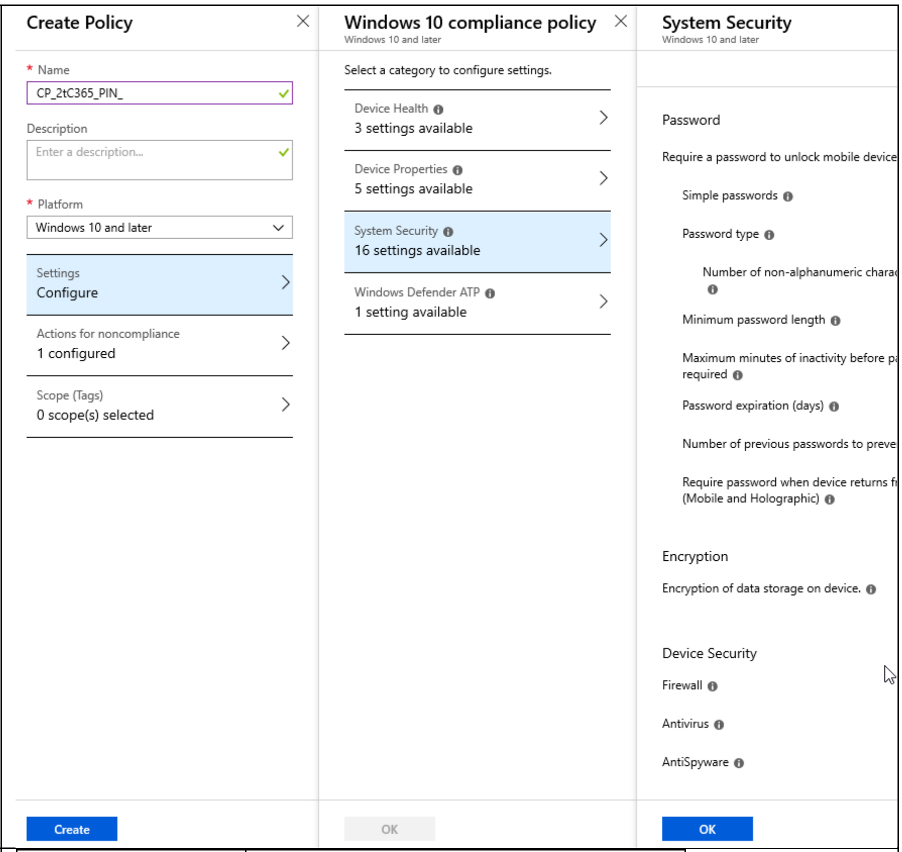
Exercise 10: Device Compliance

<table>
<tr>
<td>1. Go to <b>Intune->Device Compliance -> Compliance policy settings</b></td>
<td>

Home &gt; Microsoft Intune &gt; Device compliance - Compliance policy settings
Microsoft Intune
Search (Ctrl+/)
Overview
Quick start
Manage
Device enrollment
Device compliance
Device configuration
Devices
Client apps
eBooks
Conditional access
On-premises access
Users
Groups
Roles
Software updates
Help and support
Help and support
Troubleshoot
Device compliance - Compliance policy settings
Search (Ctrl+/)
Overview
Manage
Policies
Notifications
Locations
Monitor
Device compliance
Devices without compliance po...
Setting compliance
Policy compliance
Audit logs
Windows health attestation rep...
Threat agent status
Setup
Compliance policy settings
Windows Defender ATP
Mobile Threat Defense
Partner device management
Help and support
Help and support
Save
Discard

These settings configure the way the compliance service treats devices.
Mark devices with no compliance policy assigned as Compliant [✓ Not Compliant]
Enhanced jailbreak detection [✓ Enabled] Disabled
Compliance status validity period (days) 7</td>
</tr>
<tr>
<td>2. Configure the settings &gt; Click <b>Save</b></td>
<td><table><tr><td>Mark devices with no compliance</td><td>Not Compliant</td></tr><tr><td>Enhanced Jailbreak detection</td><td>Enabled</td></tr><tr><td>Compliance status validity period</td><td>7</td></tr></table></td>
</tr>
</table>

3. Go to **Intune->Device Compliance->Policies->Create Policy;**



Create Policy

* Name
CP_2tC365_PIN_

Description
Enter a description...

* Platform
Windows 10 and later

Settings
Configure

Actions for noncompliance
1 configured

Scope (Tags)
0 scope(s) selected

Create

Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health
3 settings available

Device Properties
5 settings available

System Security
16 settings available

Windows Defender ATP
1 setting available

OK

System Security
Windows 10 and later

Password

Require a password to unlock mobile device

Simple passwords

Password type

Number of non-alphanumeric chara

Minimum password length

Maximum minutes of inactivity before p
required

Password expiration (days)

Number of previous passwords to preve

Require password when device returns f
(Mobile and Holographic)

Encryption

Encryption of data storage on device.

Device Security

Firewall

Antivirus

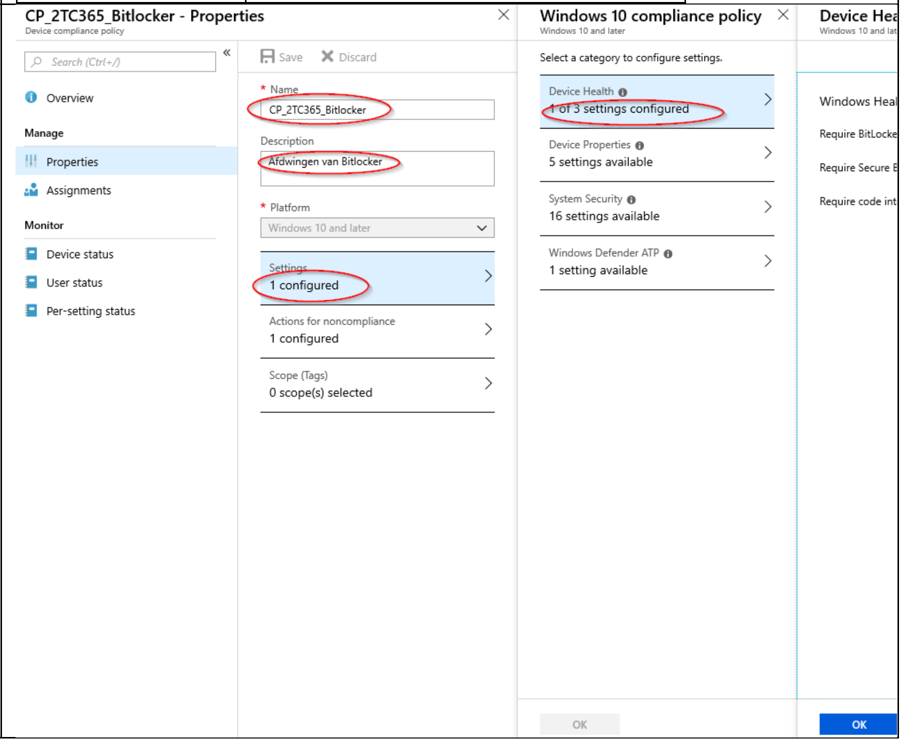
AntiSpyware

OK

4. Configure the settings >

Name	CP_2tC365_PIN
Platform	Windows 10 and later

5. Repeat steps 1 / 4 for **another policy (Bitlocker)**



CP_2TC365_Bitlocker - Properties
Device compliance policy

Search (Ctrl+/)

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Per-setting status

Save Discard

* Name
CP_2TC365_Bitlocker

Description
Afdwingen van Bitlocker

* Platform
Windows 10 and later

Settings
1 configured

Actions for noncompliance
1 configured

Scope (Tags)
0 scope(s) selected

Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health
1 of 3 settings configured

Device Properties
5 settings available

System Security
16 settings available

Windows Defender ATP
1 setting available

OK

Device Hea
Windows 10 and lat

Windows Heal

Require BitLocke

Require Secure B

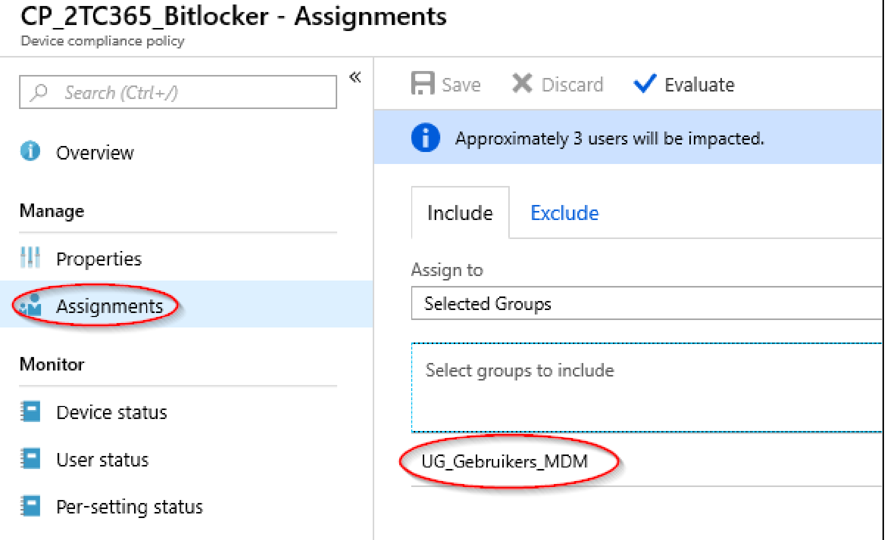
Require code int

OK

6. Configure the settings -> Click **Ok**
7. Click on **Configure**
8. Configure settings as showed on the screenshot -> Click **Save**
9.

Name	CP_2TC365_Bitlocker
Description	Afdwingen van Bitlocker
Platform	Windows 10 and later

10. Go to Intune->Device Compliance->Policies-> **CP_2TC365_Bitlocker->** Assignments-> Select groups



CP_2TC365_Bitlocker - Assignments
Device compliance policy

Approximately 3 users will be impacted.

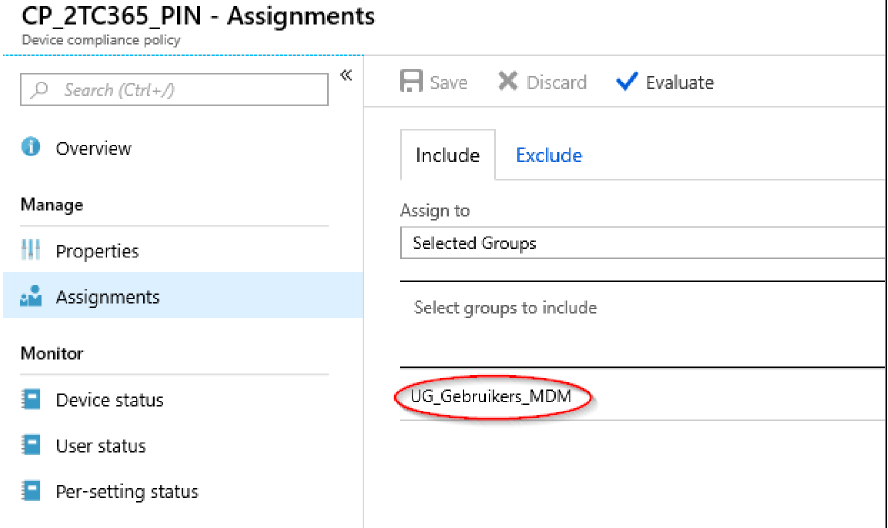
Assign to: Selected Groups

Select groups to include: UG_Gebruikers_MDM

11. Configure the settings > Click **Save**

Groups	UG_Gebruikers_MDM

12. Go to Intune->Device Compliance -> Policies-> **CP_2tC365_PIN** -> Assignments-> Select groups;



CP_2TC365_PIN - Assignments
Device compliance policy

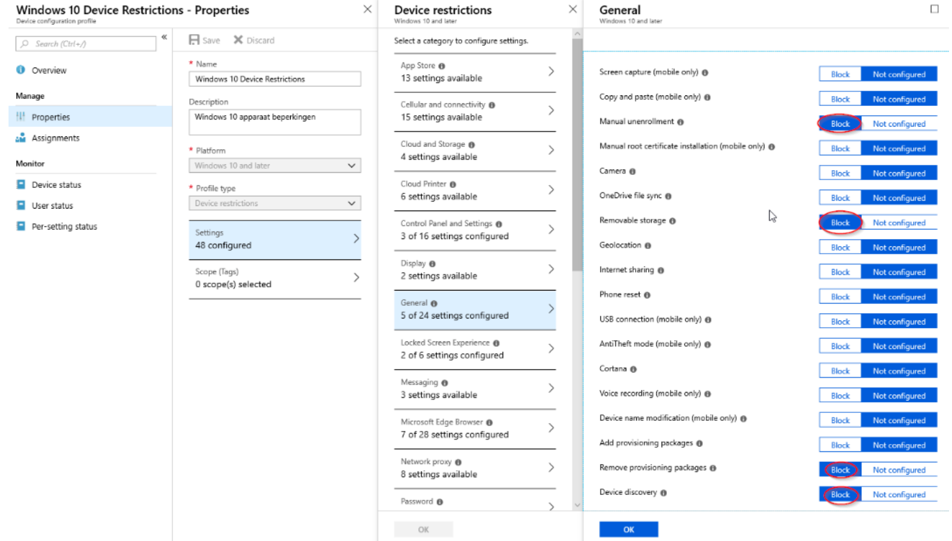
Assign to: Selected Groups

Select groups to include: UG_Gebruikers_MDM

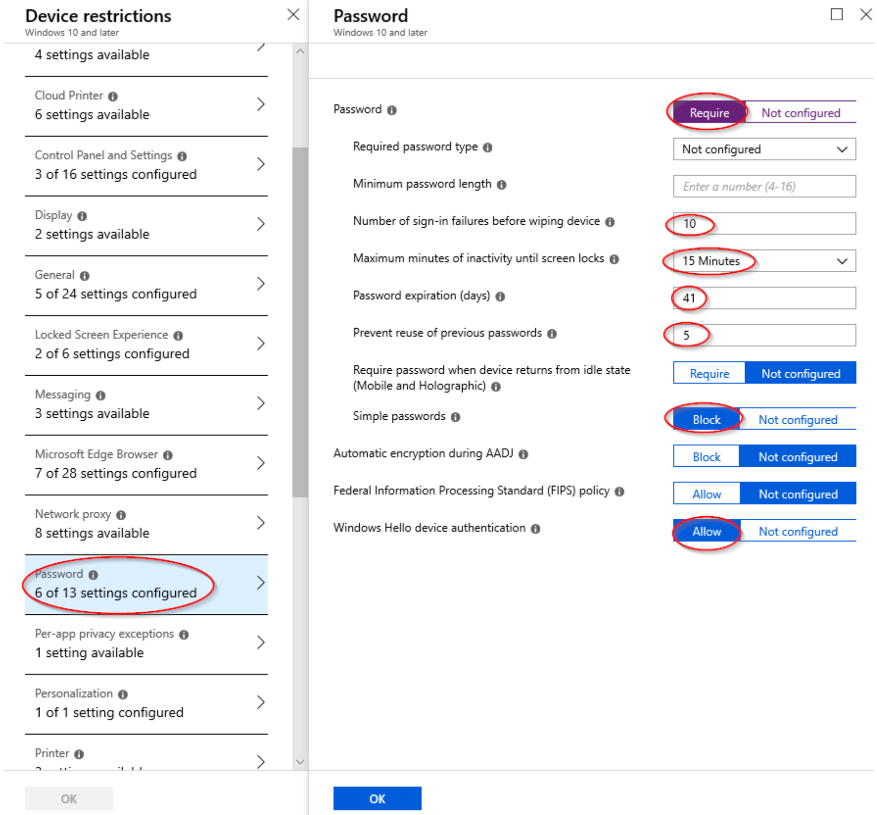
13. Configure the settings > Click **Save**

