



2tCloud

## Modern Workplace Hands-on lab

AAD Premium, Intune, Office ProPlus



# Microsoft 365 Enterprise

## Lab Guide

Thursday, October 18, 2018

Version 2.0

*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

Name	Version Approved	Position	Date

## Table of Contents

Document Revision .....	2
Change Record .....	2
Introduction .....	4
Objectives .....	4
Student Materials .....	4
Activity 1: Getting Started.....	5
Objectives .....	5
Exercise 1a: Create Windows 10 PRO VM in Azure .....	5
Exercise 1b: Create Windows 10 Enterprise VM .....	5
Activity 2: Prepare Modern workplace with Intune .....	9
Exercise 2: Create an AAD Group.....	10
Exercise 3: Configure MDM and MAM Intune settings .....	12
Exercise 4: Activate Self Service Password Reset .....	13
Exercise 5: Company branding.....	15
Exercise 6: Terms of use .....	19
Exercise 7: Device Settings.....	38
Exercise 8: Device Compliance .....	39
Exercise 9: Conditional Access .....	43
Exercise 10a: Device Configuration - Windows Device Restrictions.....	46
Exercise 10b: Device Configuration - Windows Device Configuration .....	51
Exercise 11: Windows 10 Update Rings.....	54
Exercise 12: Office ProPlus Deployment via Intune.....	56
Exercise 13: Windows Store for Business .....	59
Exercise 14: Company portal .....	61
Exercise 15: MSI app deployment .....	65
Exercise 16: Windows Hello .....	70
Activity 3: Windows 10 PRO / Enterprise configuration.....	71
Exercise 17: Configure Windows 10 Enterprise Azure Active Directory join (organisatie) .....	19
Exercise 17a Azure steps.....	27
Exercise 17b – Hyper V Win10 VM .....	19
Exercise 18: Selective Wipe .....	<b>Error! Bookmark not defined.</b>

## 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/tree/master/modernworkplace>

## Activity 1: Getting Started

### Objectives

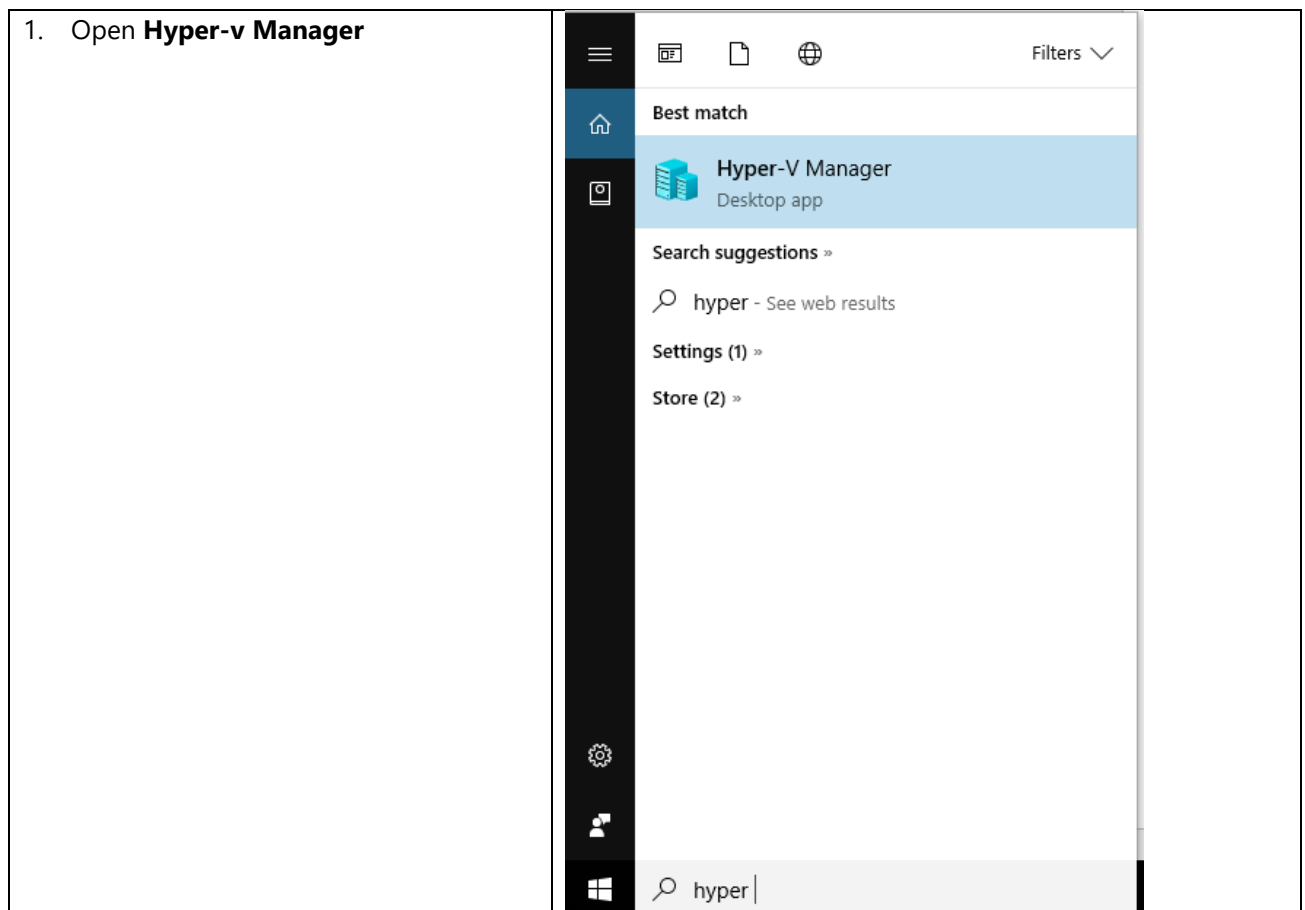
In this activity, you will configure the components necessary to perform this lab:

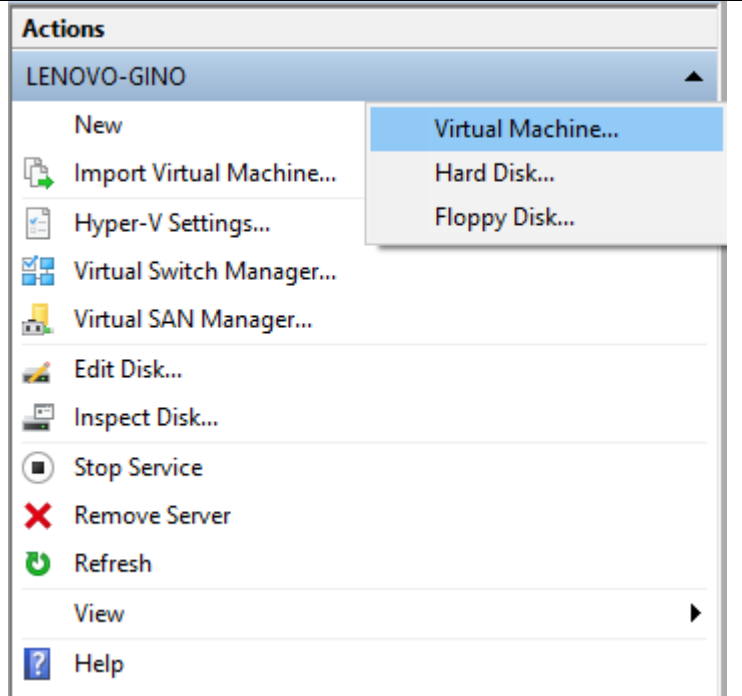
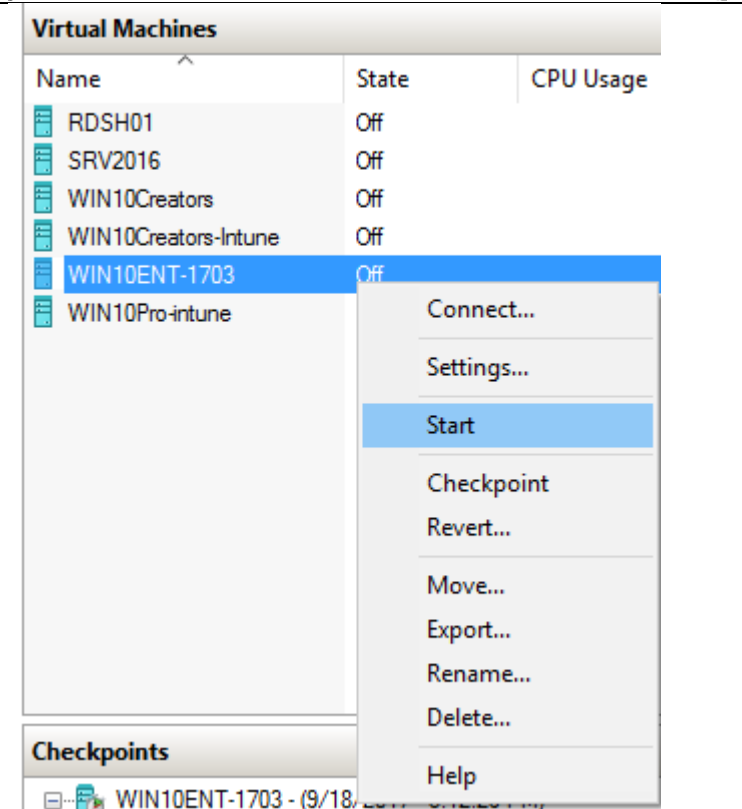
- Windows 10 Pro N, version 1803 - Azure VM

### When Azure tenant \ subscription is not available

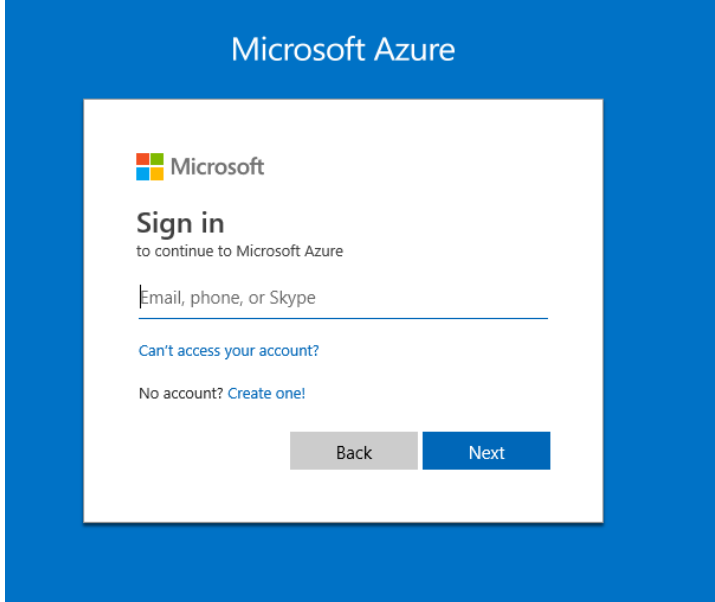
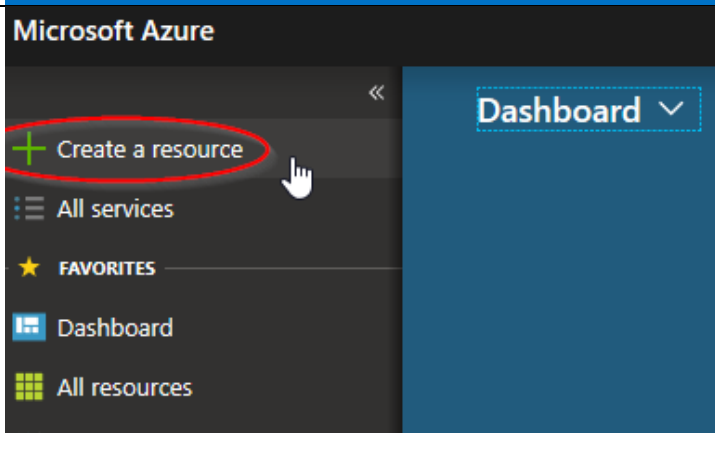
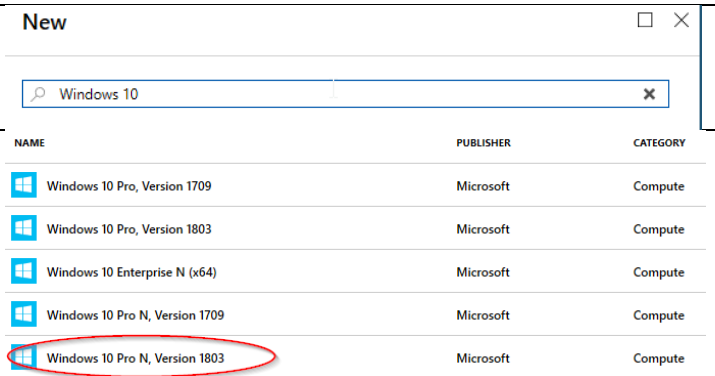

















- ISO of Windows 10 Enterprise 1803 handed out by Copaco
- Hyper V Manager VM configuration

### Exercise 1a: Create Windows 10 Enterprise VM



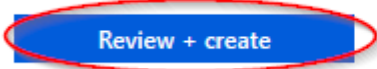
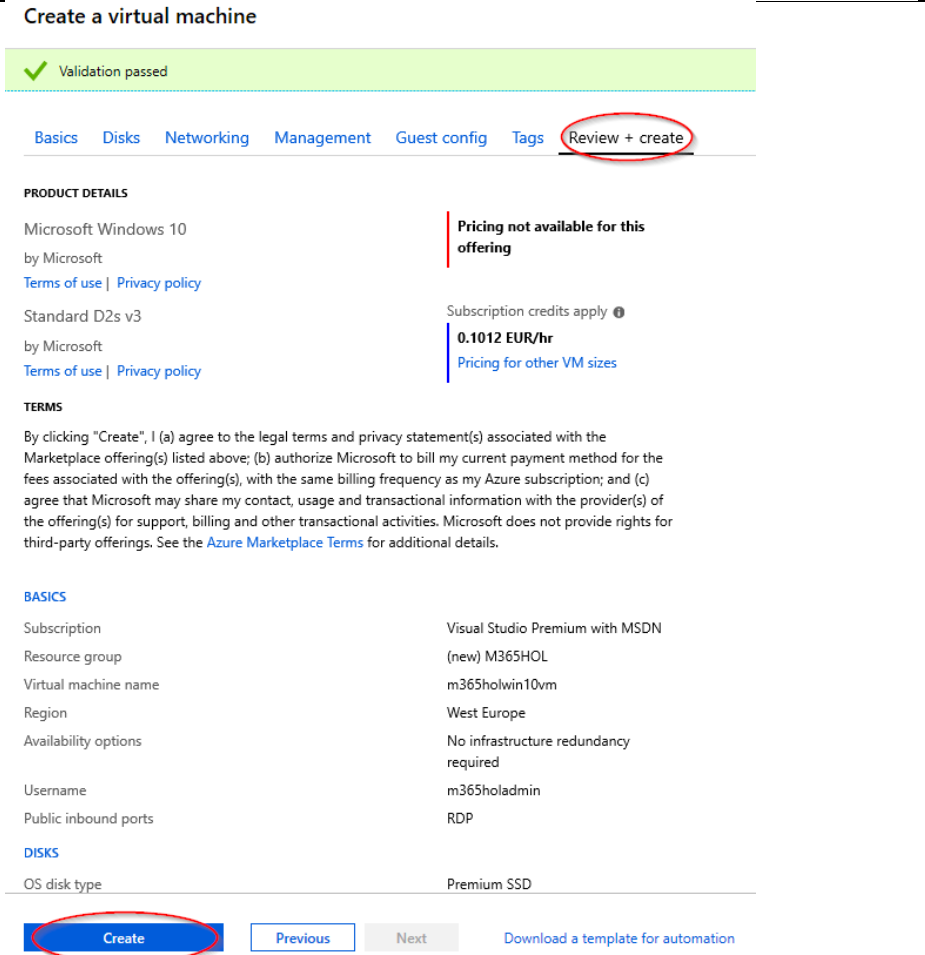
<ol style="list-style-type: none"> <li>2. Create <b>New &gt; virtual machine</b></li> <li>3. Name <b>WIN10ENT-1803</b></li> <li>4. Generation <b>Generation 2</b></li> <li>5. Assign Memory <b>4096 MB</b></li> <li>6. Configure Networking <b>Connection External</b></li> <li>7. Create VHD <b>Standard settings</b></li> <li>8. Installation Options <b>install an OS from a bootable CD/DVD</b></li> <li>9. Image file: "Win10.iso"</li> <li>10. Finish / complete the configuration</li> </ol>	
<ol style="list-style-type: none"> <li>11. Start VM <b>WIN10ENT-1803</b></li> </ol>	
<ol style="list-style-type: none"> <li>12. Start Windows installation with <b>default settings (Custom installation)</b></li> </ol>	