Groups	UG_Gebruikers_MDM

Exercise 11a: Device Configuration - Windows Device Restrictions

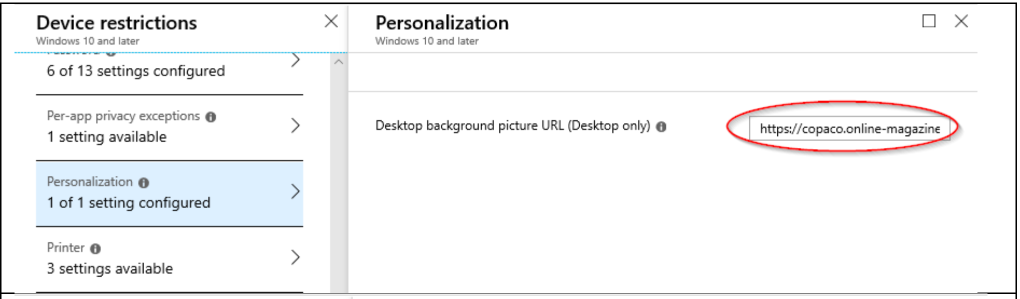
<table>
<tr>
<td>1. Go to <b>Intune->Device Configuration-> Profiles-> Create Profile;</b></td>
<td>
Windows 10 Device Restrictions - Properties
Device configuration profile
Search (Ctrl+/)
Overview
Manage
Properties
Assignments
Monitor
Device status
User status
Per-setting status
Save Discard
* Name: Windows 10 Device Restrictions
Description: Windows 10 apparaat beperkingen
* Platform: Windows 10 and later
* Profile type: Device restrictions
Settings: 48 configured
Scope (Tags): 0 scope(s) selected

Device restrictions
Windows 10 and later
Select a category to configure settings.
App Store: 13 settings available
Cellular and connectivity: 15 settings available
Cloud and Storage: 4 settings available
Cloud Printer: 6 settings available
Control Panel and Settings: 3 of 16 settings configured
Display: 2 settings available
General: 5 of 24 settings configured
Locked Screen Experience: 2 of 6 settings configured
Messaging: 3 settings available
Microsoft Edge Browser: 7 of 28 settings configured
Network proxy: 8 settings available
Password
OK

General
Windows 10 and later
Screen capture (mobile only): Block [✓ Not configured]
Copy and paste (mobile only): Block [✓ Not configured]
Manual unenrollment: [✓ Block] Not configured
Manual root certificate installation (mobile only): Block [✓ Not configured]
Camera: Block [✓ Not configured]
OneDrive file sync: Block [✓ Not configured]
Removable storage: [✓ Block] Not configured
Geolocation: Block [✓ Not configured]
Internet sharing: Block [✓ Not configured]
Phone reset: Block [✓ Not configured]
USB connection (mobile only): Block [✓ Not configured]
AntiTheft mode (mobile only): Block [✓ Not configured]
Cortana: Block [✓ Not configured]
Voice recording (mobile only): Block [✓ Not configured]
Device name modification (mobile only): Block [✓ Not configured]
Add provisioning packages: Block [✓ Not configured]
Remove provisioning packages: [✓ Block] Not configured
Device discovery: [✓ Block] Not configured
OK</td>
</tr>
<tr>
<td>2. Configure the settings &gt;</td>
<td>
<table>
<tr><td>Name</td><td>Windows 10 – Device Restrictions</td></tr>
<tr><td>Platform</td><td>Windows 10 and later</td></tr>
<tr><td>Profile type</td><td>Device restrictions</td></tr>
</table>
</td>
</tr>
<tr>
<td><b>3.</b> Configure settings as showed on the screenshot (Password)</td>
<td>
Device restrictions
Windows 10 and later
4 settings available
Cloud Printer: 6 settings available
Control Panel and Settings: 3 of 16 settings configured
Display: 2 settings available
General: 5 of 24 settings configured
Locked Screen Experience: 2 of 6 settings configured
Messaging: 3 settings available
Microsoft Edge Browser: 7 of 28 settings configured
Network proxy: 8 settings available
Password: 6 of 13 settings configured
Per-app privacy exceptions: 1 setting available
Personalization: 1 of 1 setting configured
Printer
OK

Password
Windows 10 and later
Password: [✓ Require] Not configured
Required password type: Not configured
Minimum password length: Enter a number (4-16)
Number of sign-in failures before wiping device: 10
Maximum minutes of inactivity until screen locks: 15 Minutes
Password expiration (days): 41
Prevent reuse of previous passwords: 5
Require password when device returns from idle state (Mobile and Holographic): Require [✓ Not configured]
Simple passwords: [✓ Block] Not configured
Automatic encryption during AADJ: Block [✓ Not configured]
Federal Information Processing Standard (FIPS) policy: Allow [✓ Not configured]
Windows Hello device authentication: [✓ Allow] Not configured
OK</td>
</tr>
</table>

4. Configure settings as showed on the screenshot (Personalization)



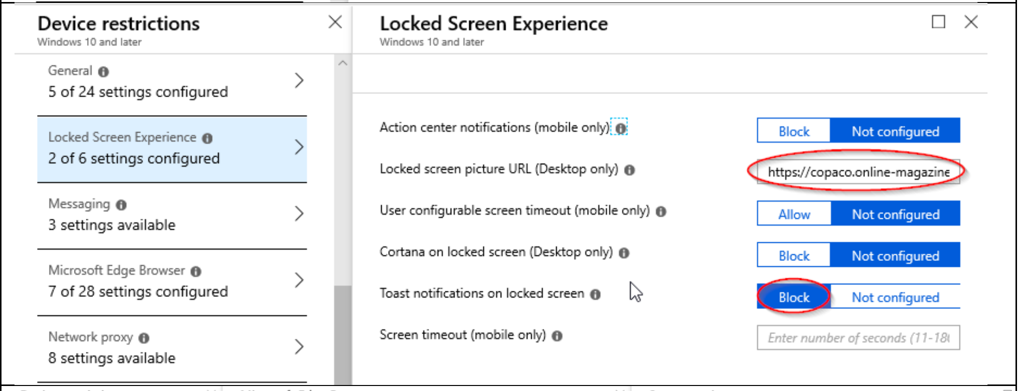
Device restrictions
Windows 10 and later

- 6 of 13 settings configured
- Per-app privacy exceptions — 1 setting available
- Personalization — 1 of 1 setting configured
- Printer — 3 settings available

Personalization
Windows 10 and later

Desktop background picture URL (Desktop only): https://copaco.online-magazine

5. Configure settings as showed on the screenshot (Lock Screen Experience)



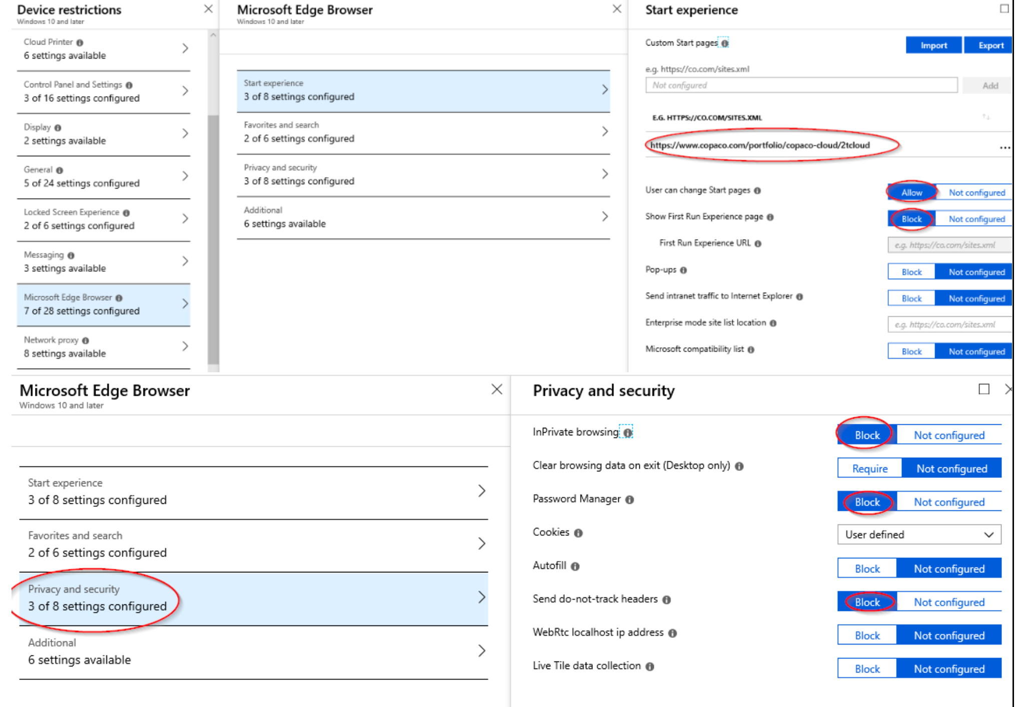
Device restrictions
Windows 10 and later

- General — 5 of 24 settings configured
- Locked Screen Experience — 2 of 6 settings configured
- Messaging — 3 settings available
- Microsoft Edge Browser — 7 of 28 settings configured
- Network proxy — 8 settings available

Locked Screen Experience
Windows 10 and later

- Action center notifications (mobile only): Block [✓ Not configured]
- Locked screen picture URL (Desktop only): https://copaco.online-magazine
- User configurable screen timeout (mobile only): Allow [✓ Not configured]
- Cortana on locked screen (Desktop only): Block [✓ Not configured]
- Toast notifications on locked screen: [✓ Block] Not configured
- Screen timeout (mobile only): Enter number of seconds (11-18

6. Configure settings as showed on the screenshot (Edge)



Device restrictions
Windows 10 and later

- Cloud Printer — 6 settings available
- Control Panel and Settings — 3 of 16 settings configured
- Display — 2 settings available
- General — 5 of 24 settings configured
- Locked Screen Experience — 2 of 6 settings configured
- Messaging — 3 settings available
- Microsoft Edge Browser — 7 of 28 settings configured
- Network proxy — 8 settings available

Microsoft Edge Browser
Windows 10 and later

- Start experience — 3 of 8 settings configured
- Favorites and search — 2 of 6 settings configured
- Privacy and security — 3 of 8 settings configured
- Additional — 6 settings available

Start experience

- Custom Start pages: e.g. https://co.com/sites.xml — Not configured
- E.G. HTTPS://CO.COM/SITES.XML: https://www.copaco.com/portfolio/copaco-cloud/2tcloud
- User can change Start pages: [✓ Allow] Not configured
- Show First Run Experience page: [✓ Block] Not configured
- First Run Experience URL: e.g. https://co.com/sites.xml
- Pop-ups: Block [✓ Not configured]
- Send intranet traffic to Internet Explorer: Block [✓ Not configured]
- Enterprise mode site list location: e.g. https://co.com/sites.xml
- Microsoft compatibility list: Block [✓ Not configured]

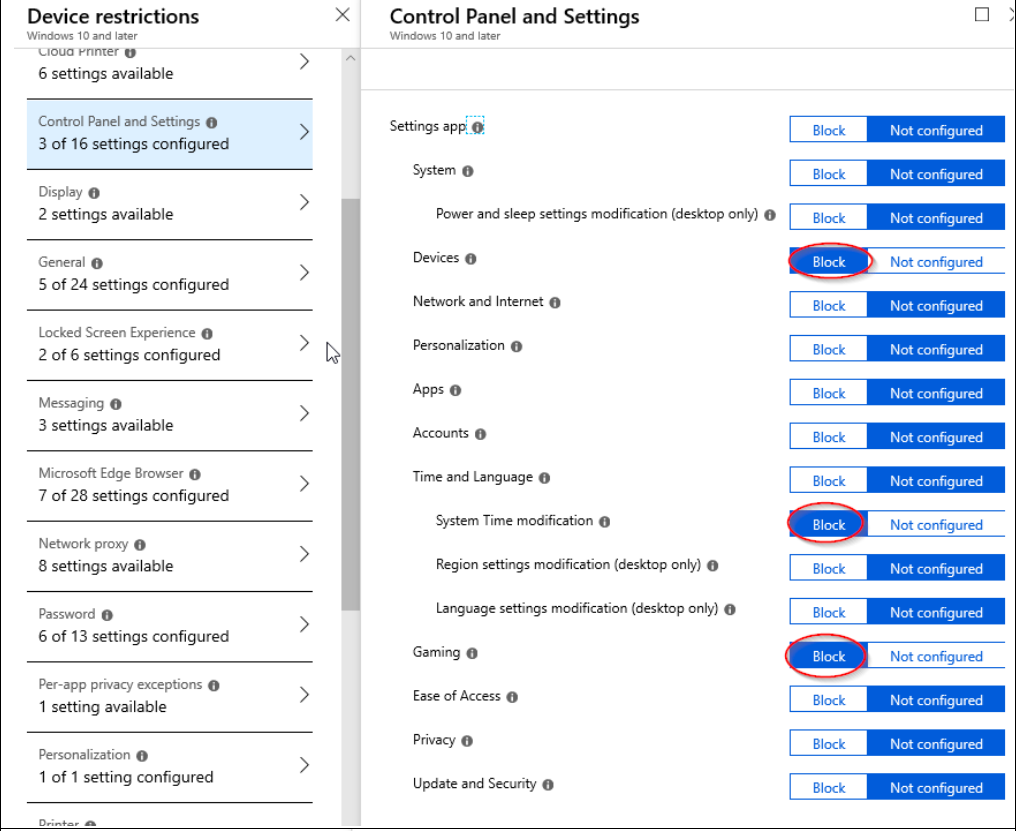
Microsoft Edge Browser
Windows 10 and later

- Start experience — 3 of 8 settings configured
- Favorites and search — 2 of 6 settings configured
- Privacy and security — 3 of 8 settings configured
- Additional — 6 settings available

Privacy and security

- InPrivate browsing: [✓ Block] Not configured
- Clear browsing data on exit (Desktop only): Require [✓ Not configured]
- Password Manager: [✓ Block] Not configured
- Cookies: User defined
- Autofill: Block [✓ Not configured]
- Send do-not-track headers: [✓ Block] Not configured
- WebRtc localhost ip address: Block [✓ Not configured]
- Live Tile data collection: Block [✓ Not configured]

7. Configure settings as showed on the screenshots (Control Panel)



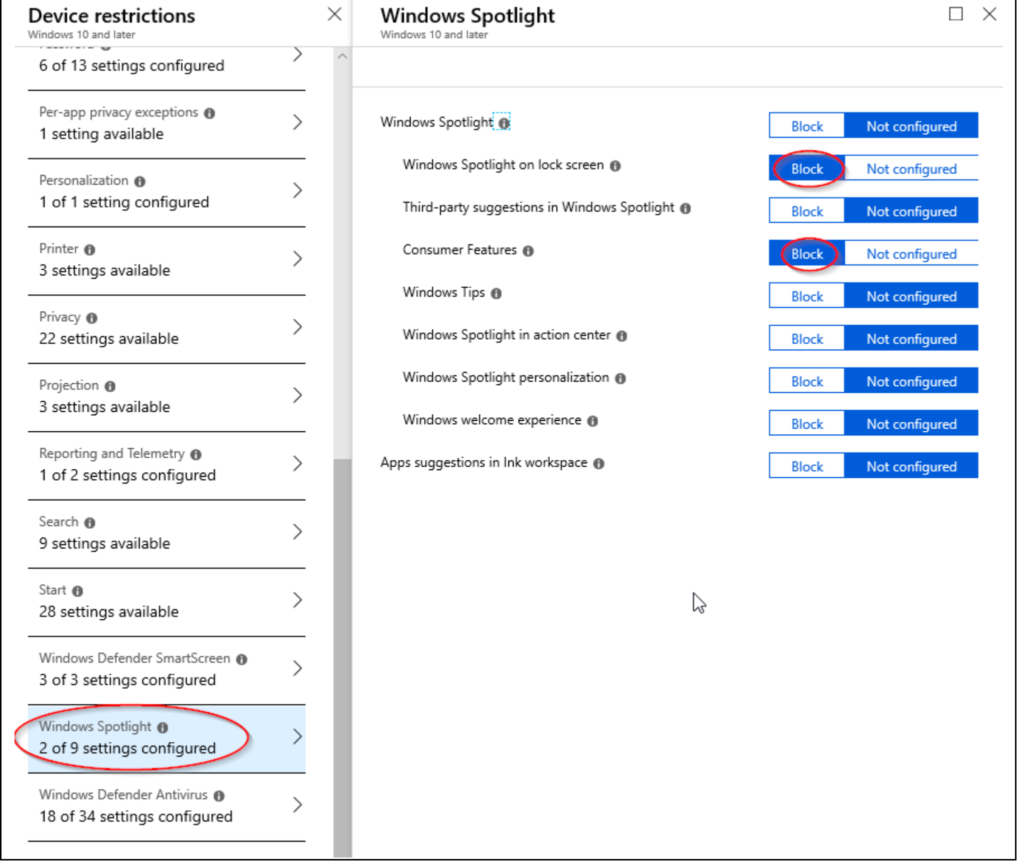
Device restrictions
Windows 10 and later