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

13. Go to <a href="https://portal.azure.com">https://portal.azure.com</a> and login with your Azure AD Work account"																			
14. Create a resource																			
15. Search for "Windows 10"	 <table><thead><tr><th>NAME</th><th>PUBLISHER</th><th>CATEGORY</th></tr></thead><tbody><tr><td> Windows 10 Pro, Version 1709</td><td>Microsoft</td><td>Compute</td></tr><tr><td> Windows 10 Pro, Version 1803</td><td>Microsoft</td><td>Compute</td></tr><tr><td> Windows 10 Enterprise N (x64)</td><td>Microsoft</td><td>Compute</td></tr><tr><td> Windows 10 Pro N, Version 1709</td><td>Microsoft</td><td>Compute</td></tr><tr><td> Windows 10 Pro N, Version 1803</td><td>Microsoft</td><td>Compute</td></tr></tbody></table>	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
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. Select "Windows 10 Pro N, Version 1803"																			
17. Click "Create" (bottom of screen)																			

<ol style="list-style-type: none"> <li>18. Select Azure Subscription</li> <li>19. Create resource group "M365HOL"</li> <li>20. Enter VM name "M365holwin10vm"</li> <li>21. Select VM Size "Standard D2s v3"</li> <li>22. Enter username "m365holadmin" with Password "Test@m365hol2018"</li> </ol>	<h3>Create a virtual machine</h3> <p>Basics Disks Networking Management Guest config Tags Review + create</p> <p>Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Looking for classic VMs? <a href="#">Create VM from Azure Marketplace</a></p> <p><b>PROJECT DETAILS</b></p> <p>Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.</p> <p>* Subscription  Visual Studio Premium with MSDN</p> <p>* Resource group  (New) M365HOL <a href="#">Create new</a></p> <p><b>INSTANCE DETAILS</b></p> <p>* Virtual machine name  m365holwin10vm</p> <p>* Region  West Europe</p> <p>Availability options  No infrastructure redundancy required</p> <p>* Image  Windows 10 Pro N, Version 1803 <a href="#">Browse all images and disks</a></p> <p>* Size  Standard D2s v3 2 vcpus, 8 GB memory <a href="#">Change size</a></p> <p><b>ADMINISTRATOR ACCOUNT</b></p> <p>* Username  m365holadmin</p> <p>* Password </p> <p>* Confirm password </p>
<ol style="list-style-type: none"> <li>11. Go to tab "Networking"</li> <li>12. Select "Allow selected ports"</li> <li>13. Select Inbound ports "RDP (3389)"</li> </ol>	<h3>Create a virtual machine</h3> <p>Basics Disks <b>Networking</b> Management Guest config Tags Review + create</p> <p>Configure a new or existing virtual network for your VM as well as how your VM will be accessed on the virtual network. <a href="#">Learn more</a></p> <p><b>NETWORK INTERFACE</b></p> <p>When creating a virtual machine, a network interface will be created for you.</p> <p>* Virtual network  (new) M365HOL-vnet <a href="#">Create new</a></p> <p>* Subnet  default</p> <p>Public IP  (new) m365holwin10vm-ip <a href="#">Create new</a></p> <p>Network security group <input checked="" type="radio"/> Basic <input type="radio"/> Advanced</p> <p>* Public inbound ports  <input type="radio"/> None <input checked="" type="radio"/> Allow selected ports</p> <p>* Select inbound ports</p> <div> <input type="checkbox"/> HTTP (80)  <input type="checkbox"/> HTTPS (443)  <input type="checkbox"/> SSH (22)  <input checked="" type="checkbox"/> RDP (3389)     </div> <p>Accelerated networking  <input type="radio"/> On <input checked="" type="radio"/> Off</p> <p>The selected image does not support accelerated networking.</p>



<p>14. Click "Review + create"</p>	
<p>15. Click "Create"</p> <p>16. After 10 minutes (maximum) the VM creation is finished</p>	

## Activity 2: Prepare Modern workplace with Intune

The most important components in this exercise are:



Azure Active Directory.



Users and Groups.



Intune.

## Exercise 2: Create an AAD Group

1. Go to : <http://portal.azure.com>
2. Go to: **Azure Active Directory->Manage->Groups**
3. Click **New Group** and create a group with the following settings

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

4. Add Admin account to group "**UG\_Gebruikers\_MDM**"
5. Click Create (bottom of screen)

### 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

[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

Create

Select members

Select member or invite an external user ⓘ

Search by name or email address

Searching...

Selected members:

No members selected

Select

## 6. AAD Group “UG\_Gebruikers\_MDM” is created

+ New group

Refresh

Columns

Name

Search groups

NAME	GROUP TYPE	MEMBERSHIP TYPE
UG UG_Gebruikers_MDM	Security	Assigned

## 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 

MDM discovery URL 

MDM compliance URL 

[Restore default MDM URLs](#)


---


MAM User scope  None **Some** All


---

Groups Select groups  
UG\_Gebruikers\_MDM >

---

MAM Terms of use URL 

MAM Discovery URL 

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**

Home > 2tCloud365 > Password reset - Properties

### Password reset - Properties

2tCloud365 - Azure Active Directory

Manage

Properties

Authentication methods

Registration

Notifications

Customization

On-premises integration

Activity

Audit logs

Troubleshooting + Support

Troubleshoot

New support request

Save Discard

Self service password reset enabled ⓘ

None Selected **All**

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

Home > 2tCloud365 > Password reset - Customization

**Password reset - Customization**  
2tCloud365 - Azure Active Directory

Manage

- Properties
- Authentication methods
- Registration
- Notifications
- Customization**
- On-premises integration

Activity

- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Save Discard

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

Manage

- Properties
- Authentication methods
- Registration**
- Notifications
- Customization
- On-premises integration

Activity

- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Save Discard

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: 240x240x(resizable)  
Max file size: 10KB  
PNG (preferred) or JPG

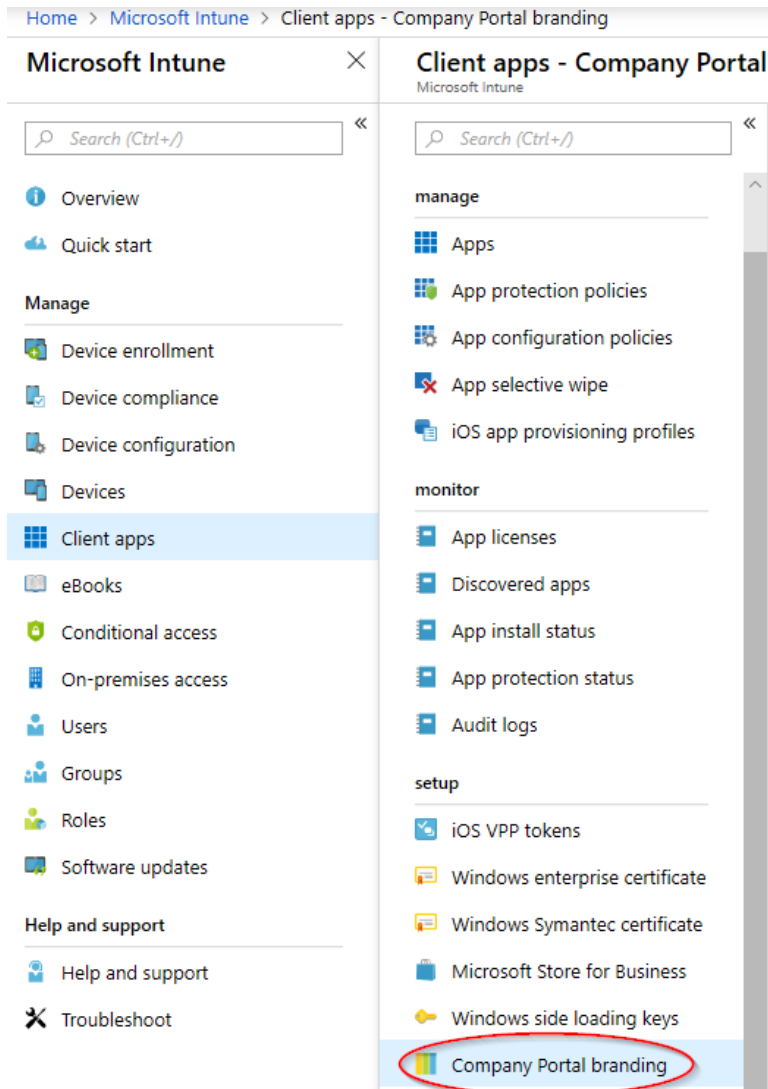
Remove  
Select a file

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	<a href="mailto:gebruikersnaam@2tcloud365.nl">gebruikersnaam@2tcloud365.nl</a>
Show option to remain signed in	No

1. Go to Intune -> Client apps -> Company Portal Branding



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

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



### Client apps - Company Portal branding

Microsoft Intune

manage

- Apps
- App protection policies
- App configuration policies
- App selective wipe
- iOS app provisioning profiles

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

Save

Enter your company's support information 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 information

\* Company name: ⓘ  
2tCloud

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

#### Support information

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

For more settings -> Next page

Show company logo	Yes
Company logo	Add logo

### Theme color

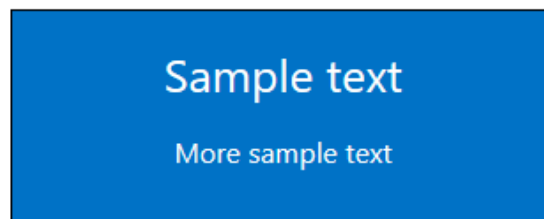
Apply a theme color to the Company Portal. Select a standard color or enter a six-digit hex code for a custom color.

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 appearance, upload a logo with a transparent 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