- Cloud Printer — 6 settings available
- Control Panel and Settings — 3 of 16 settings configured
- Display — 2 settings available
- General — 5 of 24 settings configured
- Locked Screen Experience — 2 of 6 settings configured
- Messaging — 3 settings available
- Microsoft Edge Browser — 7 of 28 settings configured
- Network proxy — 8 settings available
- Password — 6 of 13 settings configured
- Per-app privacy exceptions — 1 setting available
- Personalization — 1 of 1 setting configured
- Printer

Control Panel and Settings
Windows 10 and later

Setting		
Settings app	Block	[✓ Not configured]
System	Block	[✓ Not configured]
Power and sleep settings modification (desktop only)	Block	[✓ Not configured]
Devices	[✓ Block]	Not configured
Network and Internet	Block	[✓ Not configured]
Personalization	Block	[✓ Not configured]
Apps	Block	[✓ Not configured]
Accounts	Block	[✓ Not configured]
Time and Language	Block	[✓ Not configured]
System Time modification	[✓ Block]	Not configured
Region settings modification (desktop only)	Block	[✓ Not configured]
Language settings modification (desktop only)	Block	[✓ Not configured]
Gaming	[✓ Block]	Not configured
Ease of Access	Block	[✓ Not configured]
Privacy	Block	[✓ Not configured]
Update and Security	Block	[✓ Not configured]

8. Configure settings as showed on the screenshot (Windows Sportlight)



Device restrictions
Windows 10 and later

- Password — 6 of 13 settings configured
- Per-app privacy exceptions — 1 setting available
- Personalization — 1 of 1 setting configured
- Printer — 3 settings available
- Privacy — 22 settings available
- Projection — 3 settings available
- Reporting and Telemetry — 1 of 2 settings configured
- Search — 9 settings available
- Start — 28 settings available
- Windows Defender SmartScreen — 3 of 3 settings configured
- Windows Spotlight — 2 of 9 settings configured
- Windows Defender Antivirus — 18 of 34 settings configured

Windows Spotlight
Windows 10 and later

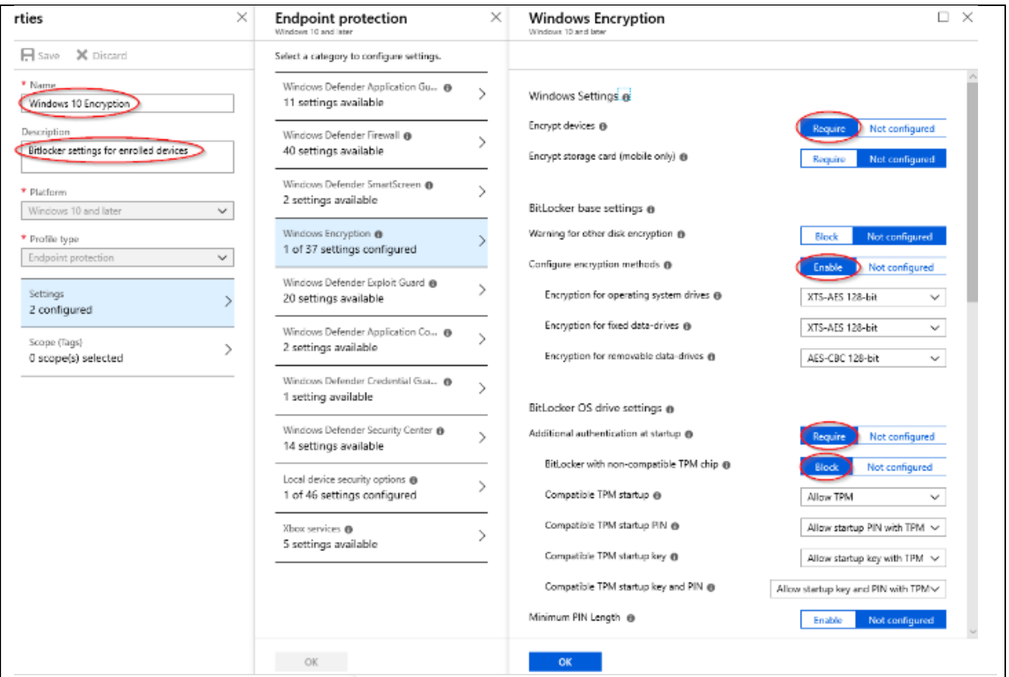
Setting		
Windows Spotlight	Block	[✓ Not configured]
Windows Spotlight on lock screen	[✓ Block]	Not configured
Third-party suggestions in Windows Spotlight	Block	[✓ Not configured]
Consumer Features	[✓ Block]	Not configured
Windows Tips	Block	[✓ Not configured]
Windows Spotlight in action center	Block	[✓ Not configured]
Windows Spotlight personalization	Block	[✓ Not configured]
Windows welcome experience	Block	[✓ Not configured]
Apps suggestions in Ink workspace	Block	[✓ Not configured]

9. Save the Configuration and assign the Configuration to the UG_gebruikers_MDM group	

Exercise 12b: Device Configuration - Windows Device Configuration

We are going to configure Bitlocker.

1. Go to Intune-> Device Configuration->Profiles-> Create Profile
2. Configure as shown on the screen shots



rties

Save | Discard

* Name: Windows 10 Encryption

Description: Bitlocker settings for enrolled devices

* Platform: Windows 10 and later

* Profile type: Endpoint protection

Settings: 2 configured

Scope (Tags): 0 scope(s) selected

Endpoint protection
Windows 10 and later

Select a category to configure settings.

- Windows Defender Application Gu... – 11 settings available
- Windows Defender Firewall – 40 settings available
- Windows Defender SmartScreen – 2 settings available
- Windows Encryption – 1 of 37 settings configured
- Windows Defender Exploit Guard – 20 settings available
- Windows Defender Application Co... – 2 settings available
- Windows Defender Credential Gua... – 1 setting available
- Windows Defender Security Center – 14 settings available
- Local device security options – 1 of 46 settings configured
- Xbox services – 5 settings available

OK

Windows Encryption
Windows 10 and later

Windows Settings

Encrypt devices: [✓ Require] Not configured

Encrypt storage card (mobile only): Require [✓ Not configured]

BitLocker base settings

Warning for other disk encryption: Block [✓ Not configured]

Configure encryption methods: [✓ Enable] Not configured

Encryption for operating system drives: XTS-AES 128-bit

Encryption for fixed data-drives: XTS-AES 128-bit

Encryption for removable data-drives: AES-CBC 128-bit

BitLocker OS drive settings

Additional authentication at startup: [✓ Require] Not configured

BitLocker with non-compatible TPM chip: [✓ Block] Not configured

Compatible TPM startup: Allow TPM

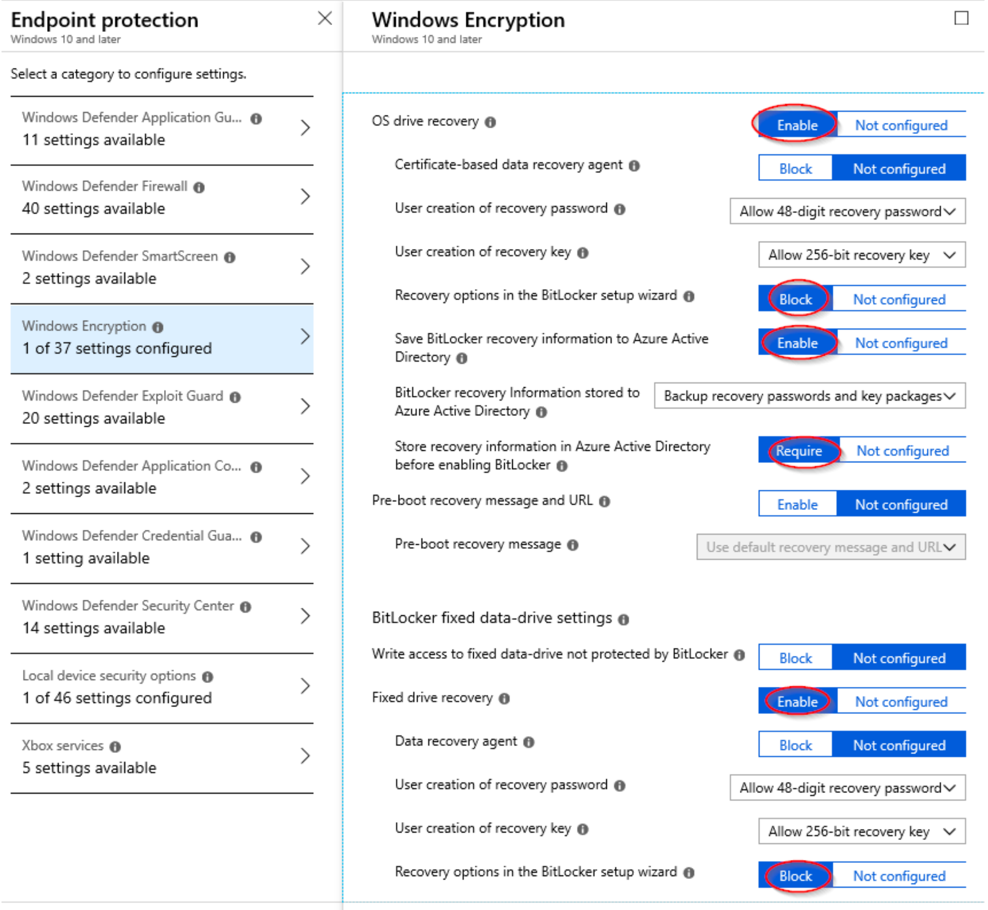
Compatible TPM startup PIN: Allow startup PIN with TPM

Compatible TPM startup key: Allow startup key with TPM

Compatible TPM startup key and PIN: Allow startup key and PIN with TPM

Minimum PIN Length: Enable [✓ Not configured]

OK



Endpoint protection
Windows 10 and later

Select a category to configure settings.

- Windows Defender Application Gu... – 11 settings available
- Windows Defender Firewall – 40 settings available
- Windows Defender SmartScreen – 2 settings available
- Windows Encryption – 1 of 37 settings configured
- Windows Defender Exploit Guard – 20 settings available
- Windows Defender Application Co... – 2 settings available
- Windows Defender Credential Gua... – 1 setting available
- Windows Defender Security Center – 14 settings available
- Local device security options – 1 of 46 settings configured
- Xbox services – 5 settings available

Windows Encryption
Windows 10 and later

OS drive recovery: [✓ Enable] Not configured

Certificate-based data recovery agent: Block [✓ Not configured]

User creation of recovery password: Allow 48-digit recovery password

User creation of recovery key: Allow 256-bit recovery key

Recovery options in the BitLocker setup wizard: [✓ Block] Not configured

Save BitLocker recovery information to Azure Active Directory: [✓ Enable] Not configured

BitLocker recovery Information stored to Azure Active Directory: Backup recovery passwords and key packages

Store recovery information in Azure Active Directory before enabling BitLocker: [✓ Require] Not configured

Pre-boot recovery message and URL: Enable [✓ Not configured]

Pre-boot recovery message: Use default recovery message and URL

BitLocker fixed data-drive settings

Write access to fixed data-drive not protected by BitLocker: Block [✓ Not configured]

Fixed drive recovery: [✓ Enable] Not configured

Data recovery agent: Block [✓ Not configured]

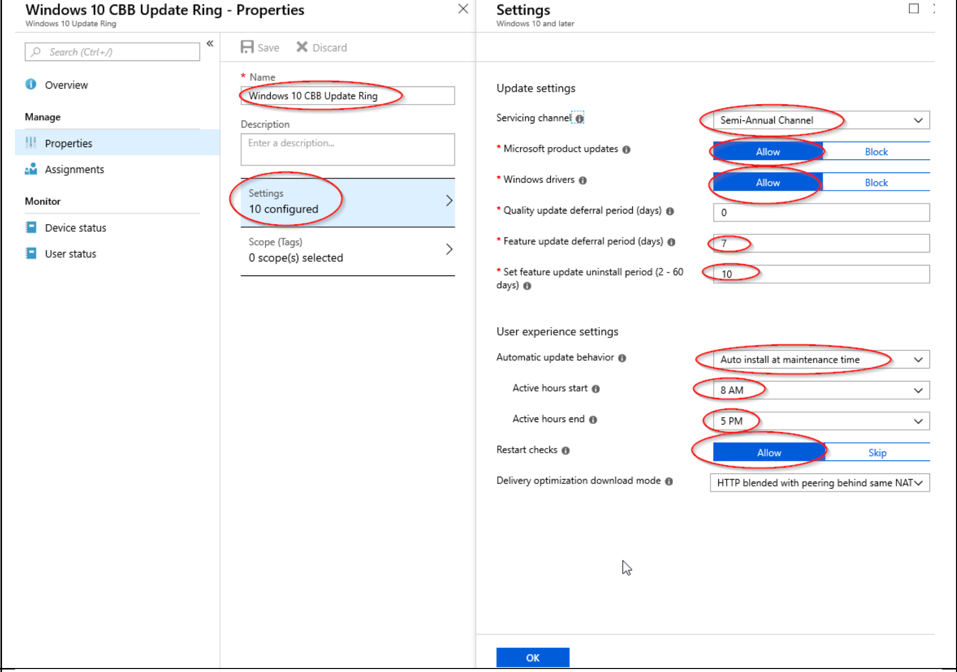
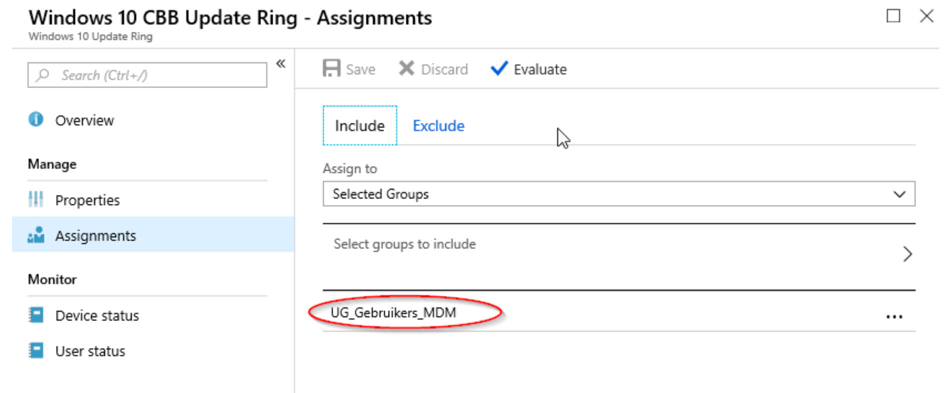
User creation of recovery password: Allow 48-digit recovery password