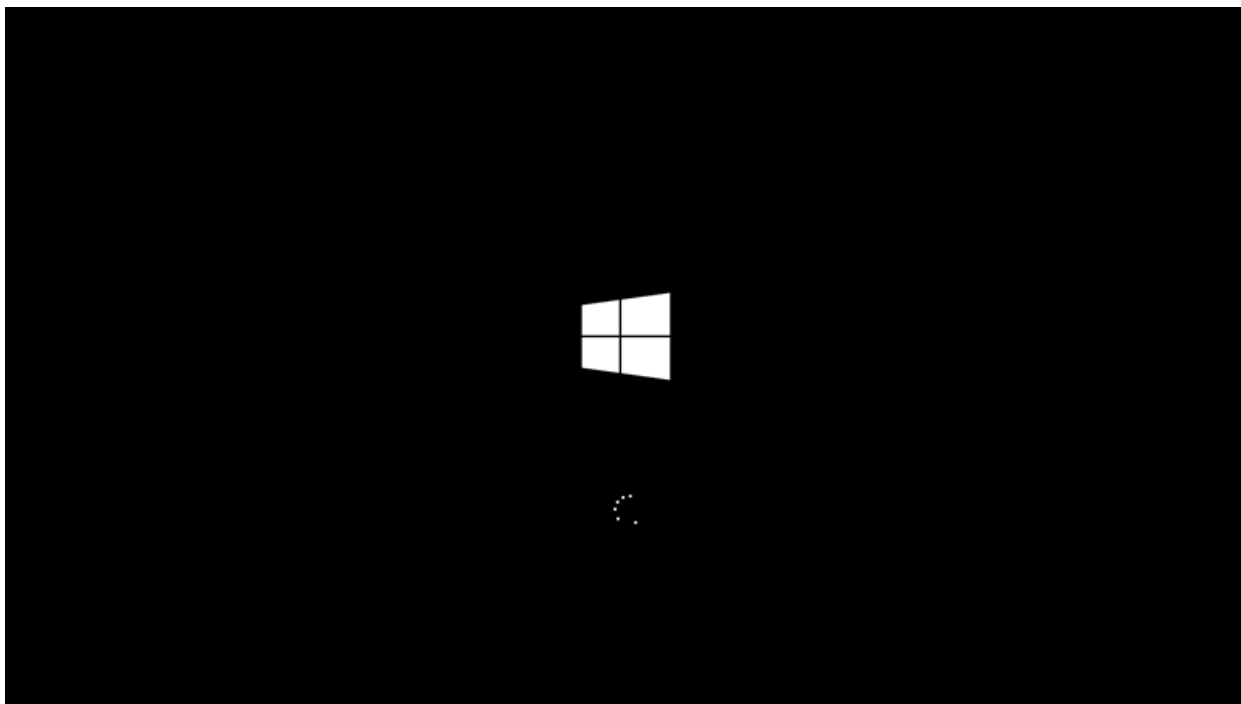
## Activity 3: Add Windows to MDM

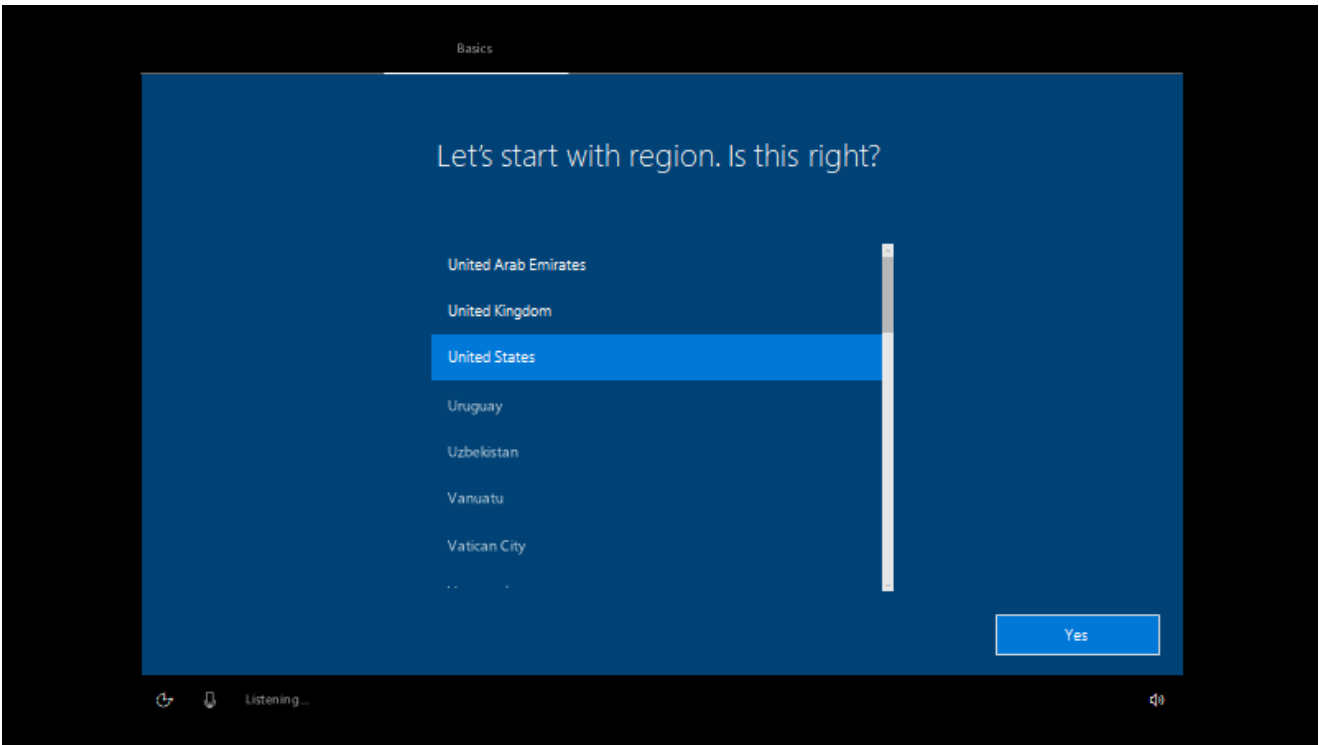
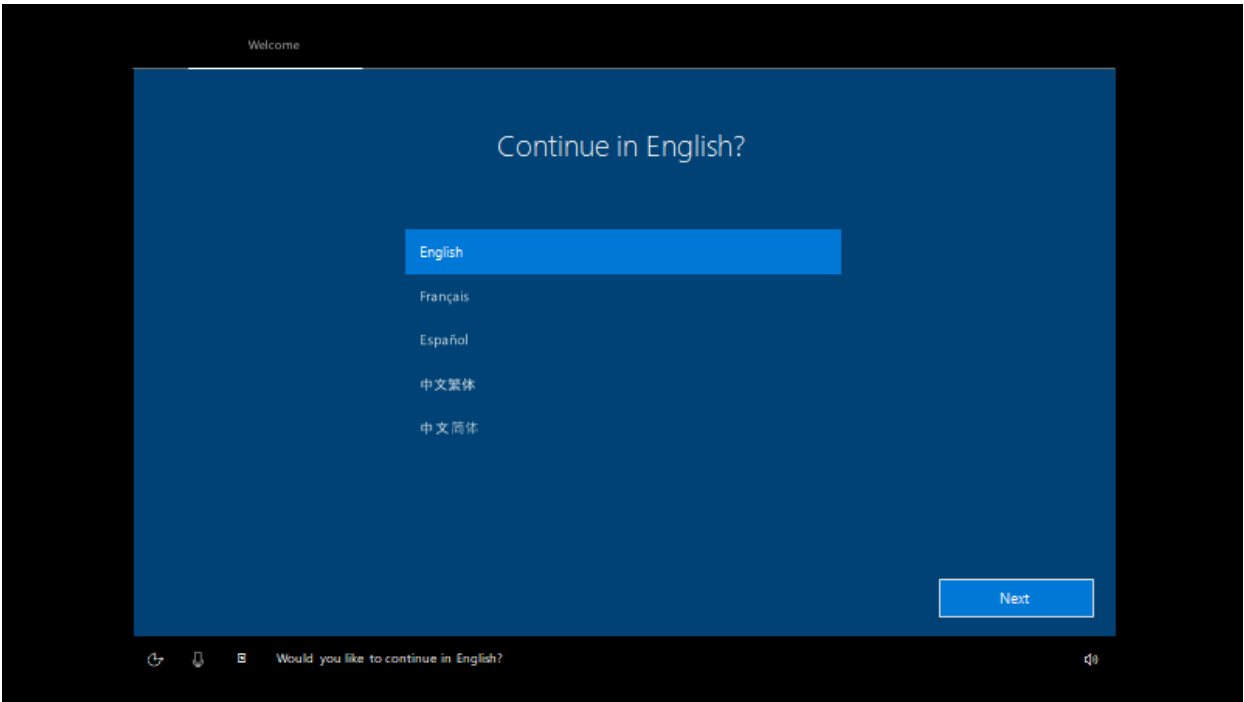
### Exercise 6: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)

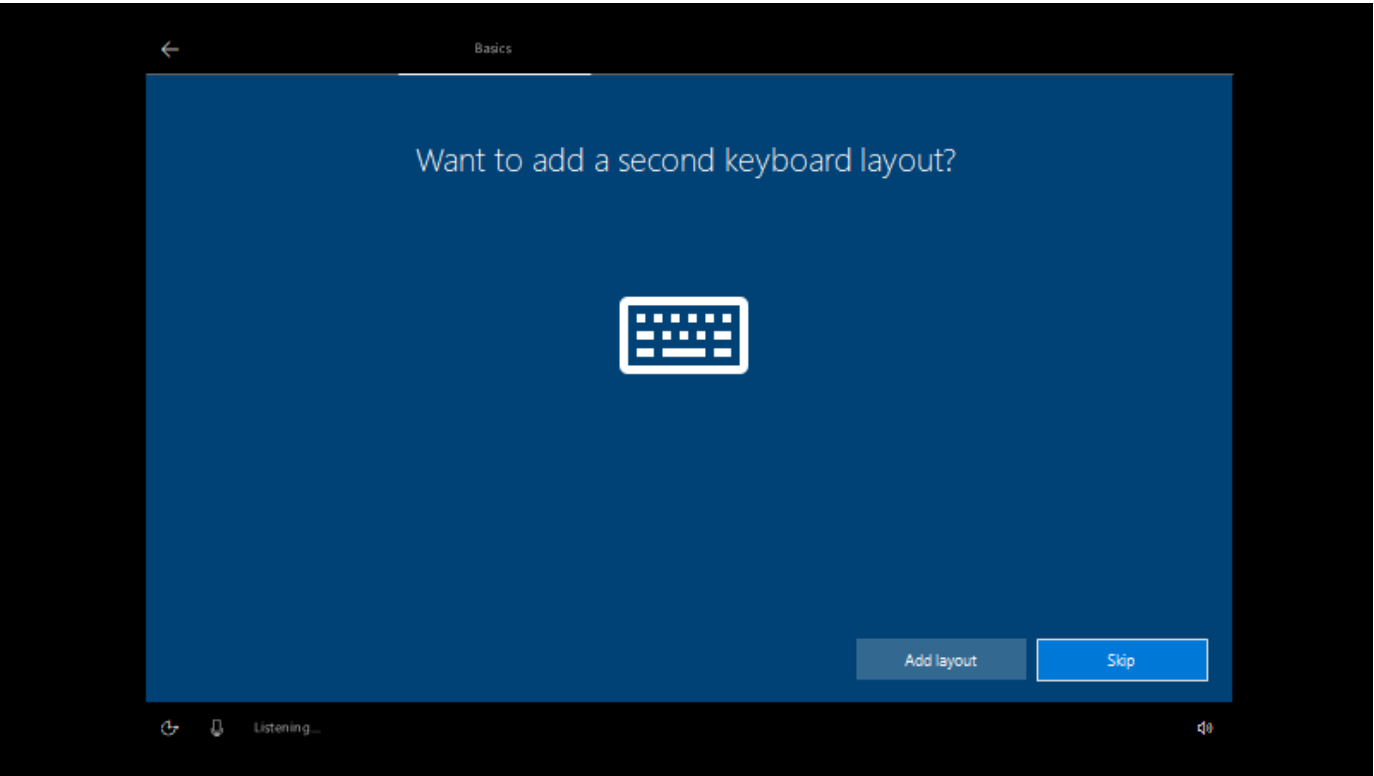
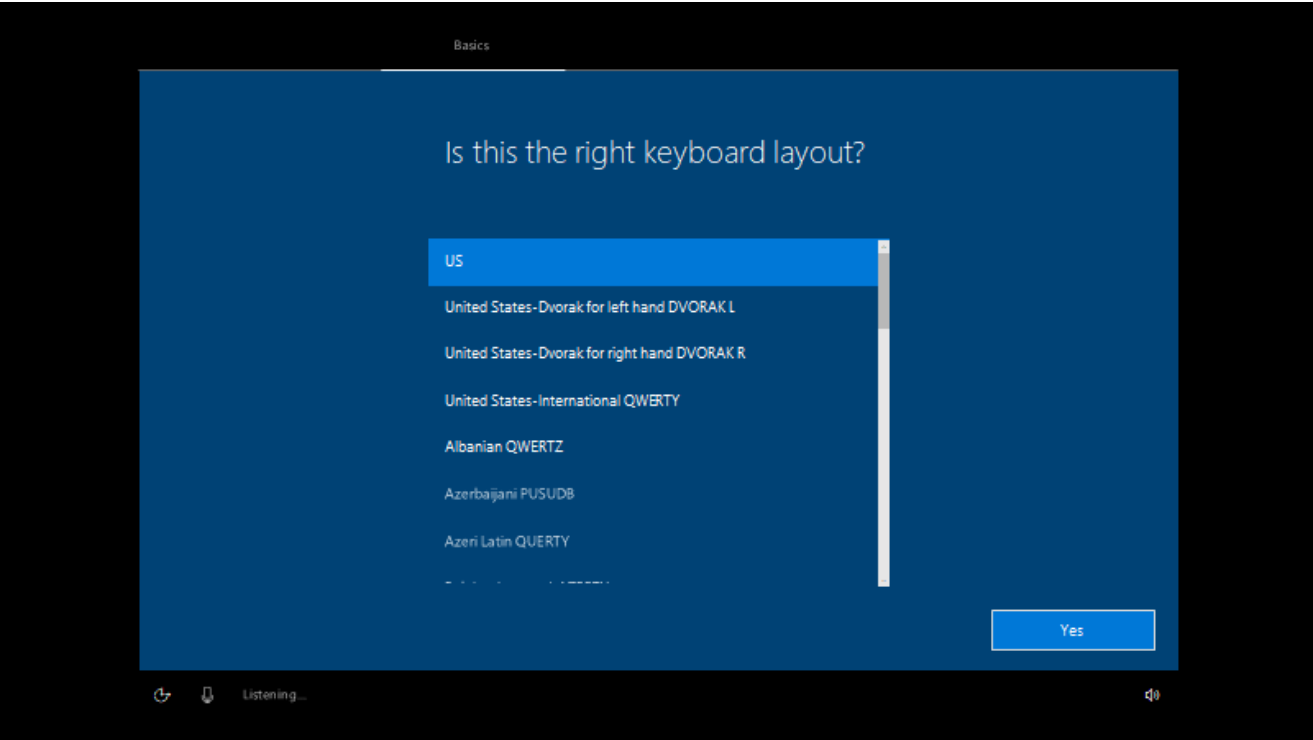
Go to the Win10 VM (Azure or Hyper-V Manager)

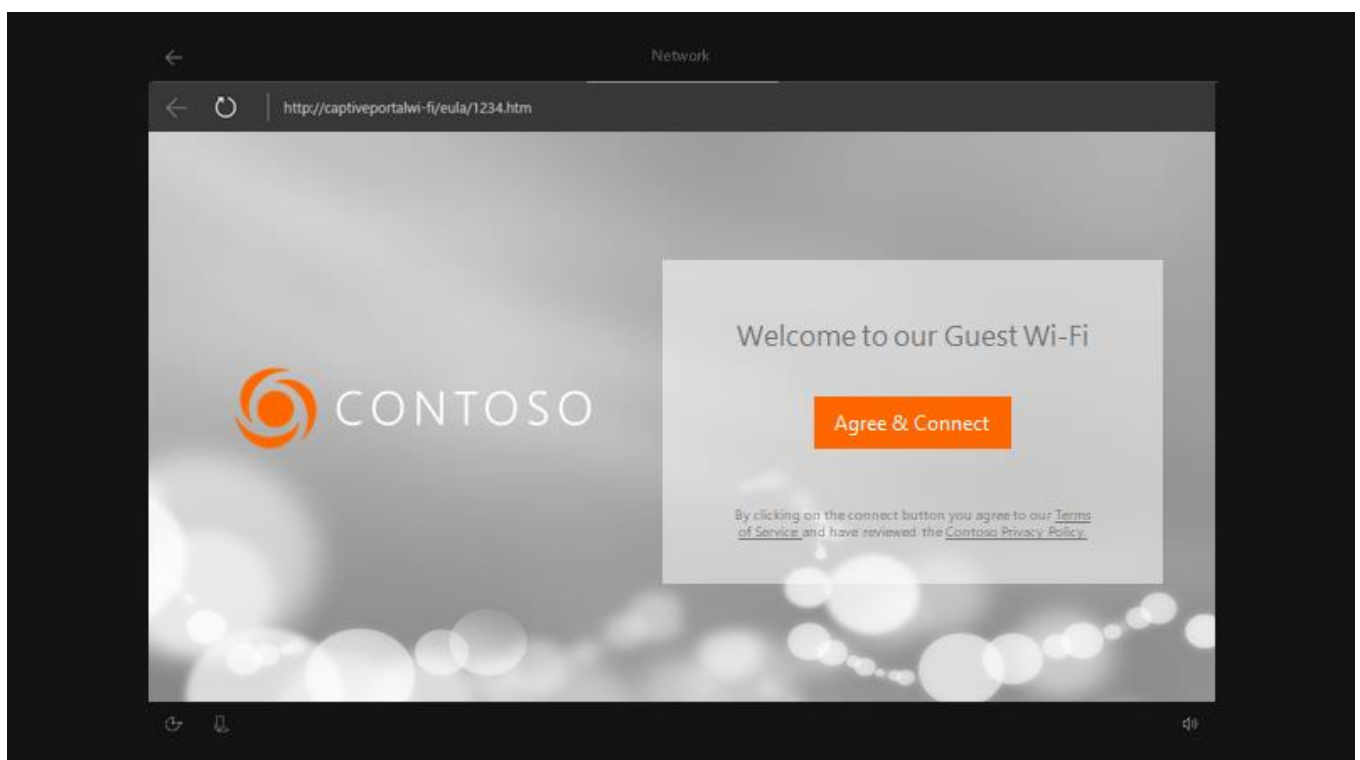
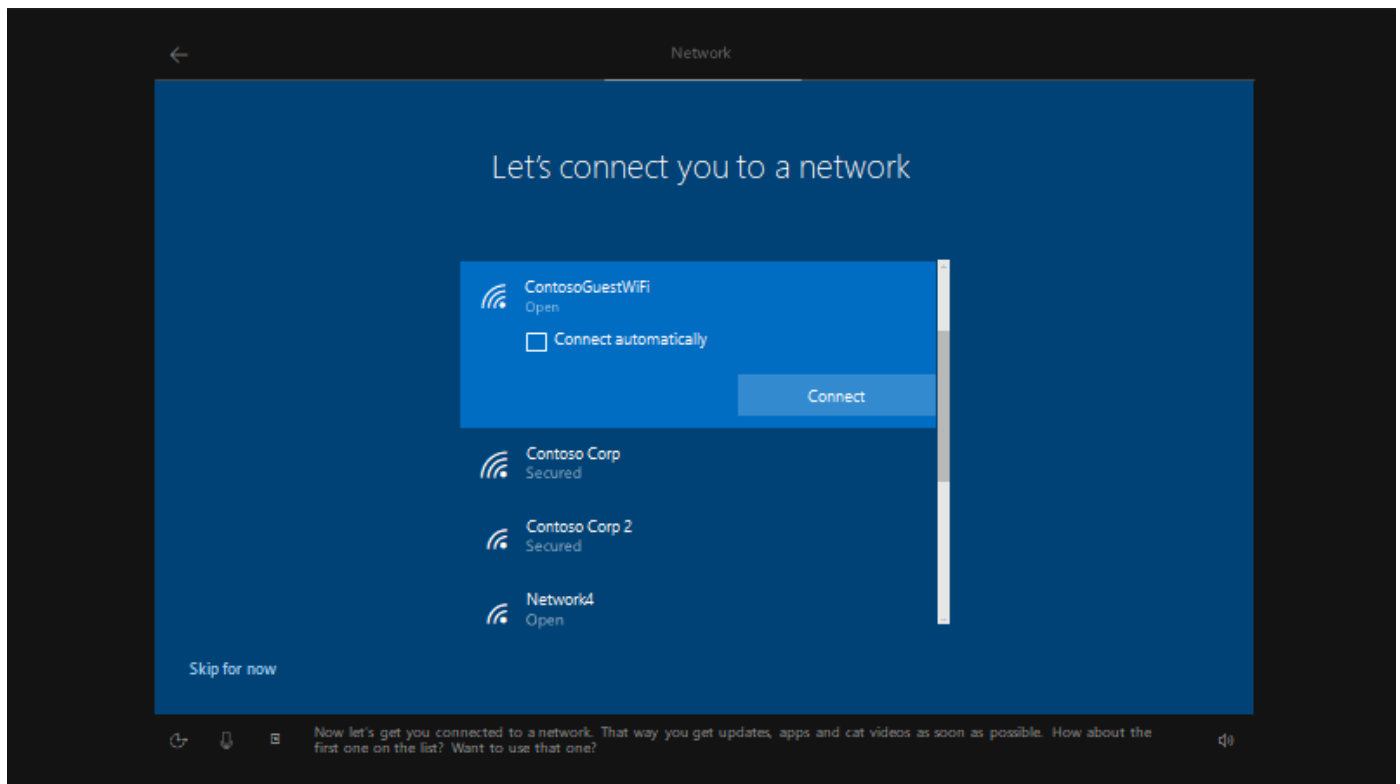
#### Exercise 6b – Hyper V Win10 VM