User creation of recovery key: Allow 256-bit recovery key

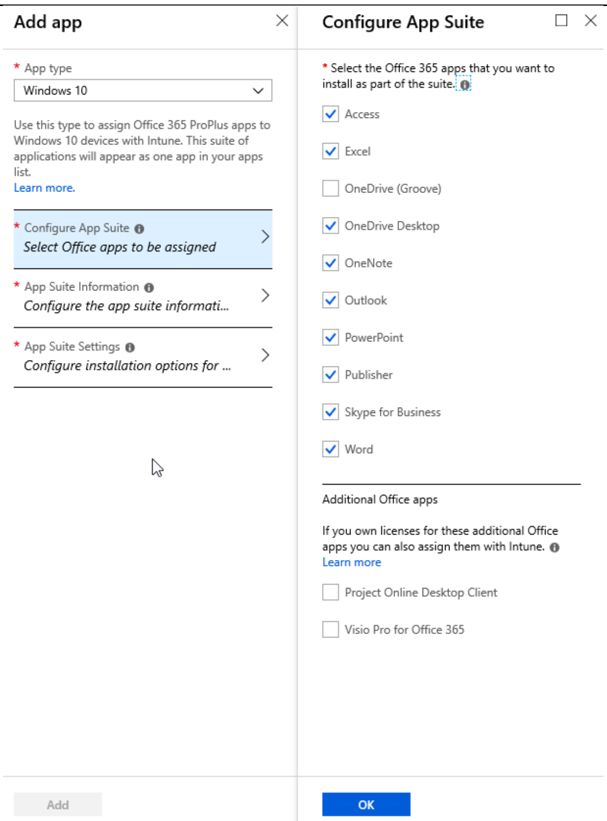
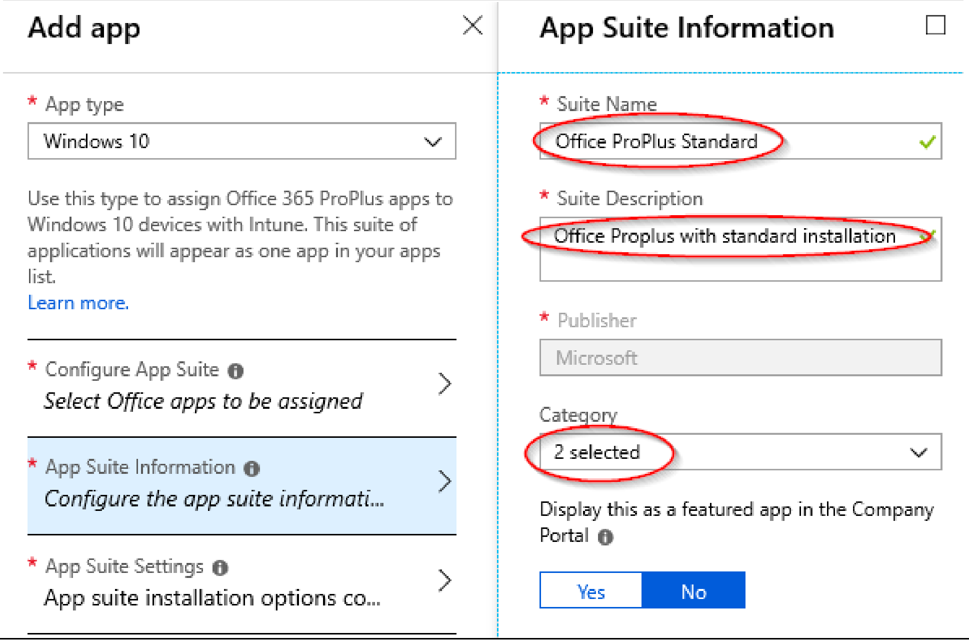
Recovery options in the BitLocker setup wizard: [✓ Block] Not configured

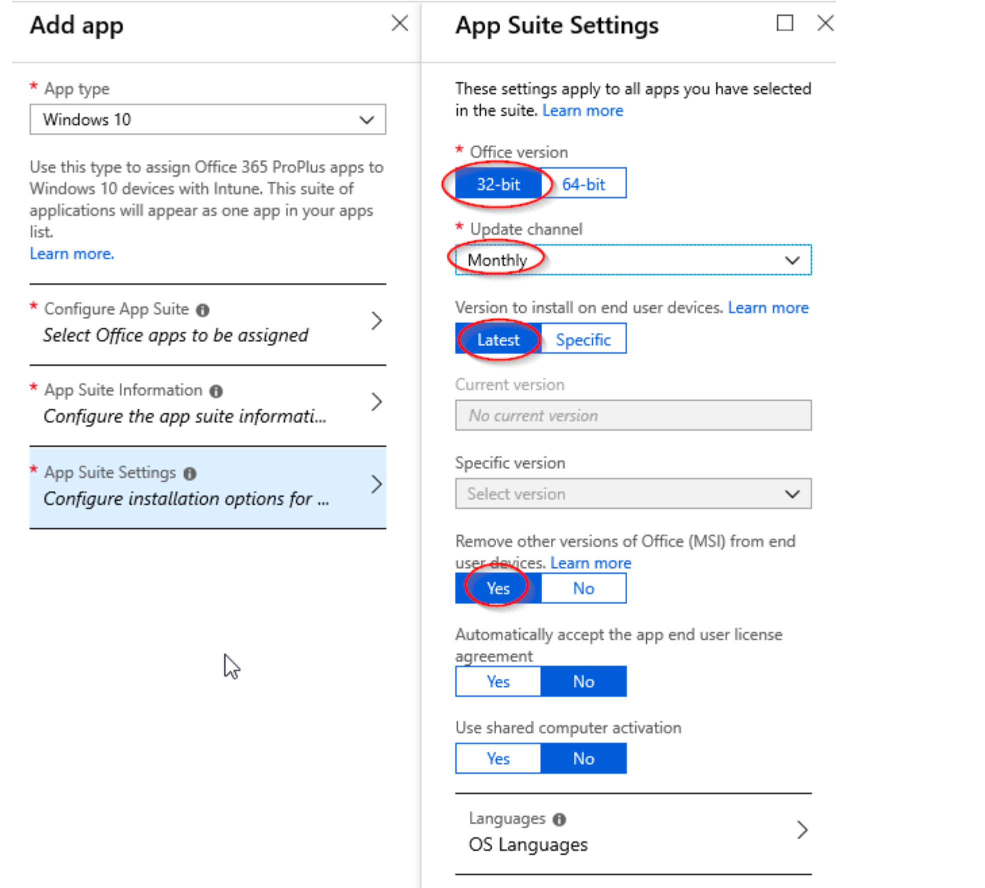
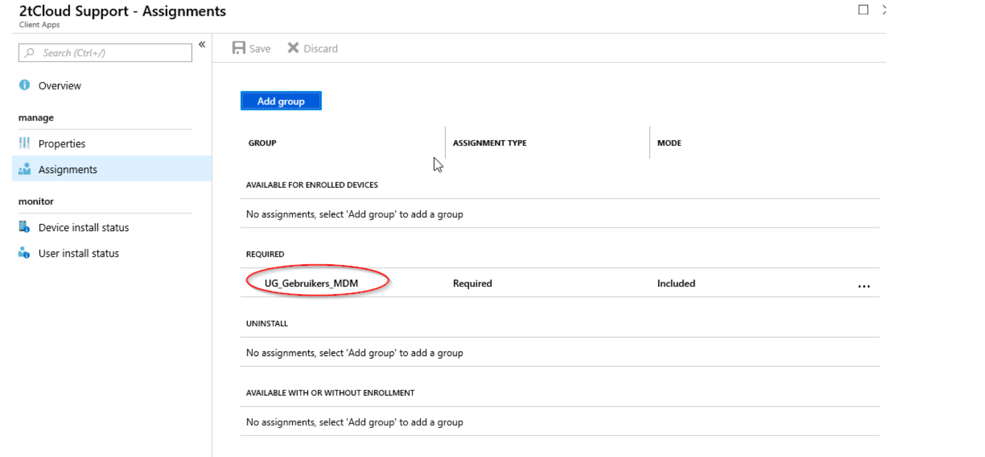
3. Save the Configuration and assign the Configuration to the UG_gebruikers_MDM group	

Exercise 12: Windows 10 Update Rings

1. Go to **Intune -> Software Updates -> Windows 10 Update Rings** 2. Click "Create" 3. Configure the settings -> Click **Settings** 4. Configure settings as showed on the screenshot	 Windows 10 CBB Update Ring - Properties Name: Windows 10 CBB Update Ring Description: Enter a description... Settings: 10 configured Scope (Tags): 0 scope(s) selected Settings Windows 10 and later Update settings Servicing channel: Semi-Annual Channel * Microsoft product updates: Allow * Windows drivers: Allow * Quality update deferral period (days): 0 * Feature update deferral period (days): 7 * Set feature update uninstall period (2 - 60 days): 10 User experience settings Automatic update behavior: Auto install at maintenance time Active hours start: 8 AM Active hours end: 5 PM Restart checks: Allow Delivery optimization download mode: HTTP blended with peering behind same NAT Windows 10 Update Ring Search (Ctrl+/) Overview Manage Properties Assignments Monitor Device status User status Save Discard Block Skip OK
5. Assign the Windows 10 Update Ring to Group "UG_Gebruikers_MDM"	 Windows 10 CBB Update Ring - Assignments Include Assign to: Selected Groups Select groups to include UG_Gebruikers_MDM Windows 10 Update Ring Search (Ctrl+/) Overview Manage Properties Assignments Monitor Device status User status Save Discard Evaluate Exclude

Exercise 13: Office ProPlus Deployment via Intune

1. Go to **Microsoft Intune -> Client Apps –> Apps**	
2. Add a App with App type "Windows 10" 3. Configure the settings 4. Assign App to group	 Add app * App type Windows 10 Use this type to assign Office 365 ProPlus apps to Windows 10 devices with Intune. This suite of applications will appear as one app in your apps list. Learn more. * Configure App Suite *Select Office apps to be assigned* * App Suite Information *Configure the app suite informati...* * App Suite Settings *Configure installation options for ...* Add Configure App Suite * Select the Office 365 apps that you want to install as part of the suite. ☑ Access ☑ Excel ☐ OneDrive (Groove) ☑ OneDrive Desktop ☑ OneNote ☑ Outlook ☑ PowerPoint ☑ Publisher ☑ Skype for Business ☑ Word Additional Office apps If you own licenses for these additional Office apps you can also assign them with Intune. Learn more ☐ Project Online Desktop Client ☐ Visio Pro for Office 365 OK  Add app * App type Windows 10 Use this type to assign Office 365 ProPlus apps to Windows 10 devices with Intune. This suite of applications will appear as one app in your apps list. Learn more. * Configure App Suite *Select Office apps to be assigned* * App Suite Information *Configure the app suite informati...* * App Suite Settings App suite installation options co... App Suite Information * Suite Name Office ProPlus Standard * Suite Description Office Proplus with standard installation * Publisher Microsoft Category 2 selected Display this as a featured app in the Company Portal Yes [✓ No]

	
5. Assign the app to MDM users	

Add app

* App type

Windows 10

Use this type to assign Office 365 ProPlus apps to Windows 10 devices with Intune. This suite of applications will appear as one app in your apps list.

Learn more.

* Configure App Suite

Select Office apps to be assigned

* App Suite Information

Configure the app suite informati...

* App Suite Settings

Configure installation options for ...

App Suite Settings

These settings apply to all apps you have selected in the suite. Learn more

* Office version

[✓ 32-bit] 64-bit

* Update channel

[✓ Monthly]

Version to install on end user devices. Learn more

[✓ Latest] Specific

Current version

No current version

Specific version

Select version

Remove other versions of Office (MSI) from end user devices. Learn more

[✓ Yes] No

Automatically accept the app end user license agreement

Yes [✓ No]

Use shared computer activation

Yes [✓ No]

Languages

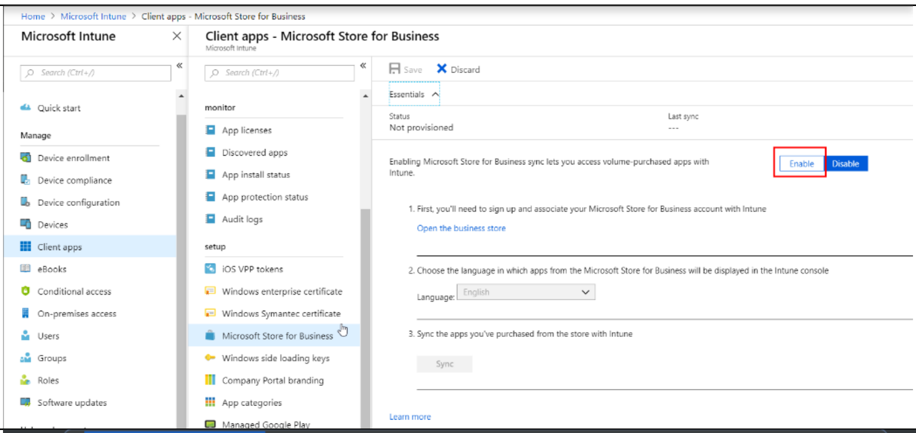
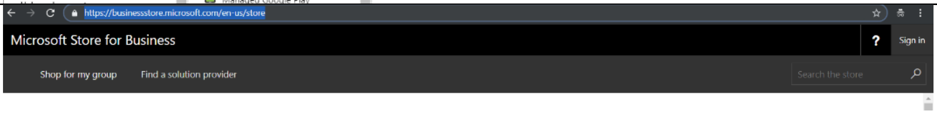
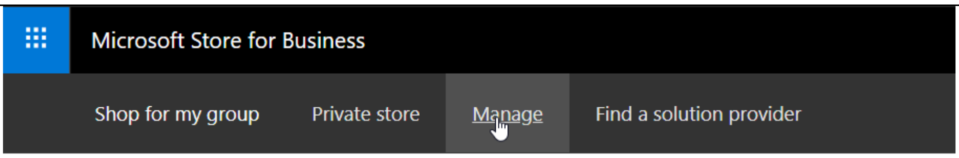
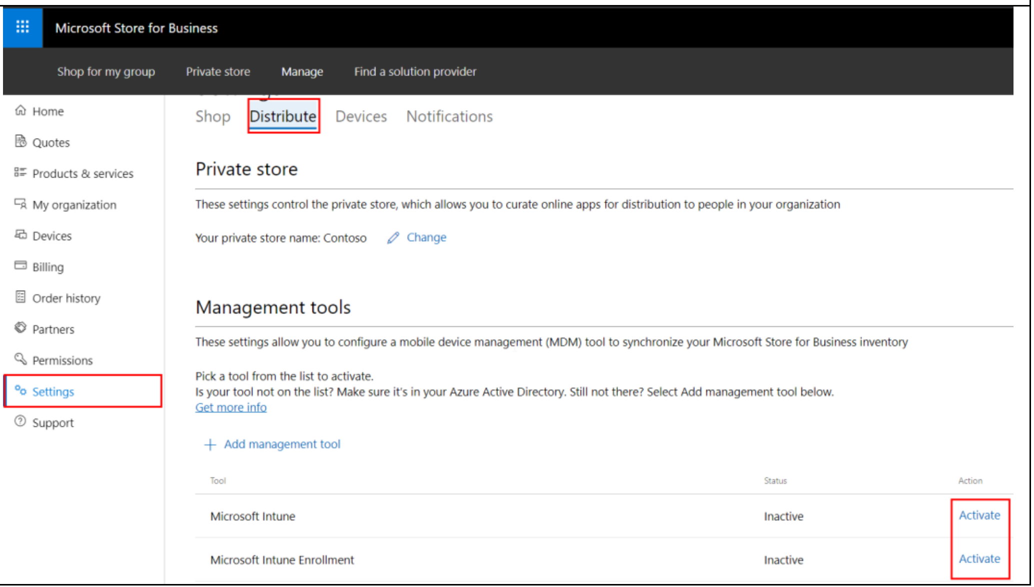
OS Languages

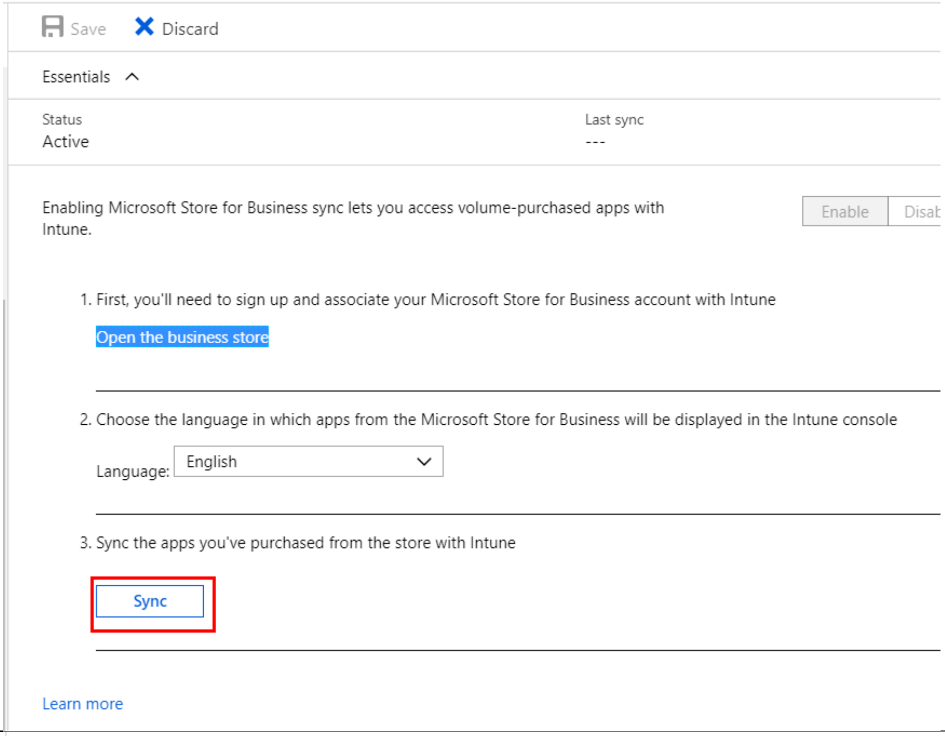
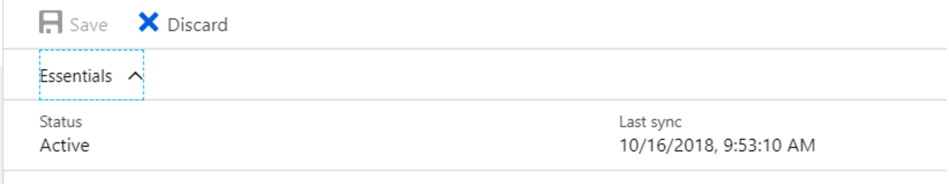
2tCloud Support - Assignments

Client Apps

GROUP	ASSIGNMENT TYPE	MODE
AVAILABLE FOR ENROLLED DEVICES		
No assignments, select 'Add group' to add a group		
REQUIRED		
UG_Gebruikers_MDM	Required	Included
UNINSTALL		
No assignments, select 'Add group' to add a group		
AVAILABLE WITH OR WITHOUT ENROLLMENT		
No assignments, select 'Add group' to add a group		

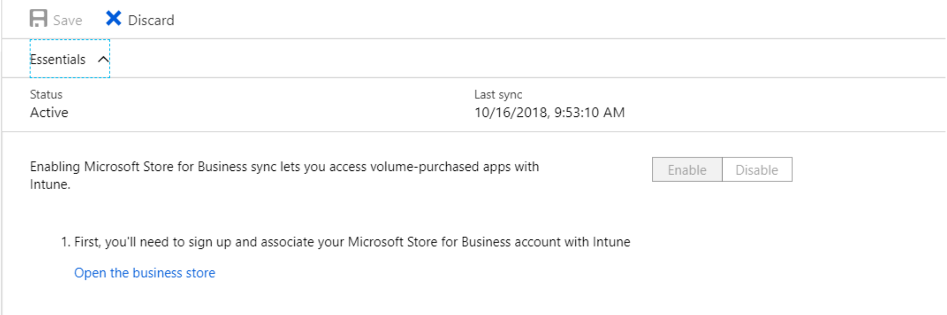
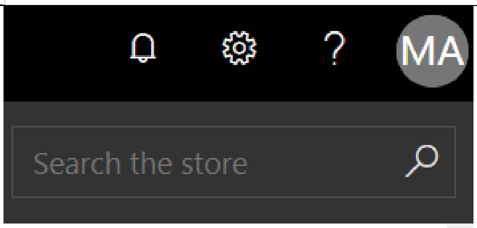
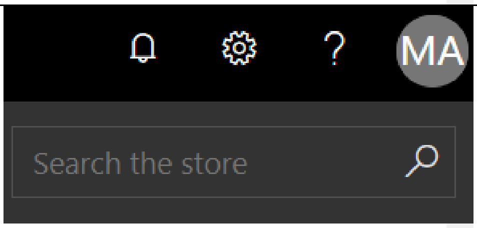
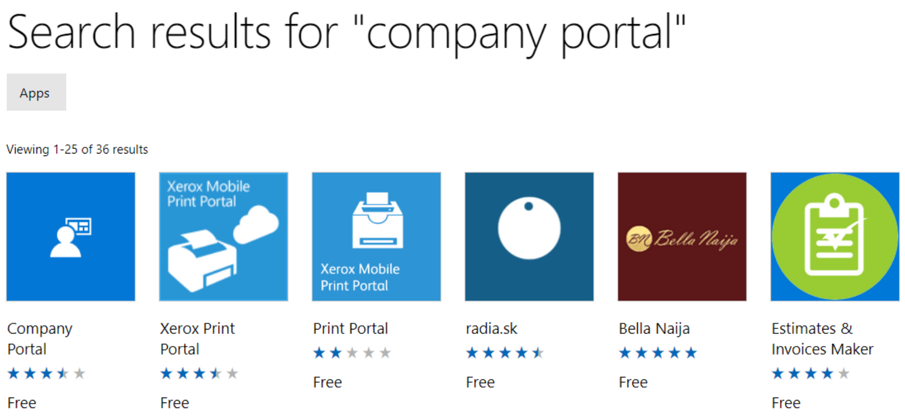
Exercise 14: Windows Store for Business

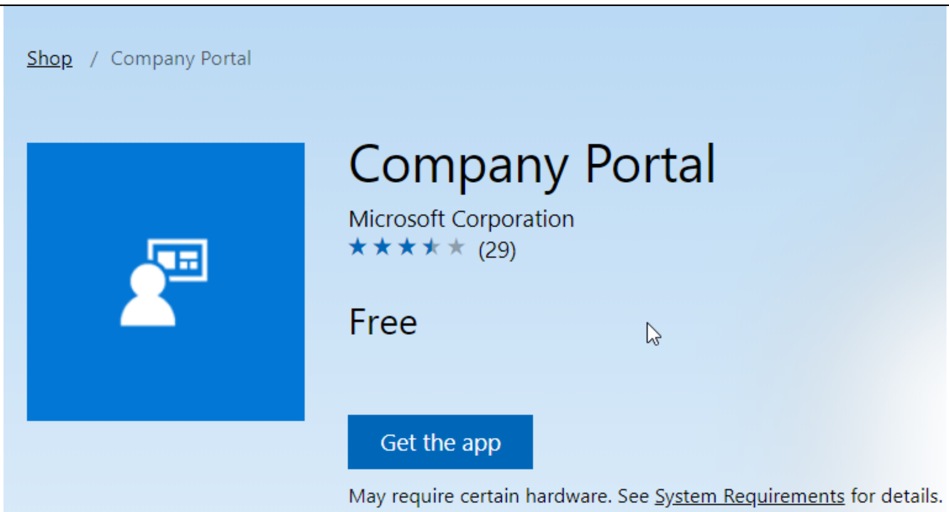
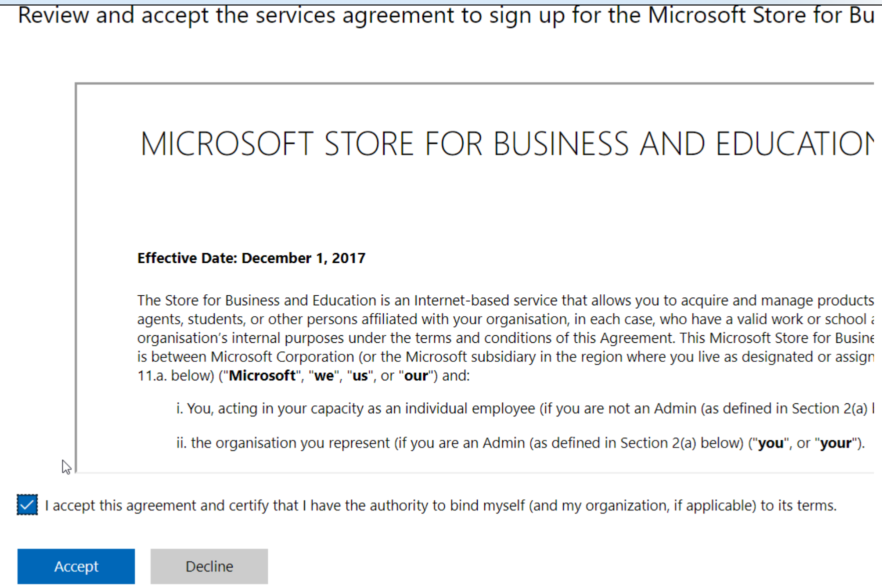
Go to Microsoft Intune → Client Apps → Microsoft store for Business 1. There you select Enable and press Save	 Home > Microsoft Intune > Client apps - Microsoft Store for Business Microsoft Intune Search (Ctrl+/) Quick start Manage Device enrollment Device compliance Device configuration Devices Client apps eBooks Conditional access On-premises access Users Groups Roles Software updates Client apps - Microsoft Store for Business Microsoft Intune Search (Ctrl+/) monitor App licenses Discovered apps App install status App protection status Audit logs setup iOS VPP tokens Windows enterprise certificate Windows Symantec certificate Microsoft Store for Business Windows side loading keys Company Portal branding App categories Managed Google Play Save Discard Essentials Enable Disable Open the business store Sync Learn more Status: Not provisioned Last sync: --- Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. 1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune 2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console Language: English 3. Sync the apps you've purchased from the store with Intune
2. After that you can select the link open Open the business store 3. Sign in with your AAD account	 https://businessstore.microsoft.com/en-us/store Microsoft Store for Business ? Sign in Shop for my group Find a solution provider Search the store
4. Once your signed in select manage 5. Accept any terms and license agreements	 Microsoft Store for Business Shop for my group Private store Manage Find a solution provider
Go to settings → Distribute 6. Activate Microsoft Intune and Microsoft Intune Enrollment	 Microsoft Store for Business Shop for my group Private store Manage Find a solution provider Home Quotes Products & services My organization Devices Billing Order history Partners Permissions Settings Support Shop Distribute Devices Notifications Private store These settings control the private store, which allows you to curate online apps for distribution to people in your organization Your private store name: Contoso Change Management tools These settings allow you to configure a mobile device management (MDM) tool to synchronize your Microsoft Store for Business inventory Pick a tool from the list to activate. Is your tool not on the list? Make sure it's in your Azure Active Directory. Still not there? Select Add management tool below. Get more info + Add management tool Tool / Status / Action Microsoft Intune / Inactive / Activate Microsoft Intune Enrollment / Inactive / Activate

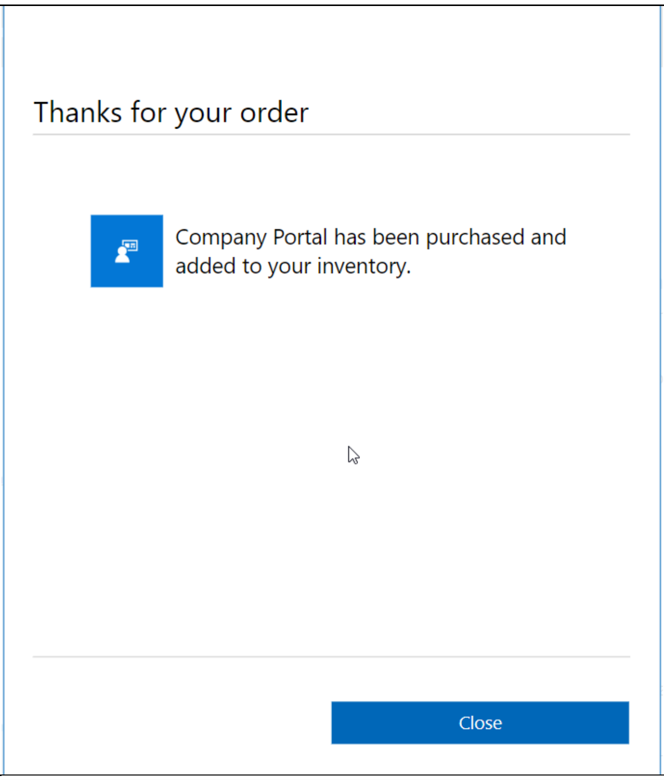
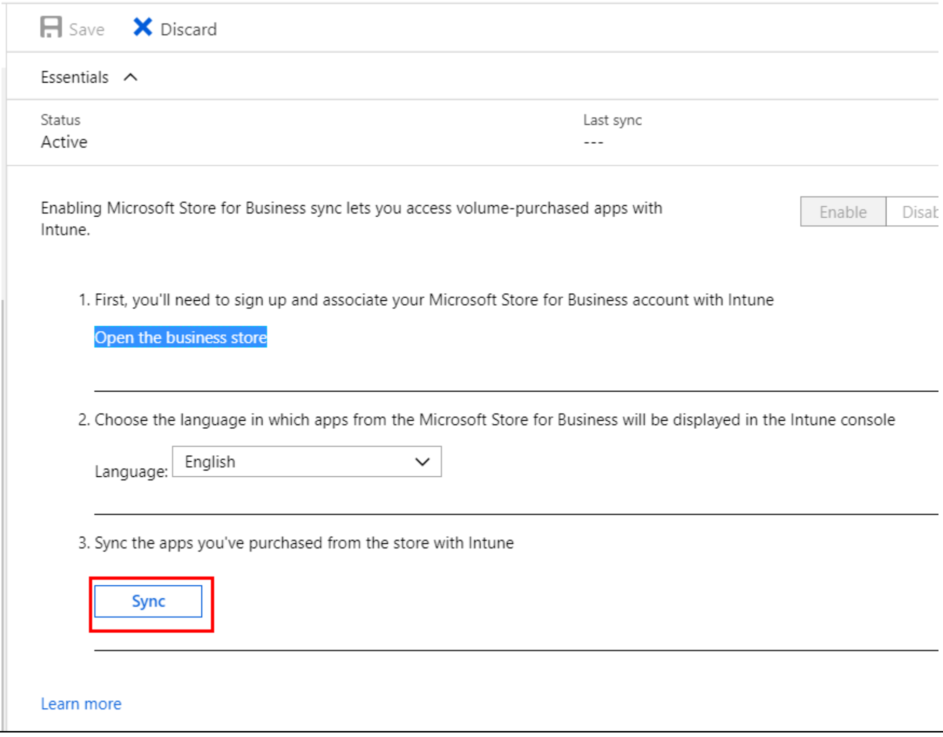
7. Go back to the Intune Portal and Select Sync	 Status: Active Last sync: --- Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. 1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune Open the business store 2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console Language: English 3. Sync the apps you've purchased from the store with Intune Learn more
8. The syncing process can take a while. But when completed you should see the last time it was successfully synced	 Status: Active Last sync: 10/16/2018, 9:53:10 AM
9. At this point you can deploy apps from the Windows Store for Business	

Exercise 15: Company portal

We are now going to use the Windows Store for Business to deploy an application.