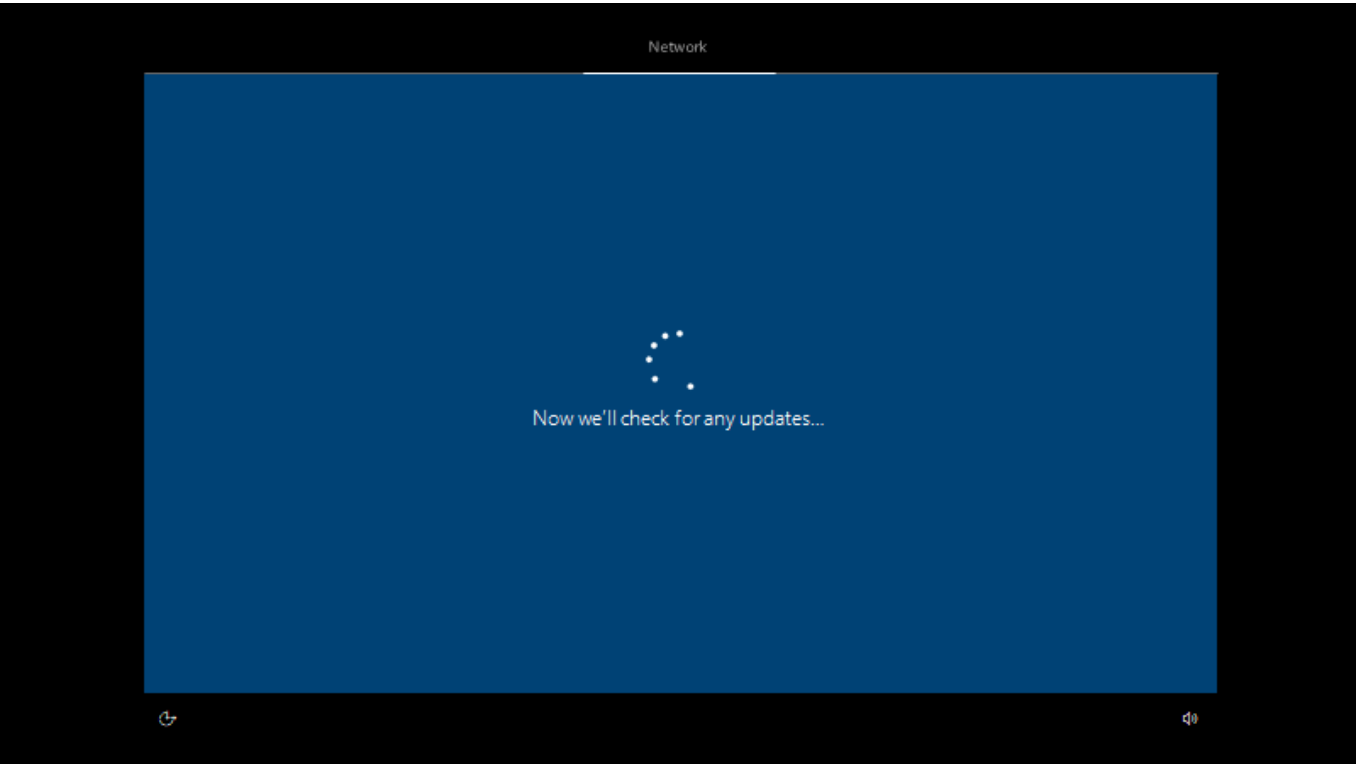
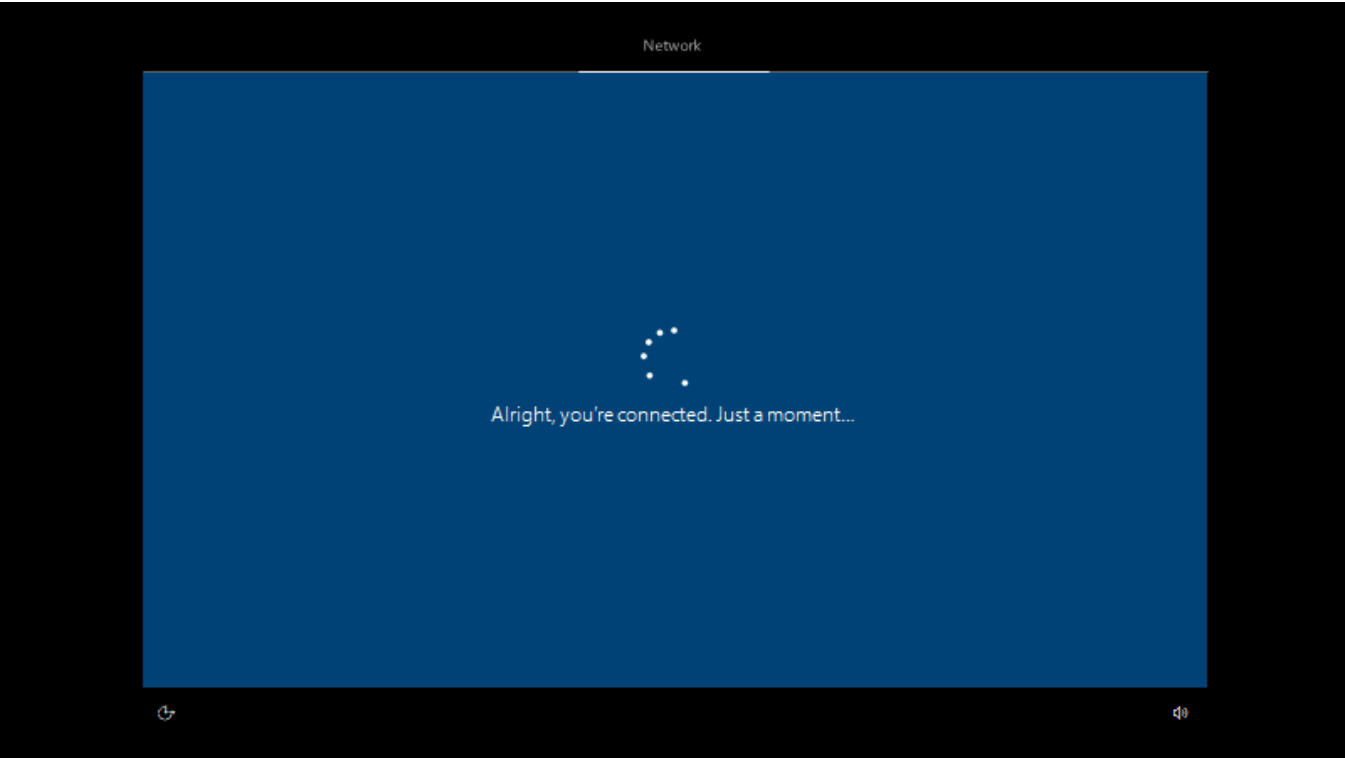
Start the setup of the Windows 10 Enterprise OS

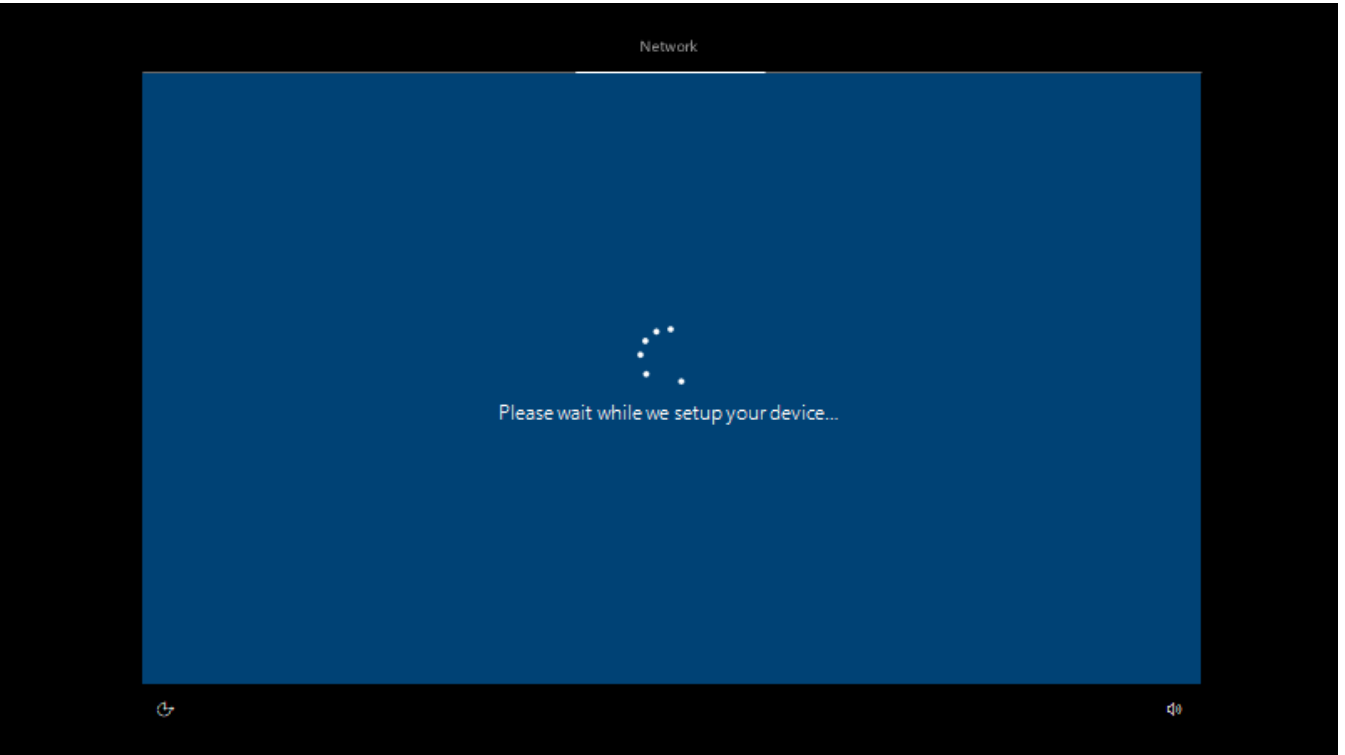
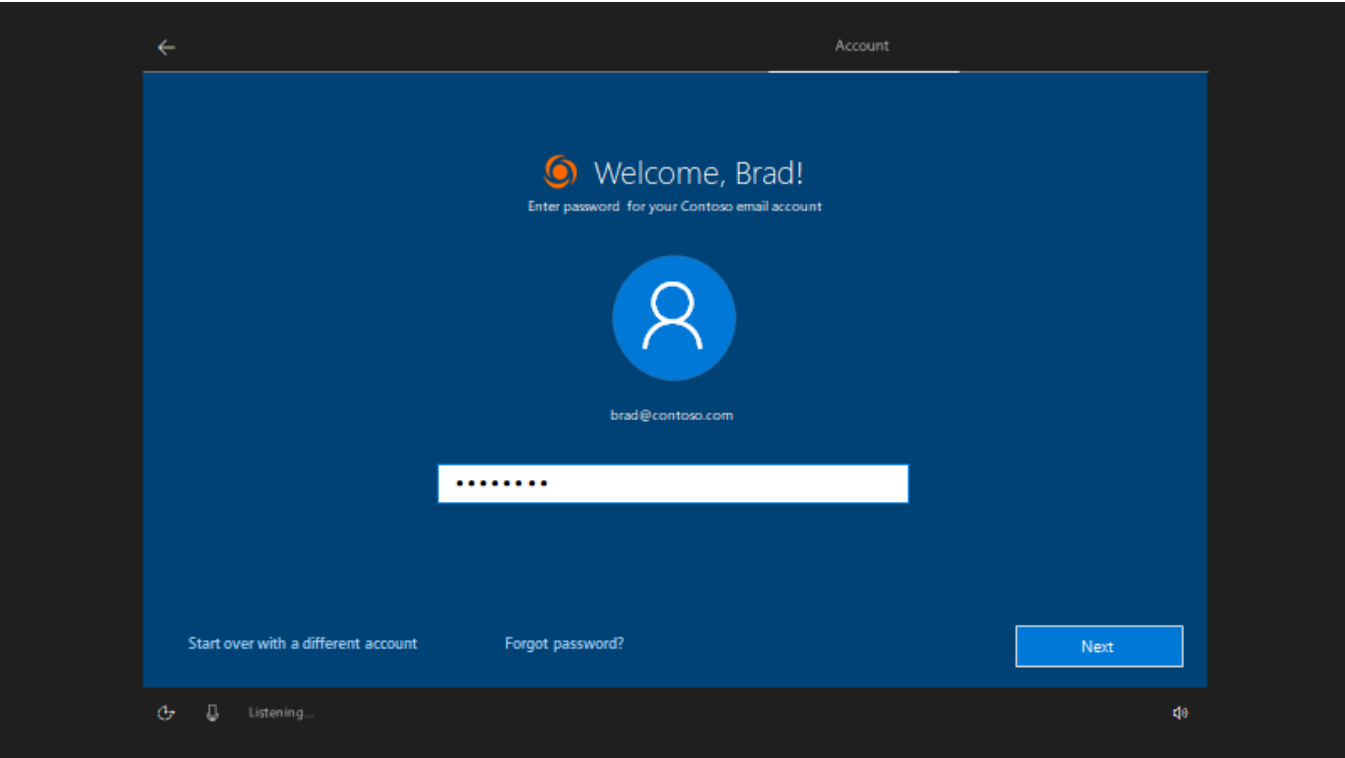




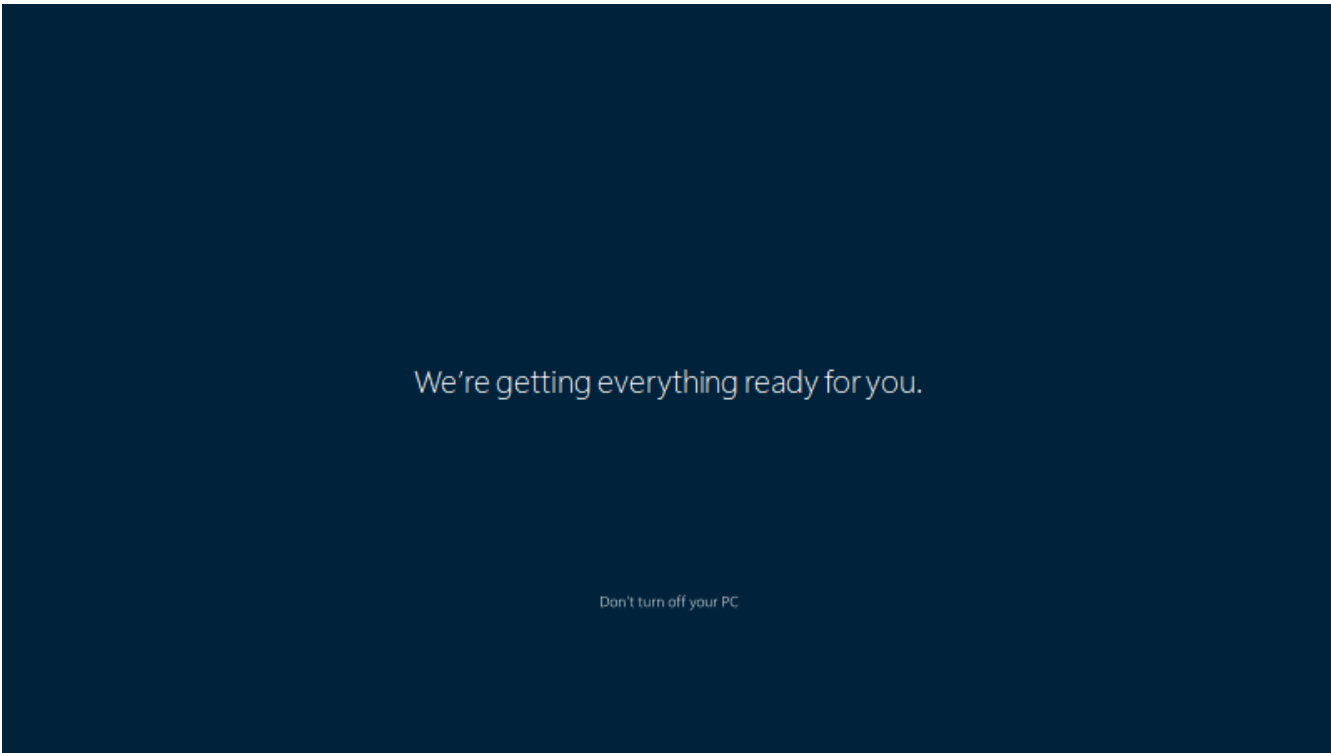
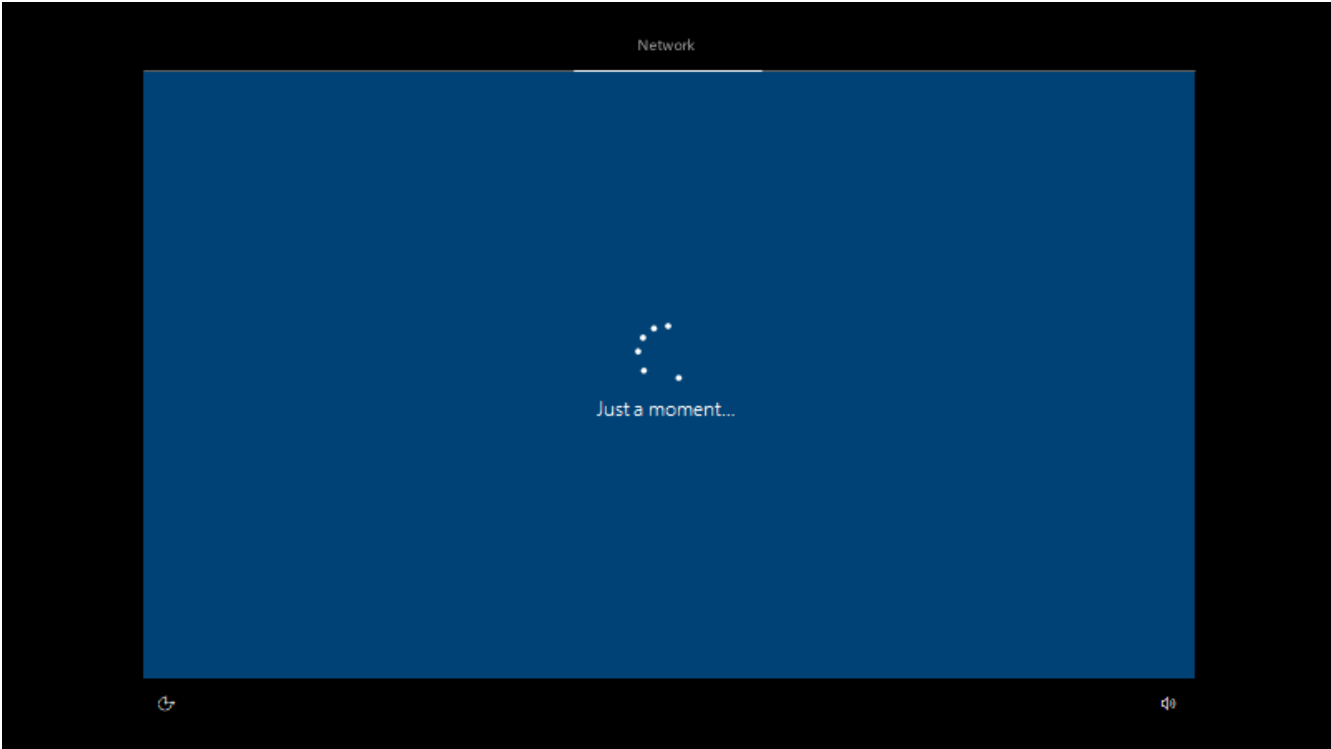












We're getting everything ready for you.

Don't turn off your PC

## Exersize 6c Azure steps OPTIONAL

1. Open <https://portal.azure.com> -> Virtual machines
2. Click "M365holwin10vm"
3. Click **Connect**
4. Download **RDP File**
5. Login with the Admin credentials (used in step 10 - Create Windows 10 PRO VM in Azure)

[Home](#) > Virtual machines


### Virtual machines

engineeringcopaco (Default Directory)

+ Add
🕒 Reservations
≡ Edit columns
🔄 Refresh
🏷️ Assign tags
▶ Start
↺ Restart
■ Stop
🗑️ Delete

**Subscriptions:** Visual Studio Premium with MSDN – Don't see a subscription? [Open Directory + Subscription settings](#)

1 items

<input type="checkbox"/>	NAME ↑↓	TYPE ↑↓	STATUS
<input type="checkbox"/>	 <a href="#">m365bootcarh</a>	Virtual machine	Running

### Connect to virtual machine

m365bootcarh


RDP
SSH

To connect to your virtual machine via RDP, select an IP address, optionally change the port number, and download the RDP file.


\* IP address

\* Port number

Download RDP File



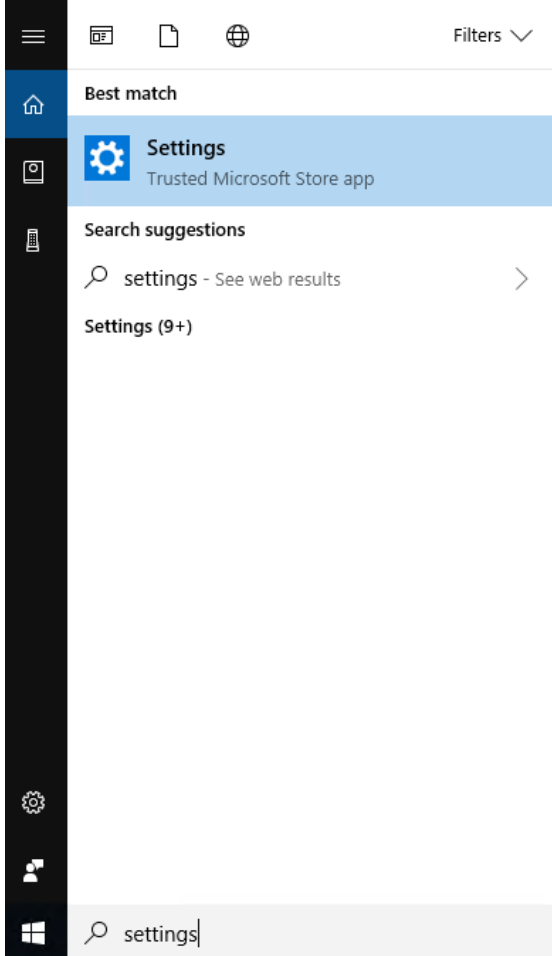
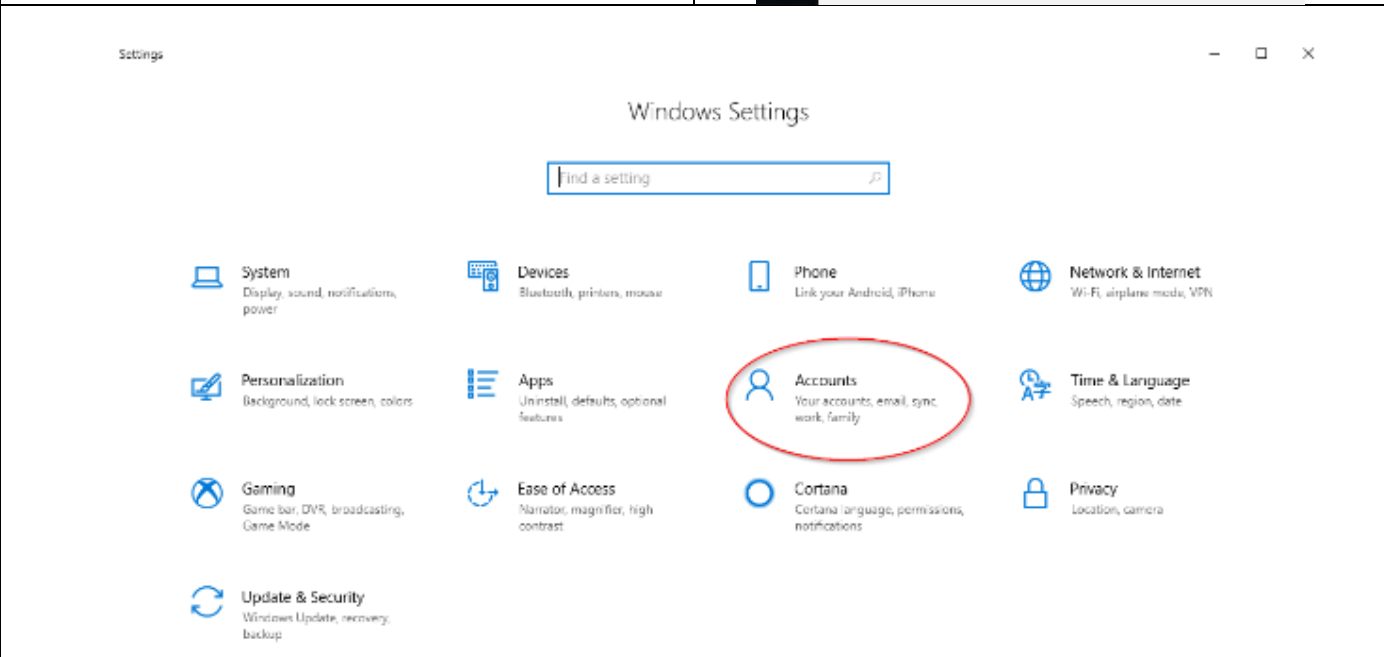
Inbound traffic to the Public IP address may be blocked. You can update inbound port rules in the **VM Networking** page.