Go to Microsoft Intune → Client Apps → Microsoft store for Business 1. Select open the business store	 Save Discard Essentials Status: Active Last sync: 10/16/2018, 9:53:10 AM Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. Enable Disable 1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune Open the business store
2. Check if you are signed in. If not sign in with your account	
3. Use the search bar to search for company portal (bedrijfs portaal)	
4. Select Company Portal	 Search results for "company portal" Apps Viewing 1-25 of 36 results Company Portal ★★★★☆ Free Xerox Print Portal ★★★★☆ Free Print Portal ★★☆☆☆ Free radia.sk ★★★★★ Free Bella Naija ★★★★★ Free Estimates & Invoices Maker ★★★★☆ Free Xerox Mobile Print Portal Xerox Mobile Print Portal Bella Naija

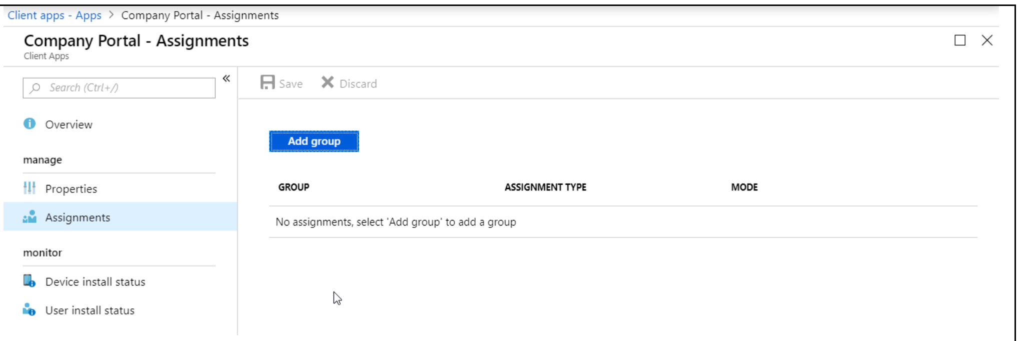
5. Select Get the app	 Shop / Company Portal Company Portal Microsoft Corporation ★★★★☆ (29) Free Get the app May require certain hardware. See System Requirements for details.
6. Accept the agreement	 Review and accept the services agreement to sign up for the Microsoft Store for Bu MICROSOFT STORE FOR BUSINESS AND EDUCATION **Effective Date: December 1, 2017** The Store for Business and Education is an Internet-based service that allows you to acquire and manage products agents, students, or other persons affiliated with your organisation, in each case, who have a valid work or school a organisation's internal purposes under the terms and conditions of this Agreement. This Microsoft Store for Busine is between Microsoft Corporation (or the Microsoft subsidiary in the region where you live as designated or assign 11.a. below) ("**Microsoft**", "**we**", "**us**", or "**our**") and: i. You, acting in your capacity as an individual employee (if you are not an Admin (as defined in Section 2(a) I ii. the organisation you represent (if you are an Admin (as defined in Section 2(a) below) ("**you**", or "**your**"). ☑ I accept this agreement and certify that I have the authority to bind myself (and my organization, if applicable) to its terms. Accept Decline

7. After that the app is added	 Thanks for your order Company Portal has been purchased and added to your inventory.
8. Go back to the Intune Portal and Select Sync	 Status: Active Last sync: --- Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. 1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune Open the business store 2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console Language: English 3. Sync the apps you've purchased from the store with Intune Learn more

After the sync is completed go to Microsoft Intune → Client apps – Apps

There you should find The company portal. Note that the Type is Microsoft Store for Business app

9. Select Company Portal and click on Assignments



Client apps - Apps > Company Portal - Assignments

Company Portal - Assignments
Client Apps

Search (Ctrl+/)

Overview

manage

Properties

Assignments

monitor

Device install status

User install status

Save Discard

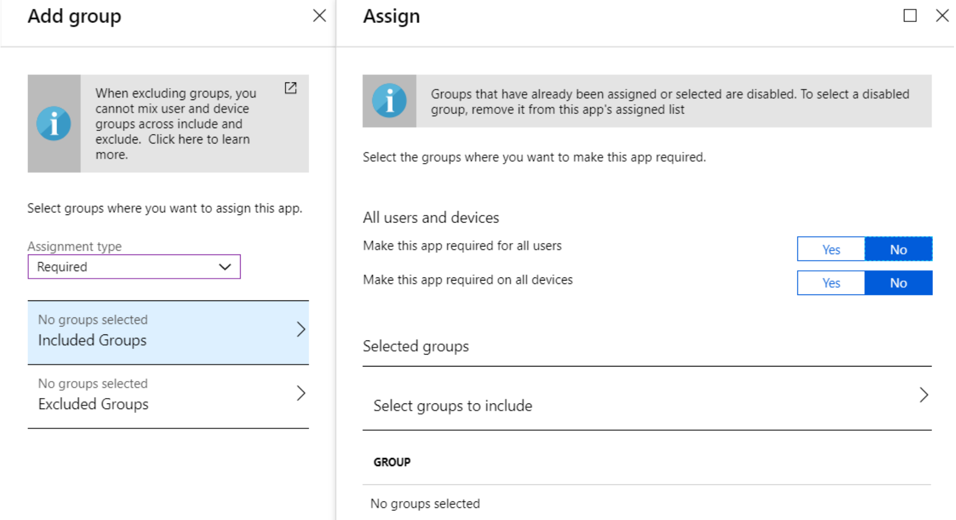
Add group

GROUP	ASSIGNMENT TYPE	MODE
No assignments, select 'Add group' to add a group		

10. Select Add group

11. On Assignment Type choose required

12. Then select group and select the MDM group that you have created.



Add group

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Assignment type: Required

No groups selected
Included Groups

No groups selected
Excluded Groups

Assign

Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list

Select the groups where you want to make this app required.

All users and devices

Make this app required for all users: Yes [✓ No]

Make this app required on all devices: Yes [✓ No]

Selected groups

Select groups to include

GROUP

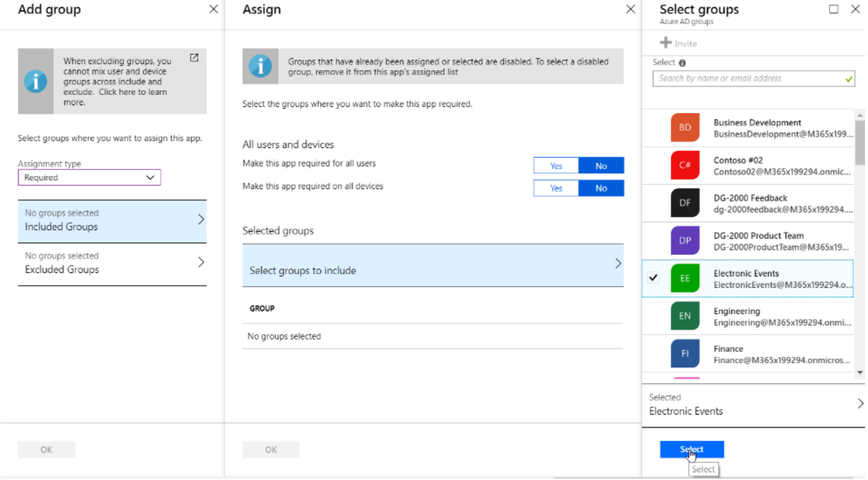
No groups selected

13. Then select group and select the MDM group that you have created.

14. Then click OK

15. Then Click OK again

16. Click Save



Add group

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Assignment type: Required

No groups selected
Included Groups

No groups selected
Excluded Groups

OK

Assign

Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list

Select the groups where you want to make this app required.

All users and devices

Make this app required for all users: Yes [✓ No]

Make this app required on all devices: Yes [✓ No]

Selected groups

Select groups to include

GROUP

No groups selected

OK

Select groups
Azure AD groups

Invite

Select

Search by name or email address

BD Business Development
BusinessDevelopment@M365x199...

C# Contoso #02
Contoso02@M365x199294.onmic...

DF DG-2000 Feedback
dg-2000feedback@M365x199294....

DP DG-2000 Product Team
DG-2000ProductTeam@M365x19...

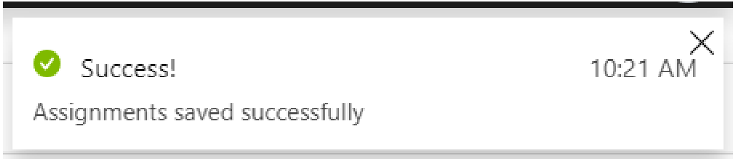
✓ EE Electronic Events
ElectronicEvents@M365x199294.o...

EN Engineering
Engineering@M365x199294.onmi...

FI Finance
Finance@M365x199294.onmicros...

Selected
Electronic Events

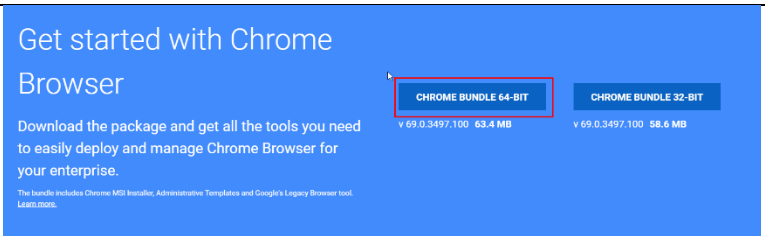
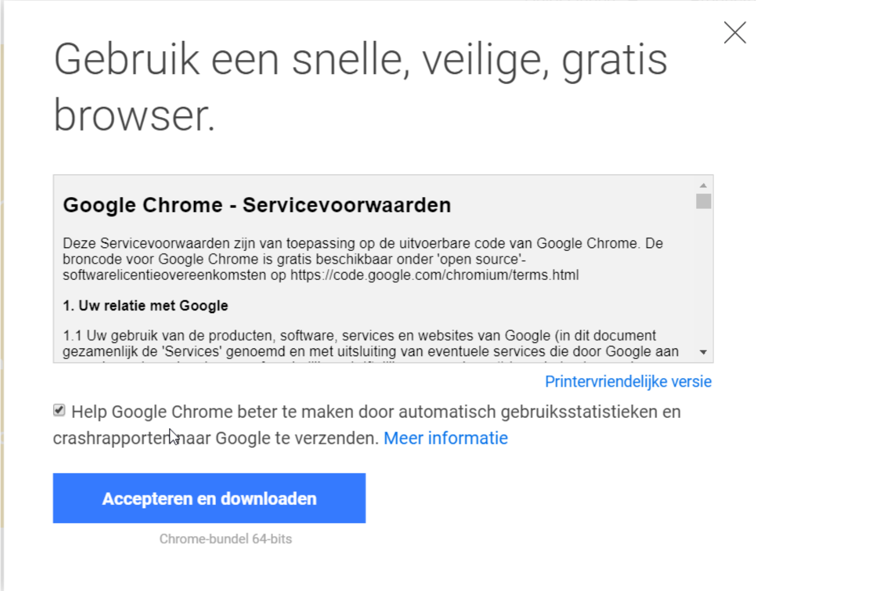
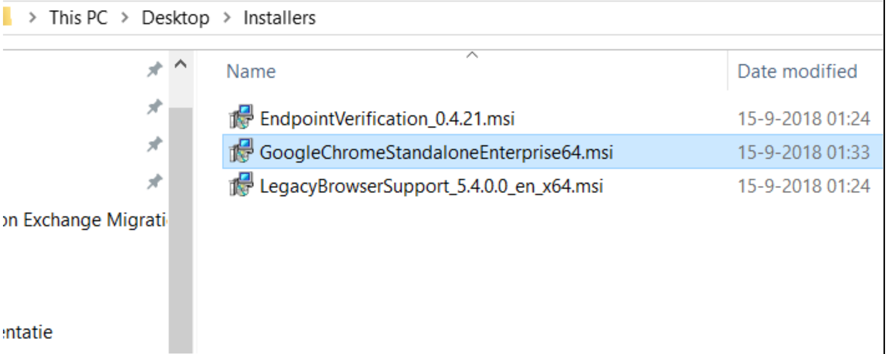
Select

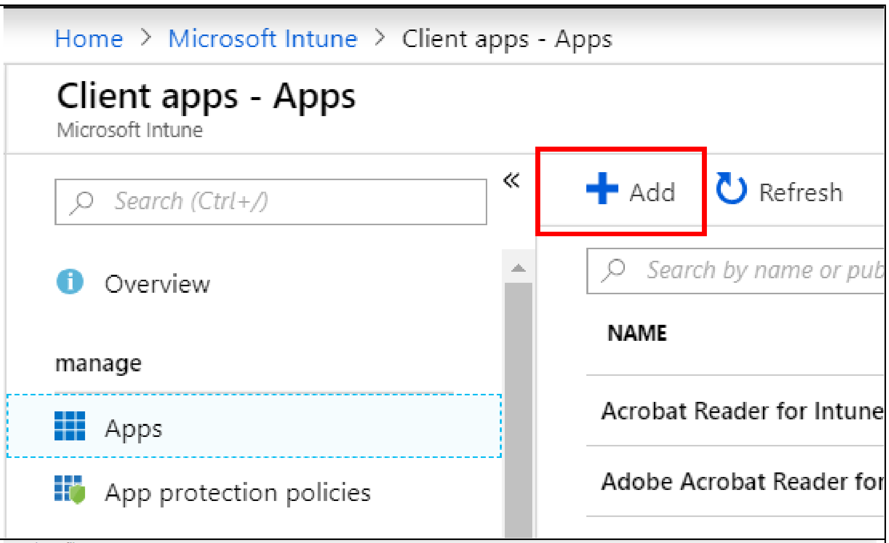
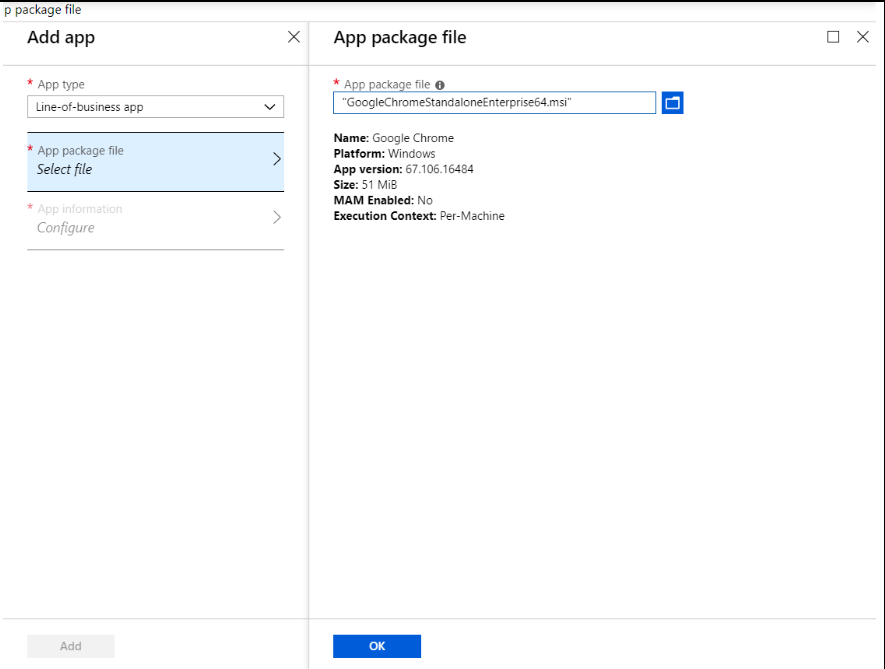


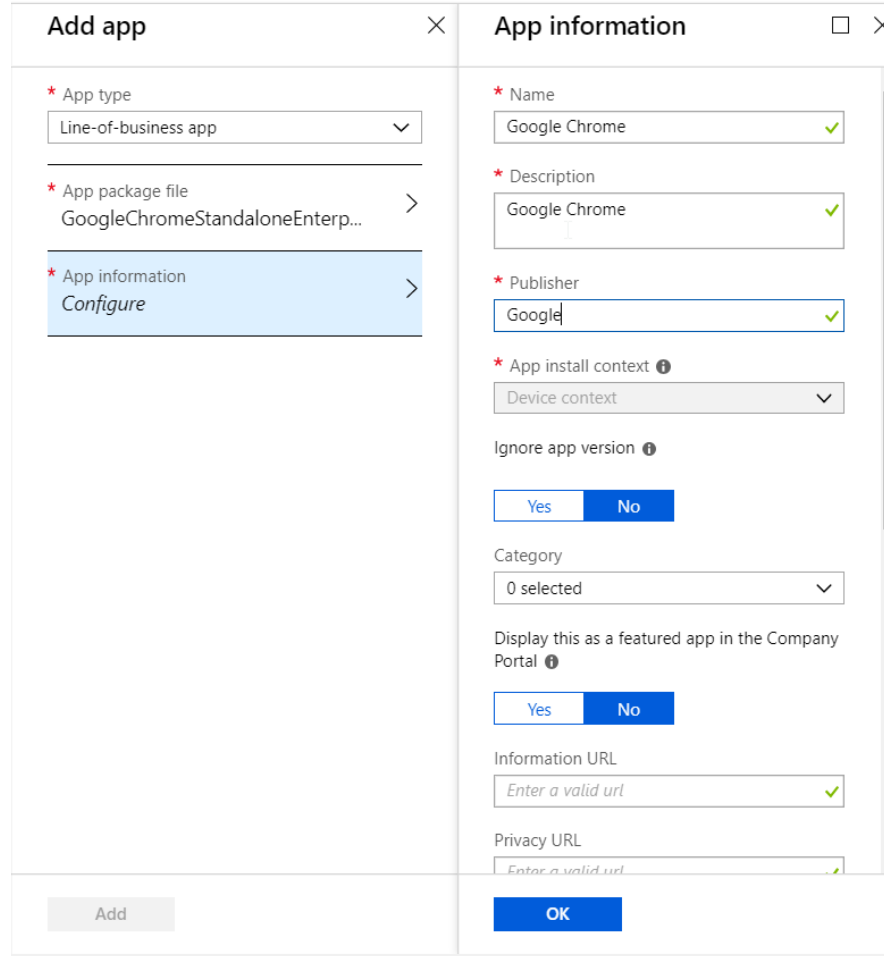
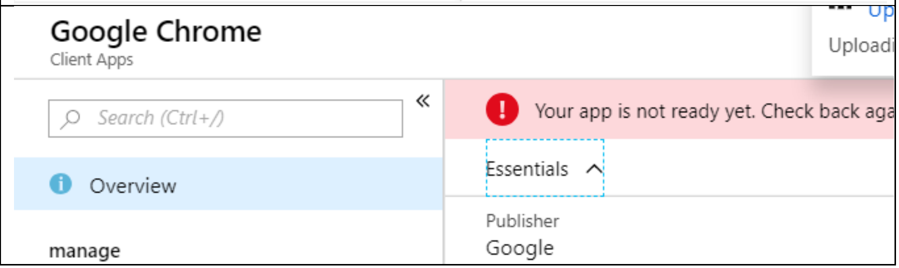
Success! 10:21 AM