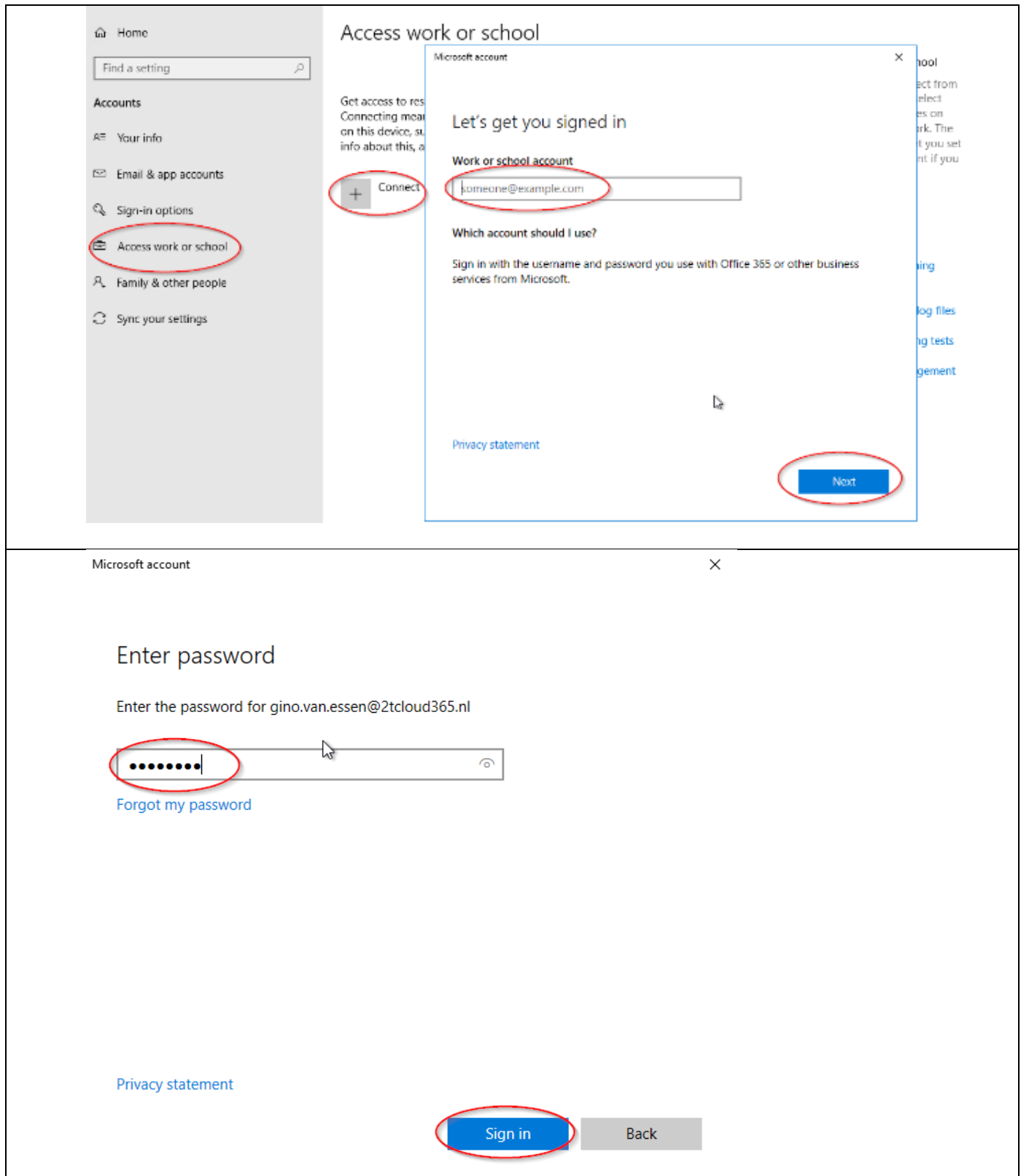


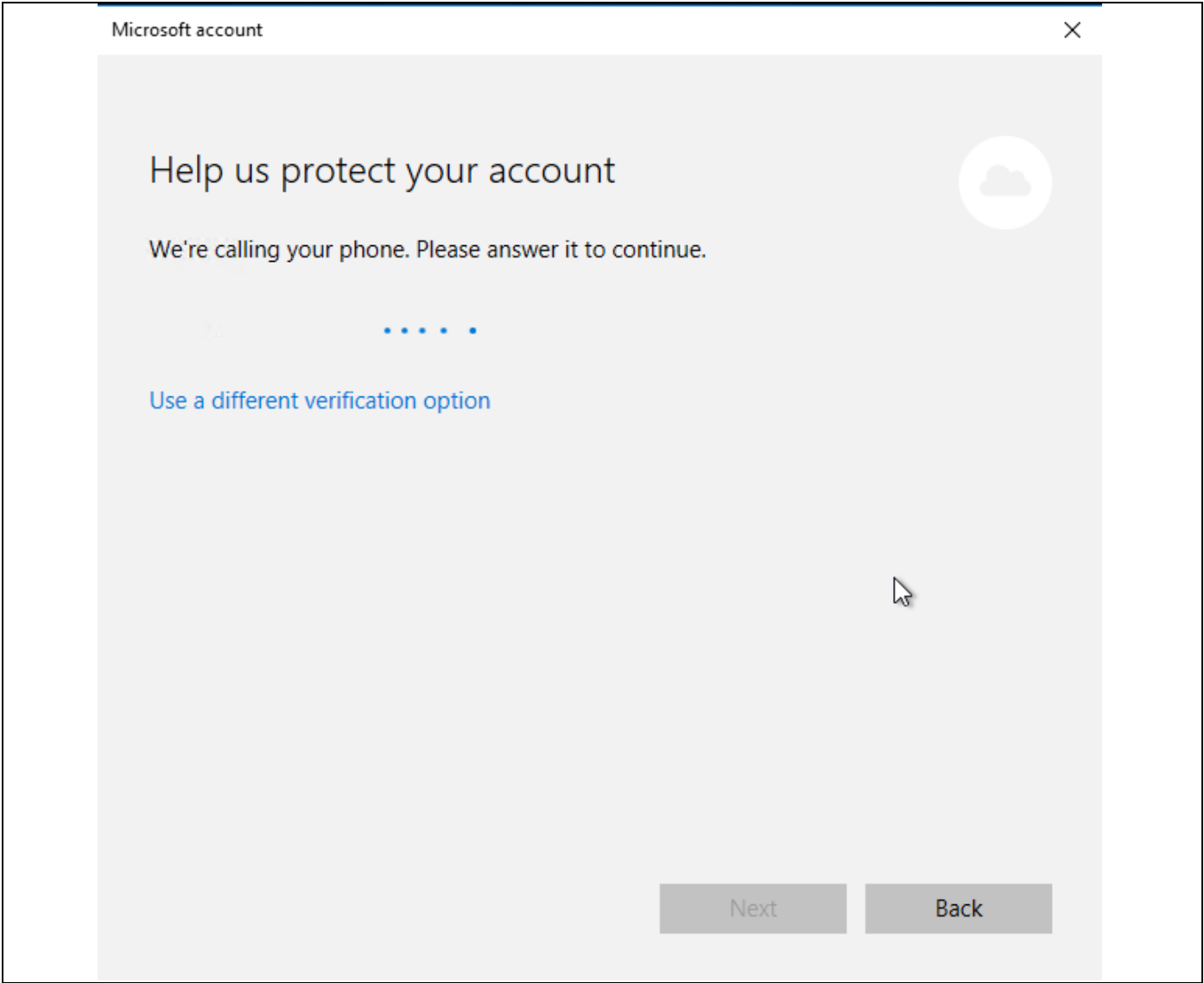
You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

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

Complete these steps on the M365holwin10vm virtual machine.

<p>Enroll a Windows 10 Device in Intune</p> <ol style="list-style-type: none"> <li>1. Login to the virtual machine and go to <b>Start &gt; Settings</b>.</li> <li>2. In the <b>Settings</b> app, browse to <b>Accounts &gt; Access work or school</b>.</li> <li>3. Click <b>Enroll only in device management</b>.</li> <li>4. The <b>Setup a work or school account</b> dialog box will show, asking for your account to enroll the device.</li> <li>5. Provide the <b>Azure AD</b> account and click <b>Next</b>.</li> <li>6. In the <b>Microsoft Intune Enrollment</b> page, enter the <b>password</b> then click <b>Sign in</b>. Click <b>Got it</b>.</li> <li>7. In the <b>Settings</b> app, you should see that the device is now connected to the corporate MDM.</li> <li>8. Click <b>Sync</b> and confirm that the sync was <b>successful</b>.</li> </ol>	 <p>The screenshot shows the Windows Search interface. The search bar at the top contains the text 'settings'. Below the search bar, the results are categorized under 'Best match'. The first result is 'Settings', labeled as a 'Trusted Microsoft Store app'. Below this, there are 'Search suggestions' including 'settings - See web results'. At the bottom, there is a section for 'Settings (9+)'.</p>
 <p>The screenshot shows the Windows Settings application. The title bar at the top says 'Settings'. The main heading is 'Windows Settings'. Below this is a search bar with the placeholder text 'Find a setting'. The settings are organized into a grid of categories, each with an icon and a list of sub-features. The categories are: System (Display, sound, notifications, power), Devices (Bluetooth, printers, mouse), Phone (Link your Android, iPhone), Network &amp; Internet (Wi-Fi, airplane mode, VPN), Personalization (Background, lock screen, colors), Apps (Uninstall, defaults, optional features), Accounts (Your accounts, email, sync, work, family), Time &amp; Language (Speech, region, date), Gaming (Game bar, DVR, broadcasting, Game Mode), Ease of Access (Narrator, magnifier, high contrast), Cortana (Cortana language, permissions, notifications), and Privacy (Location, camera). The 'Accounts' category is circled in red.</p>	





Microsoft account

✕

### Choose the best category for this device

This category helps your IT admin provide access to company resources for this device.  
After setting this category, you must contact your IT admin to change it.

**Category**

Pilot

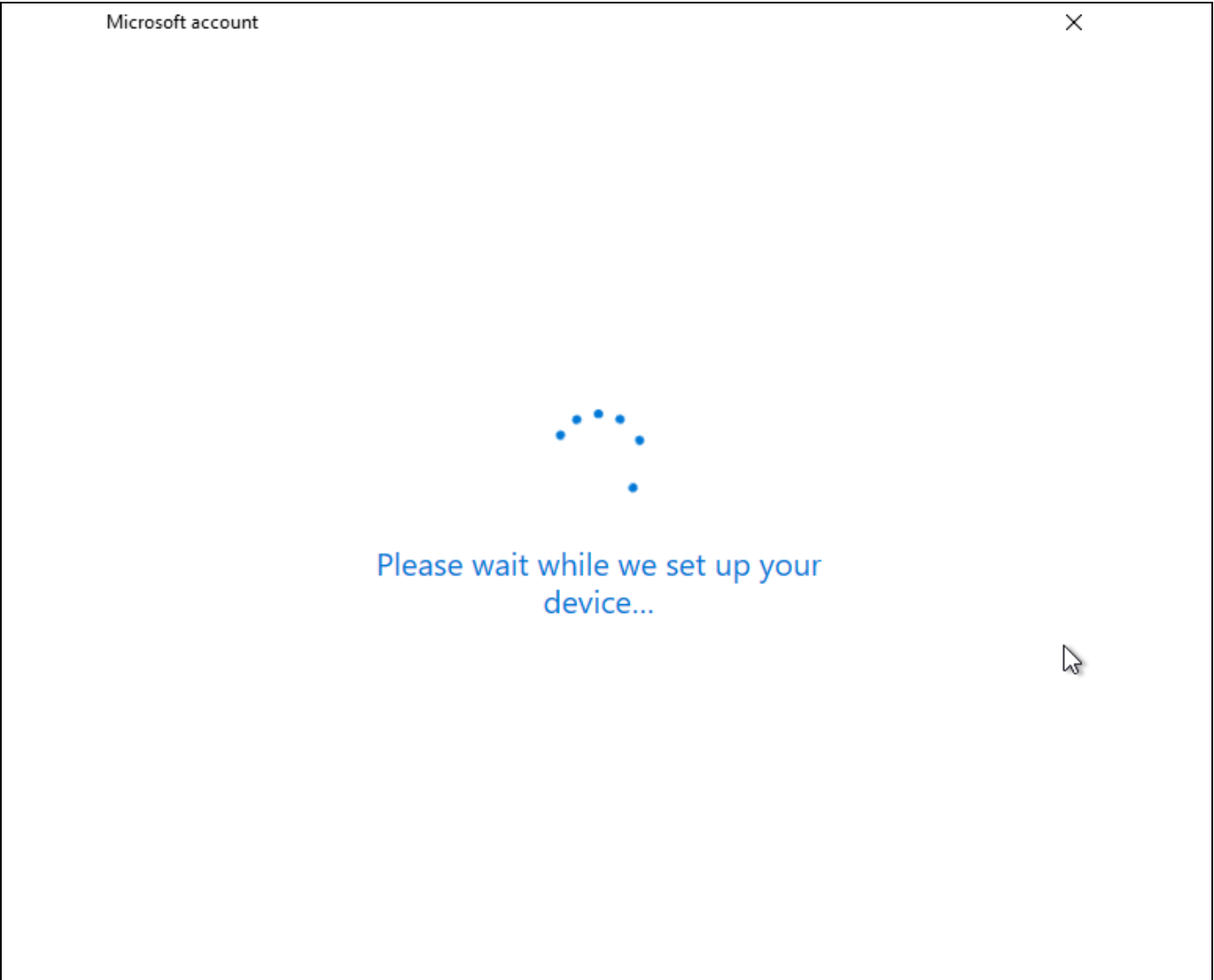
Next

### Make sure this is your organization

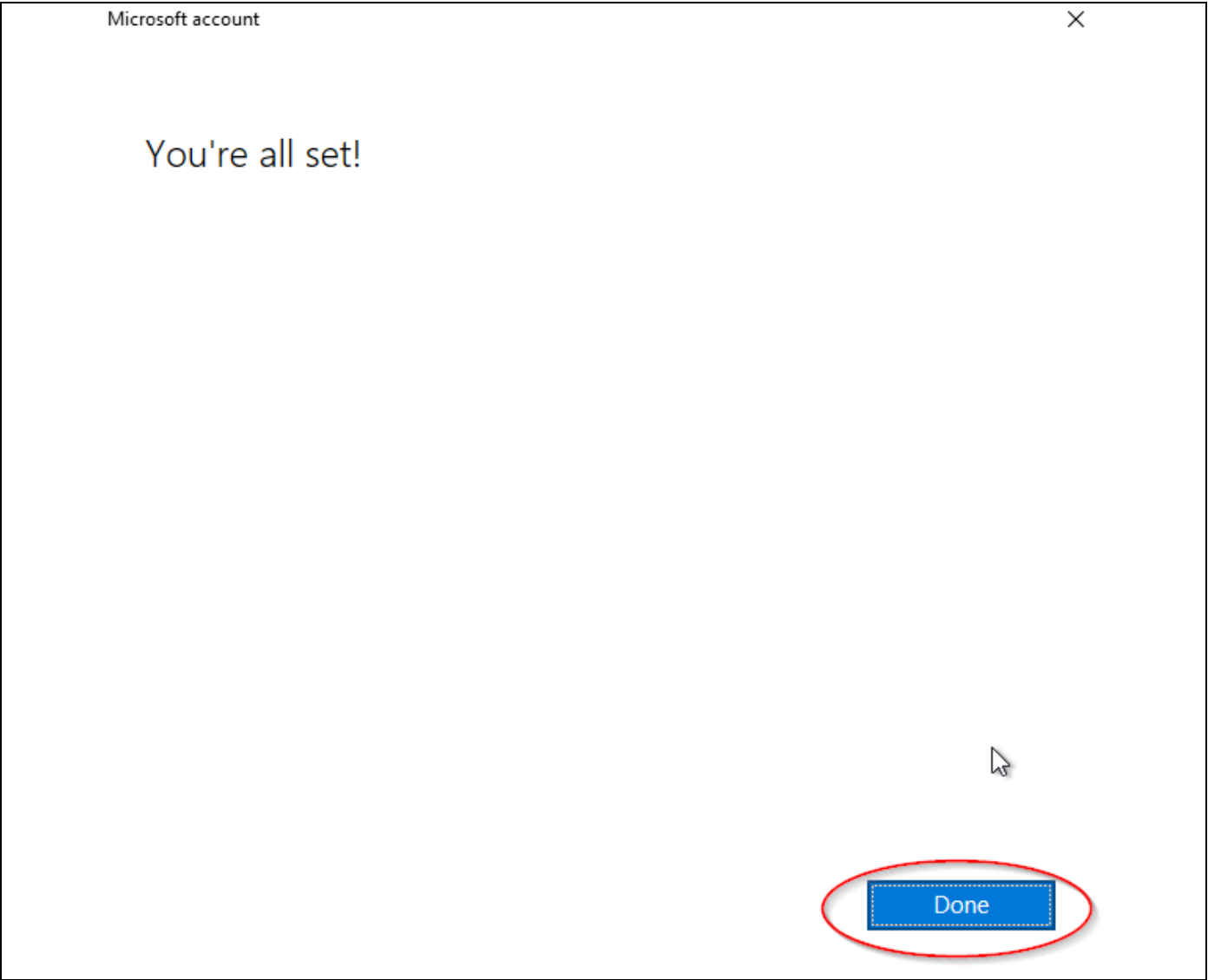
If you continue, system policies might be turned on or other changes might be made to your PC.  
Is this the right organization?