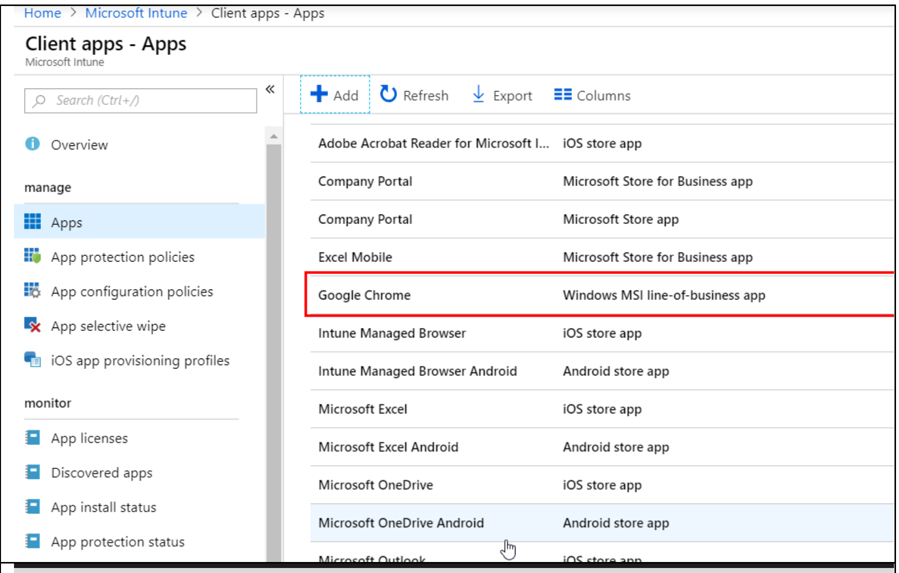
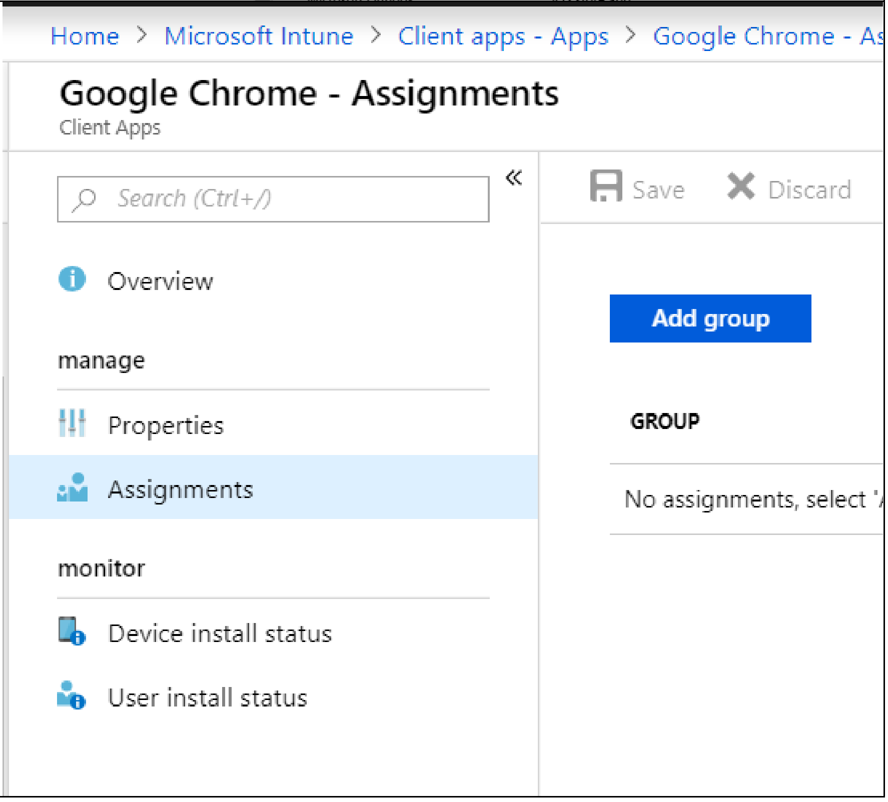
Assignments saved successfully

Exercise 16: MSI app deployment

Go to https://enterprise.google.com/chrome/chrome-browser/ 1. Search the page for Chrome Bundle 64-bit	 Get started with Chrome Browser Download the package and get all the tools you need to easily deploy and manage Chrome Browser for your enterprise. The bundle includes Chrome MSI Installer, Administrative Templates and Google's Legacy Browser tool. Learn more. CHROME BUNDLE 64-BIT v 69.0.3497.100 63.4 MB CHROME BUNDLE 32-BIT v 69.0.3497.100 58.6 MB
2. Accept and download the MSI	 Gebruik een snelle, veilige, gratis browser. **Google Chrome - Servicevoorwaarden** Deze Servicevoorwaarden zijn van toepassing op de uitvoerbare code van Google Chrome. De broncode voor Google Chrome is gratis beschikbaar onder 'open source'-softwarelicentieovereenkomsten op https://code.google.com/chromium/terms.html **1. Uw relatie met Google** 1.1 Uw gebruik van de producten, software, services en websites van Google (in dit document gezamenlijk de 'Services' genoemd en met uitsluiting van eventuele services die door Google aan Printervriendelijke versie ☑ Help Google Chrome beter te maken door automatisch gebruiksstatistieken en crashrapporten naar Google te verzenden. Meer informatie
3. This will download a zip file 4. Extract the files to your desktop 5. There you can find the GoogleChromeStandAloneEnterprise64.msi Desktop\Installers\GoogleChromeStandaloneEnterprise64.msi	 > This PC > Desktop > Installers Name — Date modified EndpointVerification_0.4.21.msi — 15-9-2018 01:24 GoogleChromeStandaloneEnterprise64.msi — 15-9-2018 01:33 LegacyBrowserSupport_5.4.0.0_en_x64.msi — 15-9-2018 01:24

Go to portal.office.com Choose Microsoft Intune → Client Apps → Apps 1. Select Add	 Home > Microsoft Intune > Client apps - Apps Client apps - Apps Microsoft Intune Search (Ctrl+/) Add Refresh Search by name or pub Overview manage Apps App protection policies NAME Acrobat Reader for Intune Adobe Acrobat Reader for
2. At App Type choos Line-of-business app 3. At App package file select GoogleChromeStandaloneEnterprise64.msi from your desktop and click OK	 * App type Line-of-business app * App package file Select file * App information Configure * App package file "GoogleChromeStandaloneEnterprise64.msi" **Name:** Google Chrome **Platform:** Windows **App version:** 67.106.16484 **Size:** 51 MiB **MAM Enabled:** No **Execution Context:** Per-Machine

4. Select App information 5. Enter a Description 6. Enter a Publisher 7. Select OK 8. Select ADD	 Add app * App type: Line-of-business app * App package file: GoogleChromeStandaloneEnterp... * App information: *Configure* Add App information * Name: Google Chrome * Description: Google Chrome * Publisher: Google * App install context: Device context Ignore app version: Yes [✓ No] Category: 0 selected Display this as a featured app in the Company Portal: Yes [✓ No] Information URL: *Enter a valid url* Privacy URL: *Enter a valid url* OK
9. Wait for the app to finish uploading	 Google Chrome Client Apps *Search (Ctrl+/)* Overview manage Your app is not ready yet. Check back aga Essentials Publisher: Google Up Uploadi

10. After Chrome is reader you need to select the app	
11. Select Assignments and add group	

Adobe Acrobat Reader for Microsoft I...	iOS store app
Company Portal	Microsoft Store for Business app
Company Portal	Microsoft Store app
Excel Mobile	Microsoft Store for Business app
Google Chrome	Windows MSI line-of-business app
Intune Managed Browser	iOS store app
Intune Managed Browser Android	Android store app
Microsoft Excel	iOS store app
Microsoft Excel Android	Android store app
Microsoft OneDrive	iOS store app
Microsoft OneDrive Android	Android store app
Microsoft Outlook	iOS store app

No assignments, select '

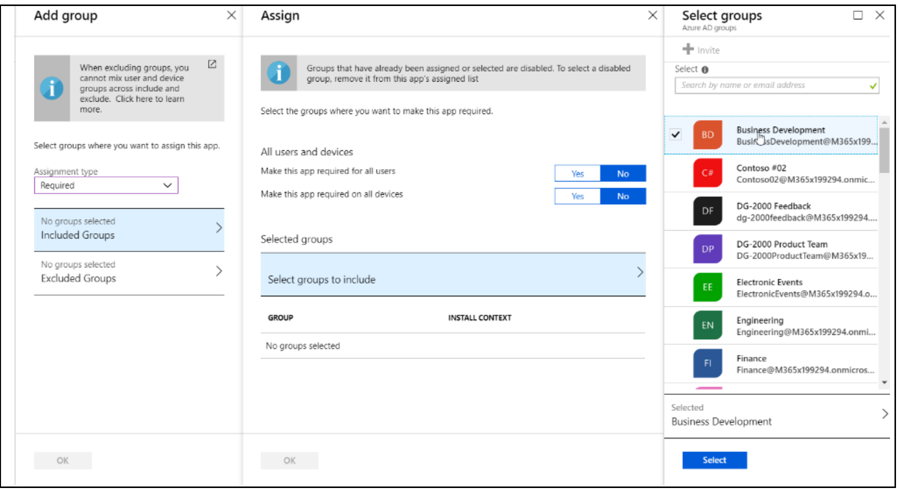
12. At assignment type choose Required

13. Select the group you created and choose Select

14. Choose OK

15. And OK again

16. Finally press Save



Add group

When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more.

Select groups where you want to assign this app.

Assignment type: Required

No groups selected
Included Groups

No groups selected
Excluded Groups

OK

Assign

Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list

Select the groups where you want to make this app required.

All users and devices

Make this app required for all users: Yes [✓ No]

Make this app required on all devices: Yes [✓ No]

Selected groups

Select groups to include

GROUP	INSTALL CONTEXT
No groups selected	

OK

Select groups
Azure AD groups

Invite

Select: Search by name or email address

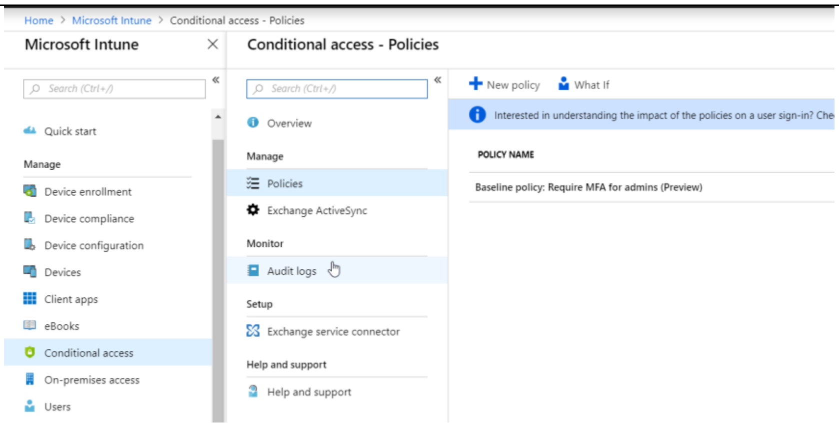
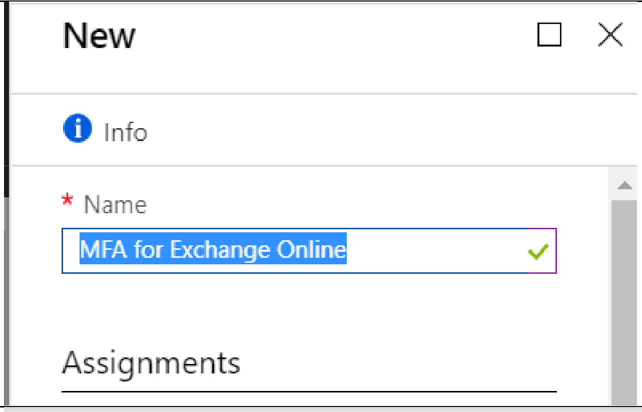
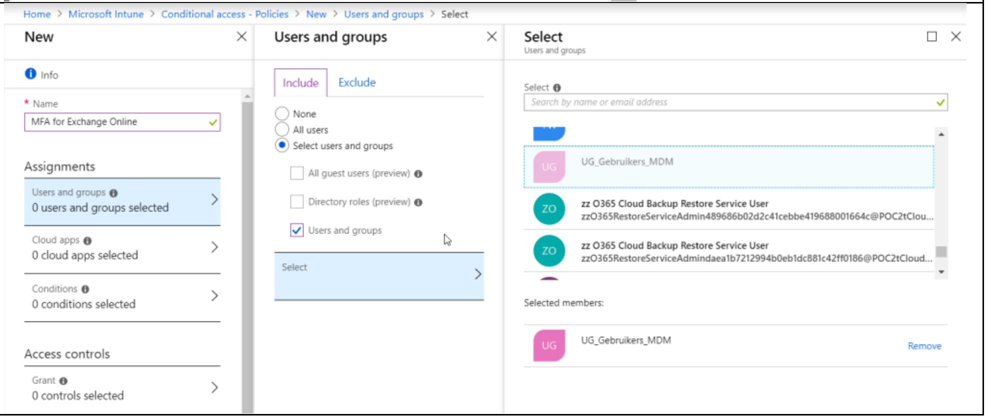
✓	BD	Business Development BusinessDevelopment@M365x199...
	C#	Contoso #02 Contoso02@M365x199294.onmic...
	DF	DG-2000 Feedback dg-2000feedback@M365x199294....
	DP	DG-2000 Product Team DG-2000ProductTeam@M365x19...
	EE	Electronic Events ElectronicEvents@M365x199294.o...
	EN	Engineering Engineering@M365x199294.onmi...
	FI	Finance Finance@M365x199294.onmicros...

Selected
Business Development

Select

Exercise 17: Conditional Access

Conditional Access is a great way to secure your environment. You can use Intune to make sure that your device is complaint, otherwise the user cannot access the company resources. Now you have created a compliance policy you want to assign actions to that policy.