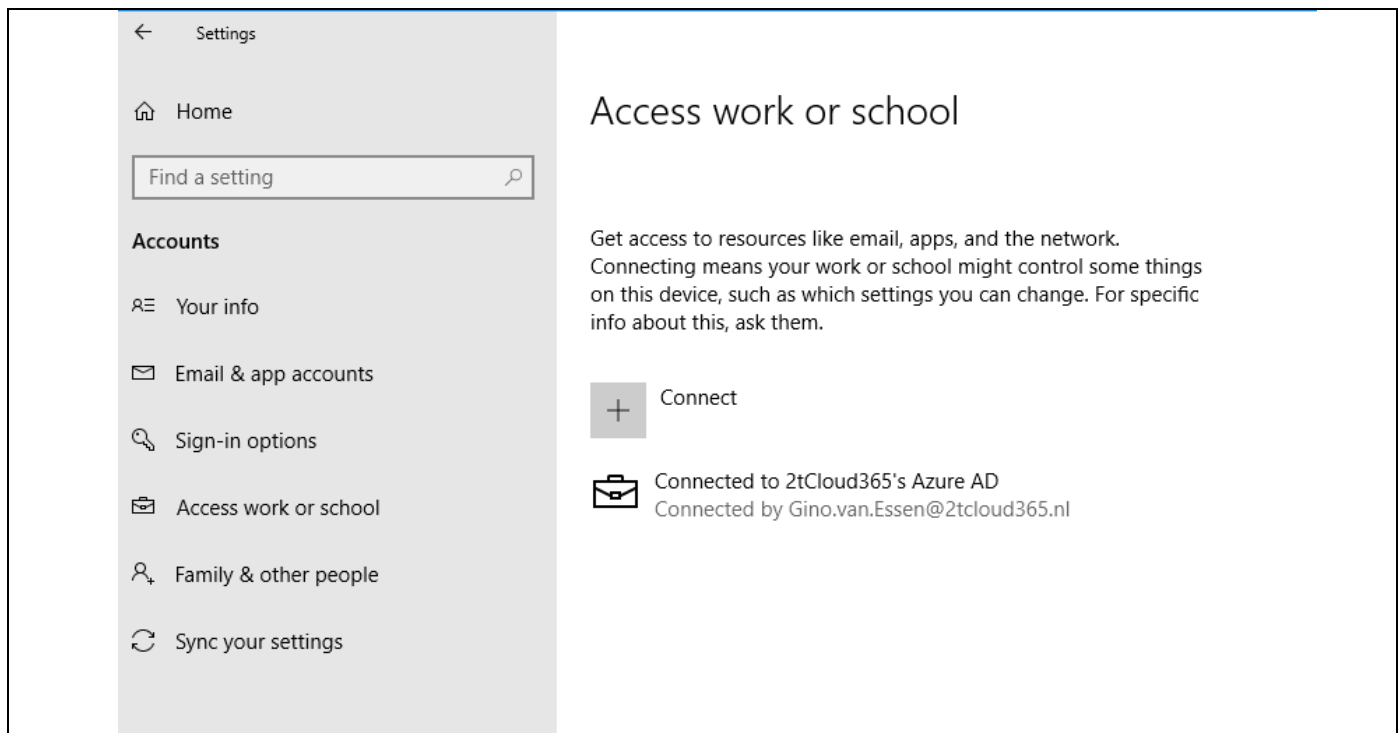
Connecting to: 2tcloud365.nl  
User name: Gino.van.Essen@2tcloud365.nl  
User type: Administrator

Cancel Join

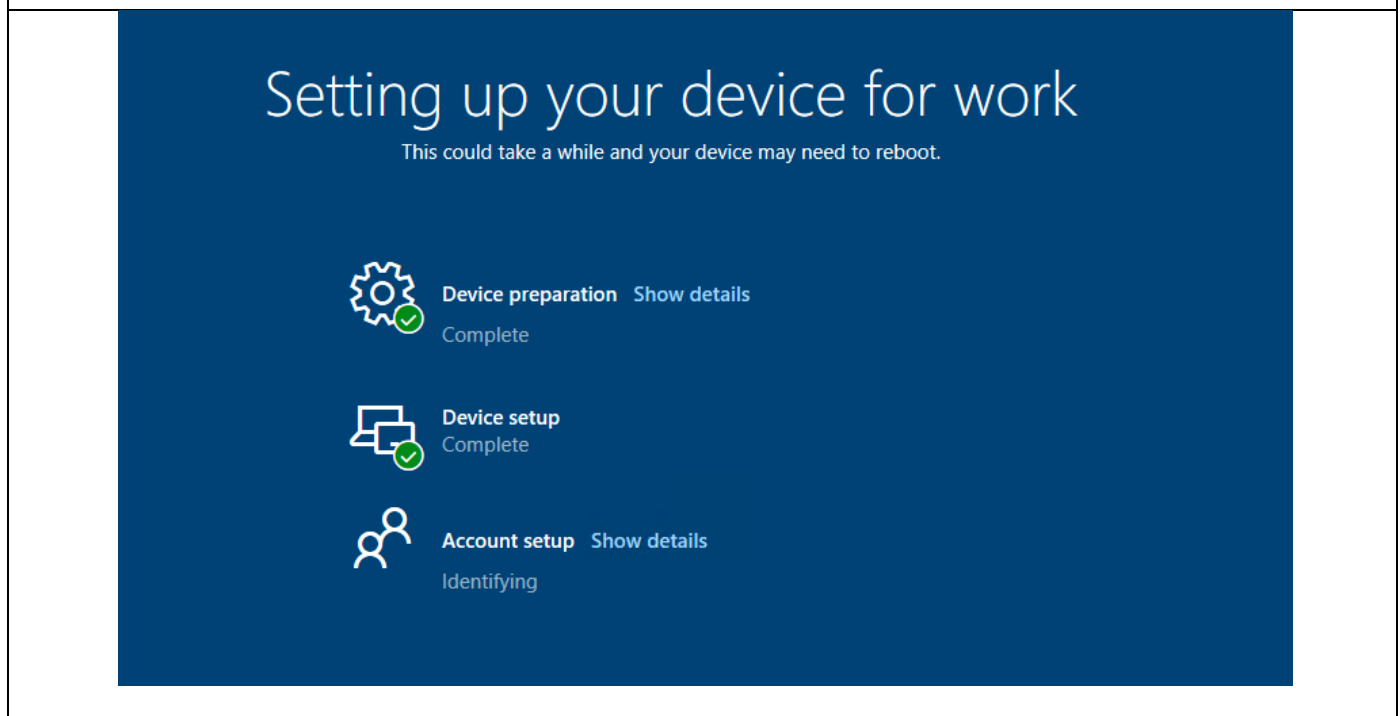


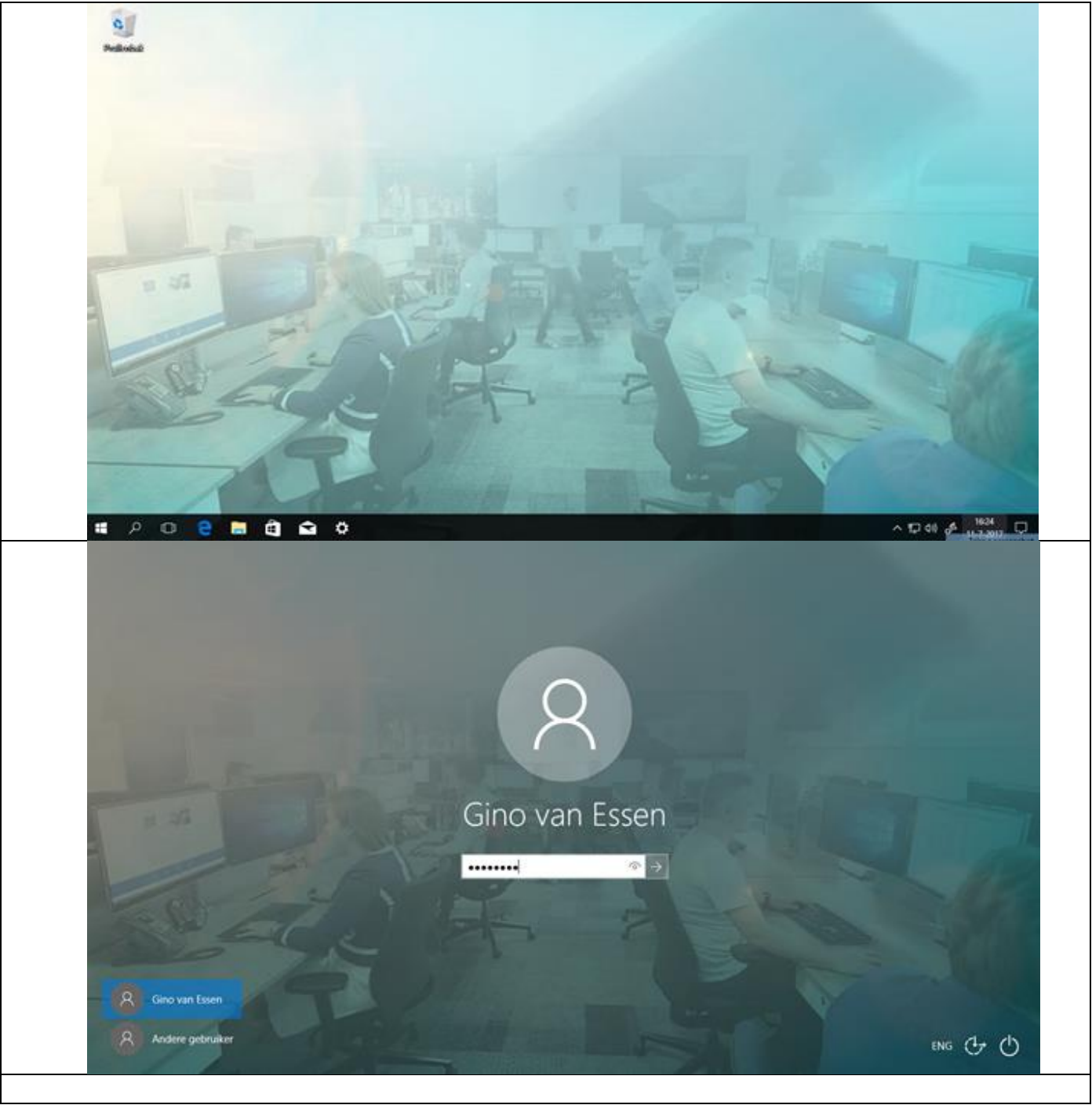






After reboot login with Azure AD account and credentials





## Activity 4: Configuration Intune

### 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
---	--

## Exercise 8: Device Settings

### 1. Go to Azure Active Directory ->Users and groups -> Device Settings;

Home > 2tCloud365 > Devices - Device settings

### Devices - Device settings

ZtCloud365 - Azure Active Directory

Manage

- All devices
- Device settings**
- Enterprise State Roaming

Activity

- Audit logs

Troubleshooting + Support

- Troubleshoot
- New support request

Save Discard

Users may join devices to Azure AD **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 **Selected** All None

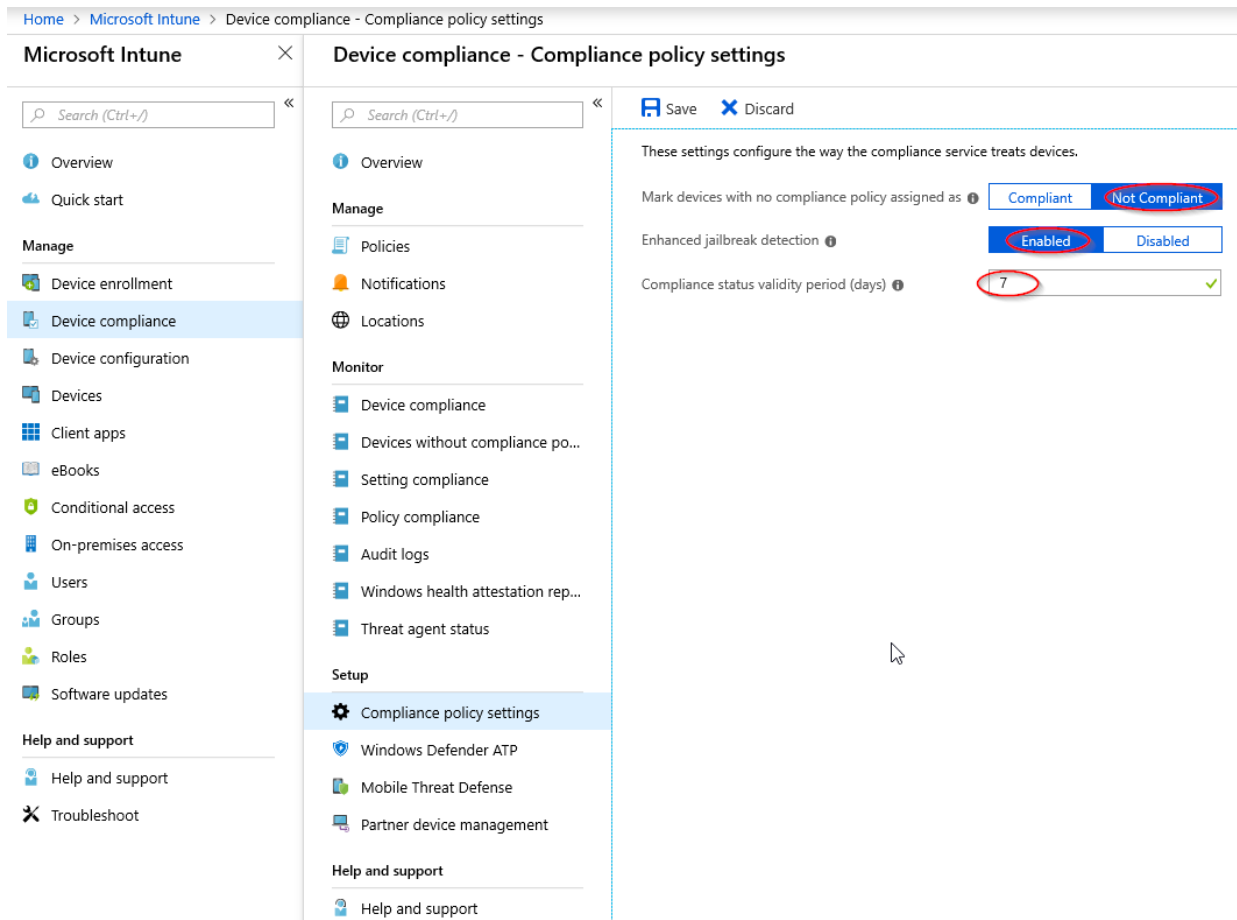
Selected  
1 member selected

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

Users may join devices to Azure AD	UG_Gebruikers_MDM
Additional local administrators on Azure AD Joined Devices	Selected -> Admin
Require Multi-Factor Auth to join devices	Yes
Maximum number of devices per user	5
Users may sync settings and enterprise app data	UG_Gebruikers_MDM