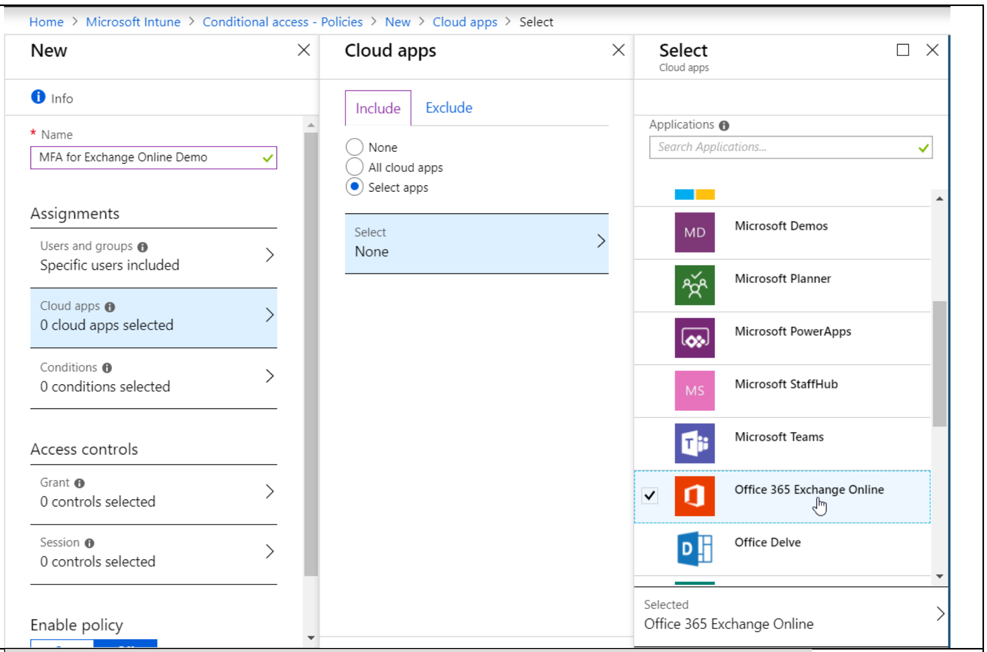
1. Go to Microsoft Intune → Conditional access and select New Policy	 Home > Microsoft Intune > Conditional access - Policies Microsoft Intune Quick start Manage Device enrollment Device compliance Device configuration Devices Client apps eBooks Conditional access On-premises access Users Conditional access - Policies Overview Manage Policies Exchange ActiveSync Monitor Audit logs Setup Exchange service connector Help and support Help and support New policy What If Interested in understanding the impact of the policies on a user sign-in? Che POLICY NAME Baseline policy: Require MFA for admins (Preview)
2. Give the policy a name: MFA for Exchange Online	 New Info * Name MFA for Exchange Online Assignments
3. Select Users and groups 4. Select: Select users and Groups 5. Check Users and groups 6. Select the group “UG_Gebruikers_MDM”	 Home > Microsoft Intune > Conditional access - Policies > New > Users and groups > Select New Info * Name MFA for Exchange Online Assignments Users and groups: 0 users and groups selected Cloud apps: 0 cloud apps selected Conditions: 0 conditions selected Access controls Grant: 0 controls selected Users and groups Include / Exclude ○ None ○ All users ● Select users and groups □ All guest users (preview) □ Directory roles (preview) ☑ Users and groups Select Select Users and groups Select Search by name or email address UG_Gebruikers_MDM zz O365 Cloud Backup Restore Service User zzO365RestoreServiceAdmin489686b02d2c41cebbe419688001664c@POC2tClou... zz O365 Cloud Backup Restore Service User zzO365RestoreServiceAdmindaea1b7212994b0eb1dc881c42ff0186@POC2tCloud... Selected members: UG_Gebruikers_MDM Remove

7. Select Cloud apps

8. Check Selects apps

9. From the select menu find and check Office 365 Exchange Online

10. Choose Done



Home > Microsoft Intune > Conditional access - Policies > New > Cloud apps > Select

New

Info

* Name: MFA for Exchange Online Demo

Assignments

- Users and groups: Specific users included
- Cloud apps: 0 cloud apps selected
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session: 0 controls selected

Enable policy

Cloud apps

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Select
Cloud apps

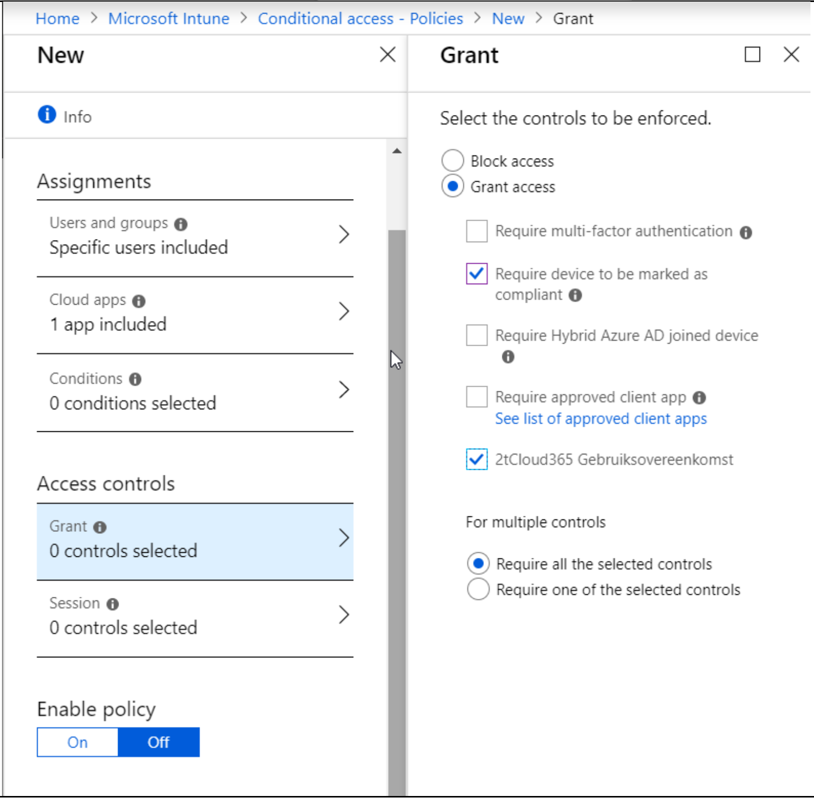
Applications: Search Applications...

- Microsoft Demos
- Microsoft Planner
- Microsoft PowerApps
- Microsoft StaffHub
- Microsoft Teams
- ✓ Office 365 Exchange Online
- Office Delve

Selected: Office 365 Exchange Online

11. Under Access controls select Grant

12. Here you select Grant access and you check Require device to be marked as compliant, and the Terms of use



Home > Microsoft Intune > Conditional access - Policies > New > Grant

New

Info

Assignments

- Users and groups: Specific users included
- Cloud apps: 1 app included
- Conditions: 0 conditions selected

Access controls

- Grant: 0 controls selected
- Session: 0 controls selected

Enable policy: On | Off

Grant

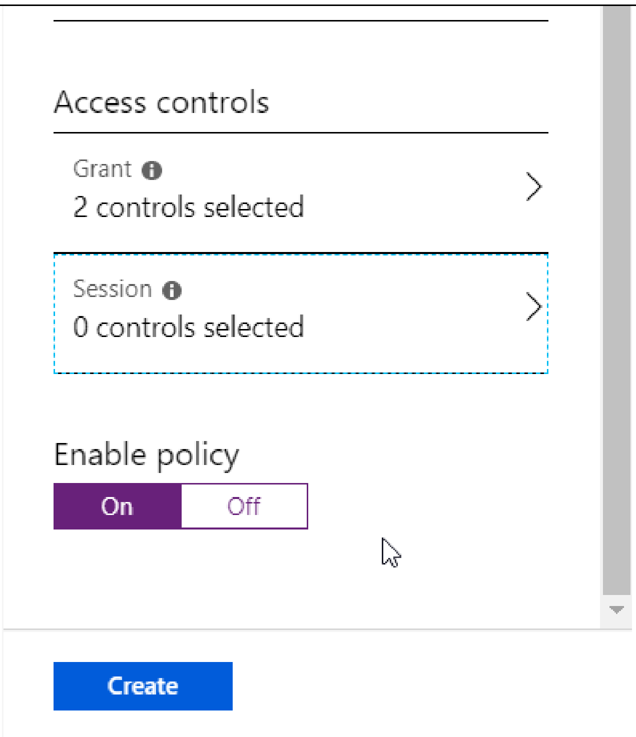
Select the controls to be enforced.

○ Block access
● Grant access

☐ Require multi-factor authentication
☑ Require device to be marked as compliant
☐ Require Hybrid Azure AD joined device
☐ Require approved client app
See list of approved client apps
☑ 2tCloud365 Gebruiksovereenkomst

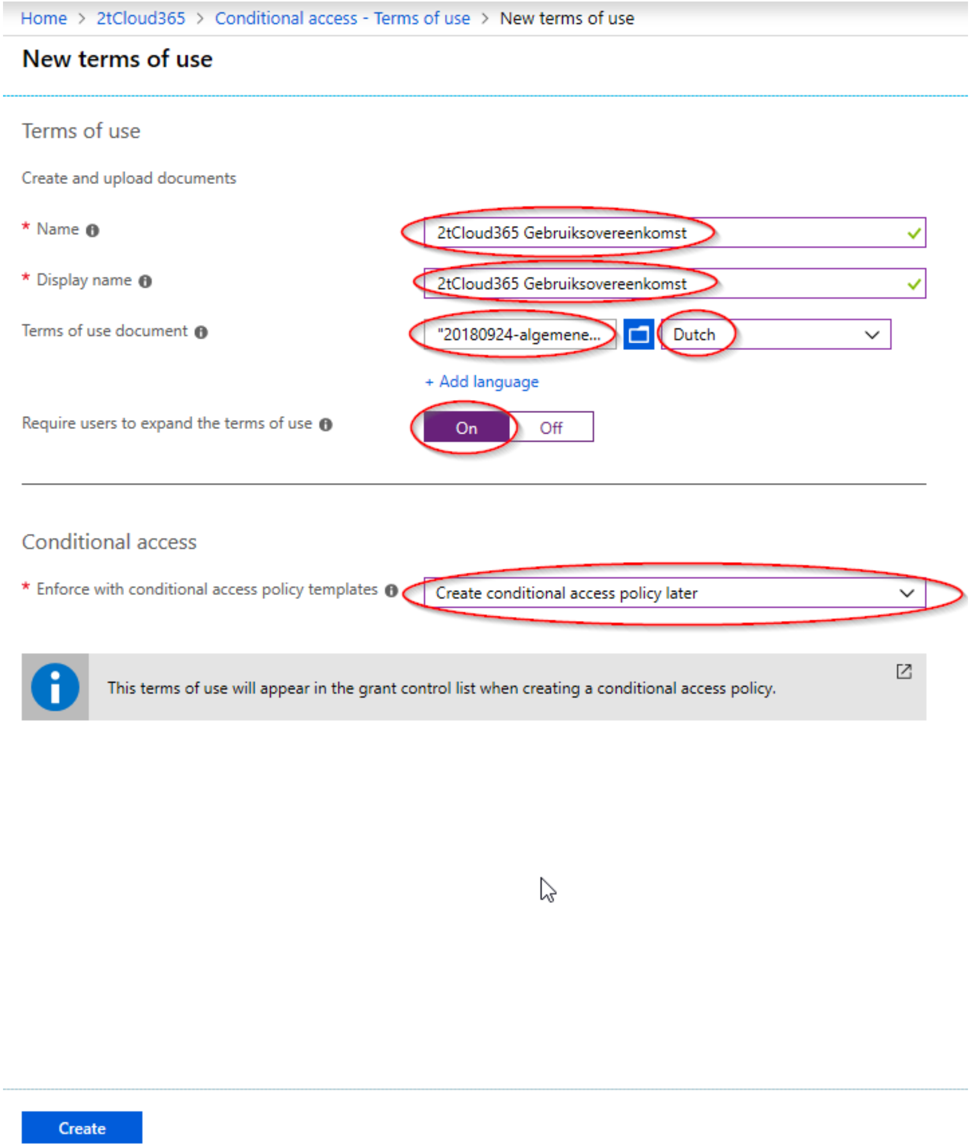
For multiple controls

● Require all the selected controls
○ Require one of the selected controls

1. Enable the policy and clik on Create	 Access controls Grant 2 controls selected Session 0 controls selected Enable policy [✓ On] Off Create

Exercise 7: Terms of use

1. Go to **Azure Active Directory -> Conditional access –> Terms of Use**



Home > 2tCloud365 > Conditional access - Terms of use > New terms of use

New terms of use

Terms of use

Create and upload documents

* Name: 2tCloud365 Gebruiksovereenkomst

* Display name: 2tCloud365 Gebruiksovereenkomst

Terms of use document: "20180924-algemene... Dutch

+ Add language

Require users to expand the terms of use: On Off

Conditional access

* Enforce with conditional access policy templates: Create conditional access policy later

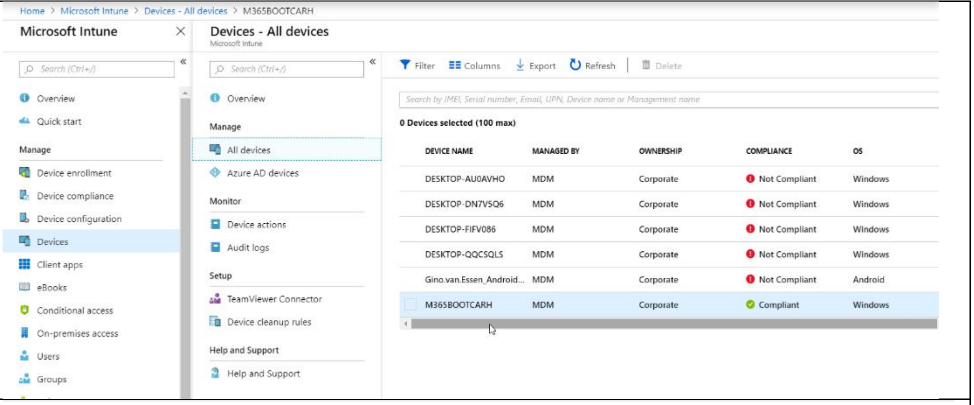
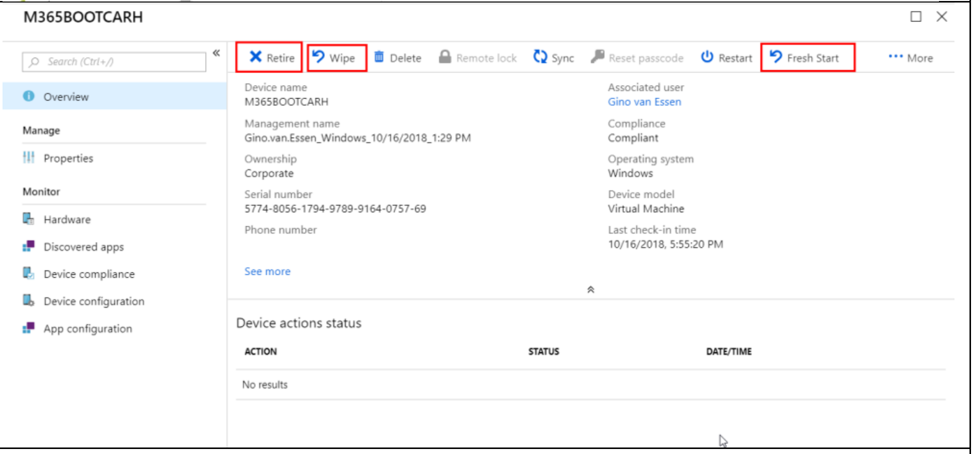
This terms of use will appear in the grant control list when creating a conditional access policy.

Create

2. Create new -> Configure the settings -> Click **Create**

Name	2tCloud365 Gebruiksovereenkomst or your own
Display name	2tCloud365 Gebruiksovereenkomst or your own
Terms of Use document	Add pdf document
Language	English or Dutch
Enfore with conditional access policy templates	Create conditional access policy later

Activity 5: Selective Wipe

Go to Microsoft Intune → Devices → All devices 1. Here you can select the device that you want to wipe	
2. On the overview page you can find Retire, Wipe and Fresh Start. 3. You can click on them to read what they will do. 4. For demonstrating purposes you can choose Retire.	
5. Go back to your test device and monitor any changes	

0 Devices selected (100 max)

DEVICE NAME	MANAGED BY	OWNERSHIP	COMPLIANCE	OS
DESKTOP-AU0AVHO	MDM	Corporate	❗ Not Compliant	Windows
DESKTOP-DN7V5Q6	MDM	Corporate	❗ Not Compliant	Windows
DESKTOP-FIFV086	MDM	Corporate	❗ Not Compliant	Windows
DESKTOP-QQCSQLS	MDM	Corporate	❗ Not Compliant	Windows
Gino.van.Essen_Android...	MDM	Corporate	❗ Not Compliant	Android
M365BOOTCARH	MDM	Corporate	✓ Compliant	Windows

Device name
M365BOOTCARH

Management name
Gino.van.Essen_Windows_10/16/2018_1:29 PM

Ownership
Corporate

Serial number
5774-8056-1794-9789-9164-0757-69

Phone number

Associated user
Gino van Essen

Compliance
Compliant

Operating system
Windows

Device model
Virtual Machine

Last check-in time
10/16/2018, 5:55:20 PM

Device actions status

ACTION	STATUS	DATE/TIME
No results		

This is the end of the lab.

Extra resources:

Modern Desktop Deployment Center
https://docs.microsoft.com/en-us/microsoft-365/enterprise/desktop-deployment-center-home?branch=desktop-deployment-book

Microsoft 365 Enterprise
https://docs.microsoft.com/en-us/microsoft-365-enterprise/

Enterprise Mobility + Security Blog
https://techcommunity.microsoft.com/t5/Enterprise-Mobility-Security/bg-p/enterprisemobilityandsecurity

Microsoft 365 Modern Desktop Lab Kit
https://www.microsoft.com/en-us/itpro/m365-powered-device-lab-kit