## Exercise 9: Device Compliance

### 1. Go to Intune->Device Compliance -> Compliance policy settings



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

Mark devices with no compliance	Not Compliant
Enhanced Jailbreak detection	Enabled
Compliance status validity period	7

1. 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

**Windows 10 compliance policy**

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

**System Security**

Windows 10 and later

**Password**

Require a password to unlock mobile devices. **Require** Not configured

Simple passwords **Block** Not configured

Password type **Alphanumeric**

Number of non-alphanumeric characters in password 1

Minimum password length Not configured

Maximum minutes of inactivity before password is required Not configured

Password expiration (days) Enter number of days (1-65535)

Number of previous passwords to prevent reuse Not configured

Require password when device returns from idle state (Mobile and Holographic) **Require** Not configured

**Encryption**

Encryption of data storage on device. **Require** Not configured

**Device Security**

Firewall **Require** Not configured

Antivirus **Require** Not configured

AntiSpyware **Require** Not configured

**Create** **OK** **OK**

2. Configure the settings >

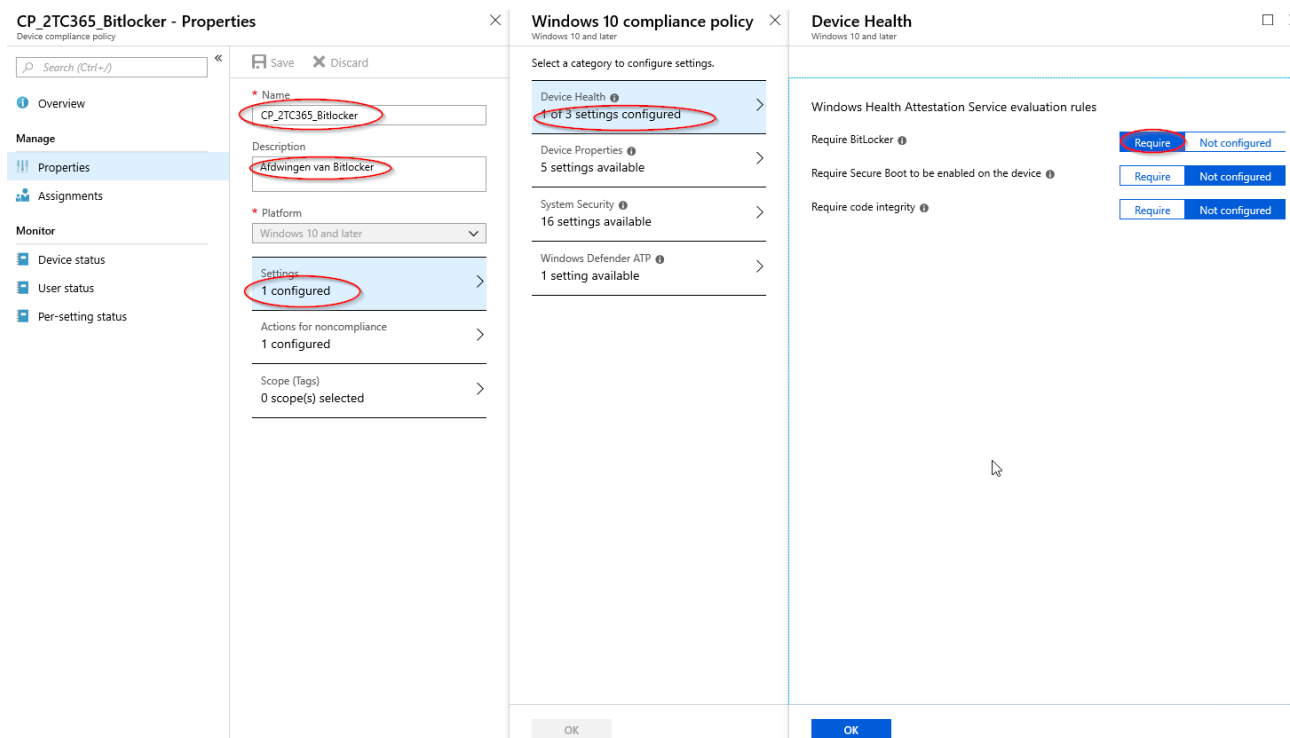
Name	CP_2tC365_PIN
Platform	Windows 10 and later

3. Click on **Configure**

4. Configure settings as showed on the screenshot -> Click **Create**



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



5. Configure the settings -> Click **Ok**

Name	CP_2TC365_Bitlocker
Description	Afdwingen van Bitlocker
Platform	Windows 10 and later

6. Click on **Configure**

7. Configure settings as showed on the screenshot -> Click **Save**

8. Go to Intune->Device Compliance->Policies-> **CP\_2TC365\_Bitlocker**-> Assignments-> Select groups;

**CP\_2TC365\_Bitlocker - Assignments** □ ×

Device compliance policy

Search (Ctrl+/) «

Save Discard Evaluate

Approximately 3 users will be impacted.

Include Exclude

Assign to  
Selected Groups

Select groups to include >

UG\_Gebruikers\_MDM ...

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Per-setting status

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

Groups	UG_Gebruikers_MDM
--------	-------------------

Go to Intune->Device Compliance -> Policies-> **CP\_2tC365\_PIN** -> Assignments-> Select groups;

**CP\_2TC365\_PIN - Assignments** □ ×

Device compliance policy

Search (Ctrl+/) «

Save Discard Evaluate

Include Exclude

Assign to  
Selected Groups

Select groups to include >

UG\_Gebruikers\_MDM ...

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

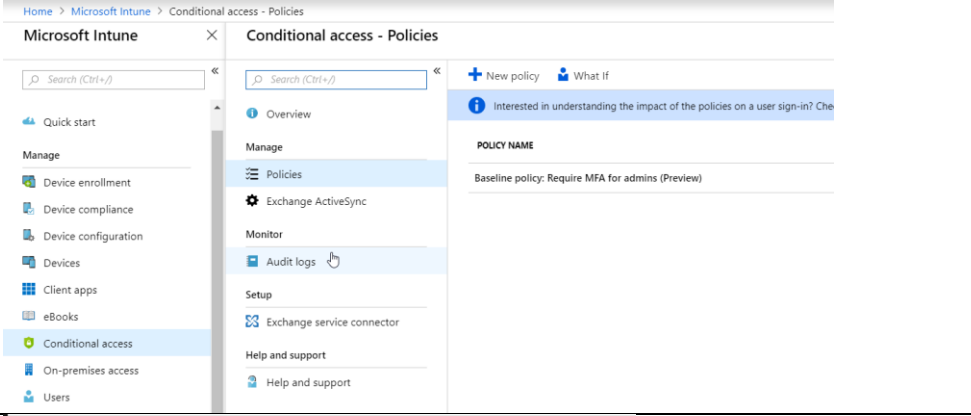
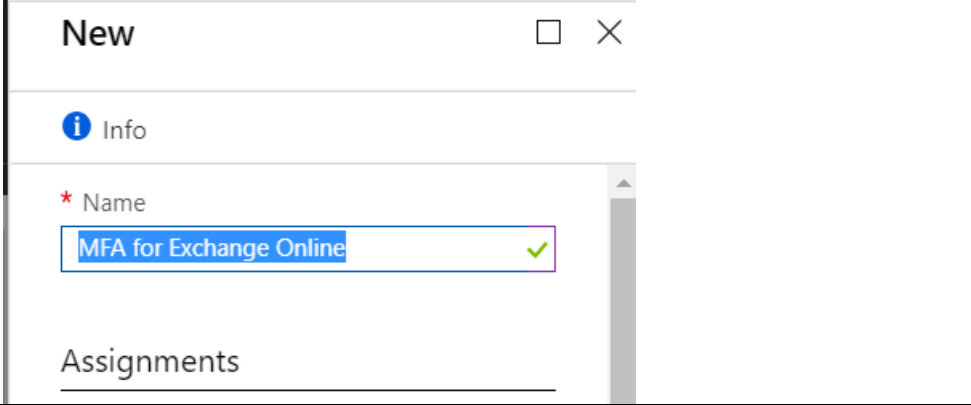
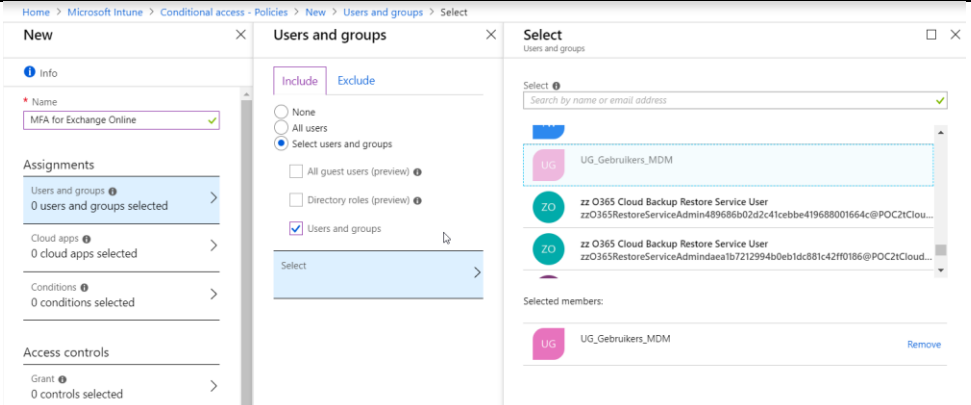
Per-setting status

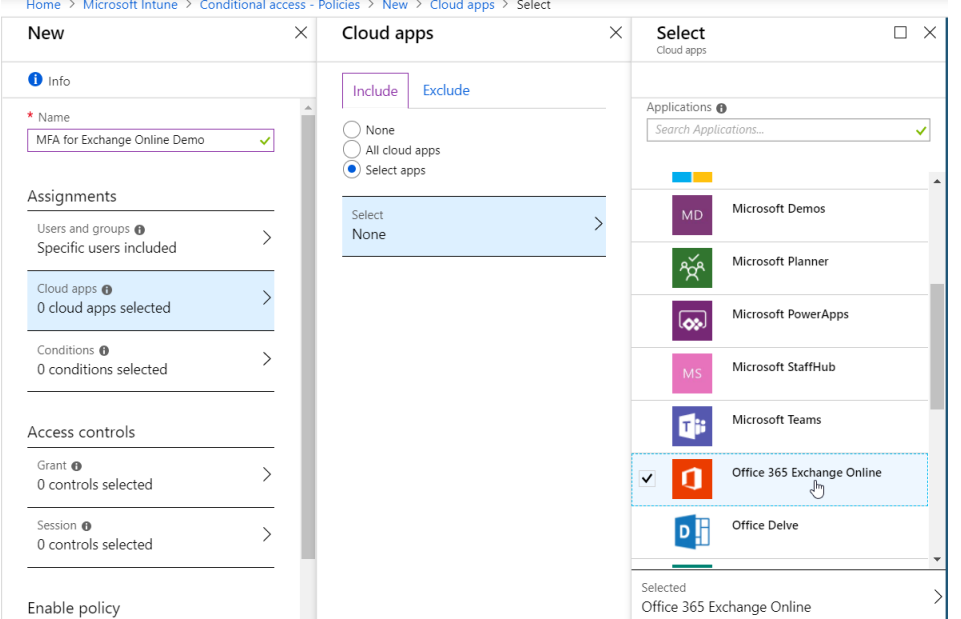
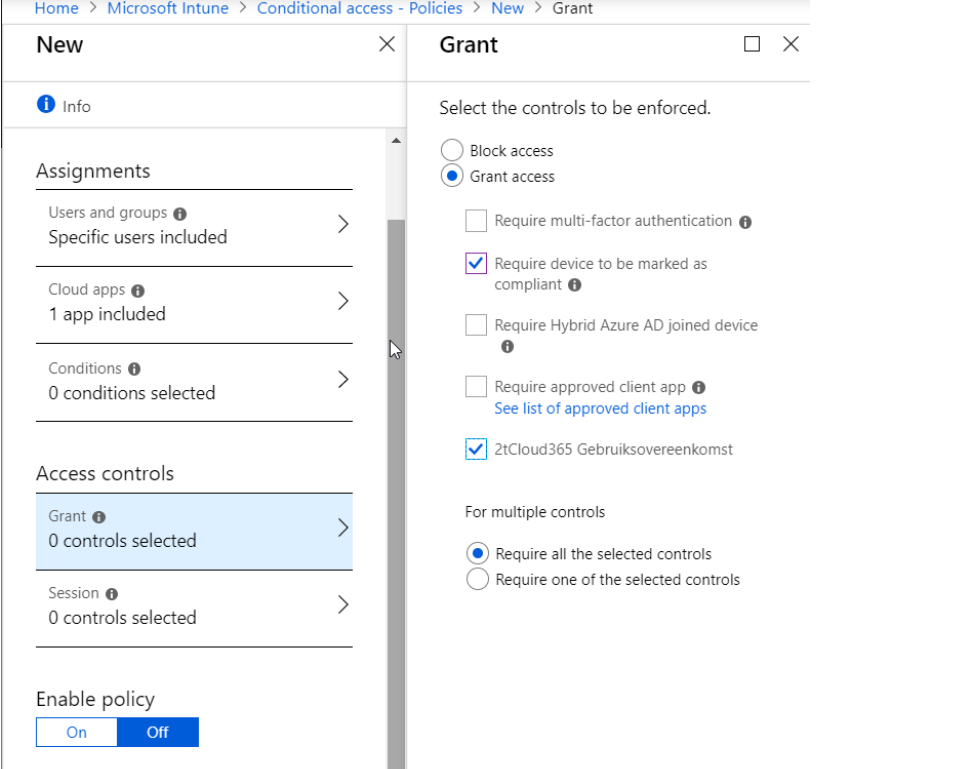
10. Configure the settings > Click **Save**

Groups	UG_Gebruikers_MDM
--------	-------------------

## Exercise 10: Conditional Access

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

<ol style="list-style-type: none"> <li>Go to Microsoft Intune → Conditional access and select New Policy</li> </ol>	
<ol style="list-style-type: none"> <li>Give the policy a name: MFA for Exchange Online</li> </ol>	
<ol style="list-style-type: none"> <li>Select Users and groups</li> <li>Select: Select users and Groups</li> <li>Check Users and groups</li> <li>Select the group "UG_Gebruikers_MDM"</li> </ol>	

<p>7. Select Cloud apps</p> <p>8. Check Selects apps</p> <p>9. From the select menu find and check Office 365 Exchange Online</p> <p>10. Choose Done</p>	
<p>11. Under Access controls select Grant</p> <p>12. Here you select Grant access and you check Require device to be marked as compliant, and the Terms of use</p>	

1. Enable the policy and click on Create

Access controls

Grant ⓘ  
2 controls selected

Session ⓘ  
0 controls selected

Enable policy

On

Off

Create

## Exercise 10a: Device Configuration - Windows Device Restrictions

### 1. Go to Intune->Device Configuration-> Profiles-> Create Profile;

**Windows 10 Device Restrictions - Properties**

Device configuration profile

Search (Ctrl+/)

Save Discard

**Overview**

**Manage**

- Properties
- Assignments

**Monitor**

- Device status
- User status
- Per-setting status

**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

**General**

Windows 10 and later

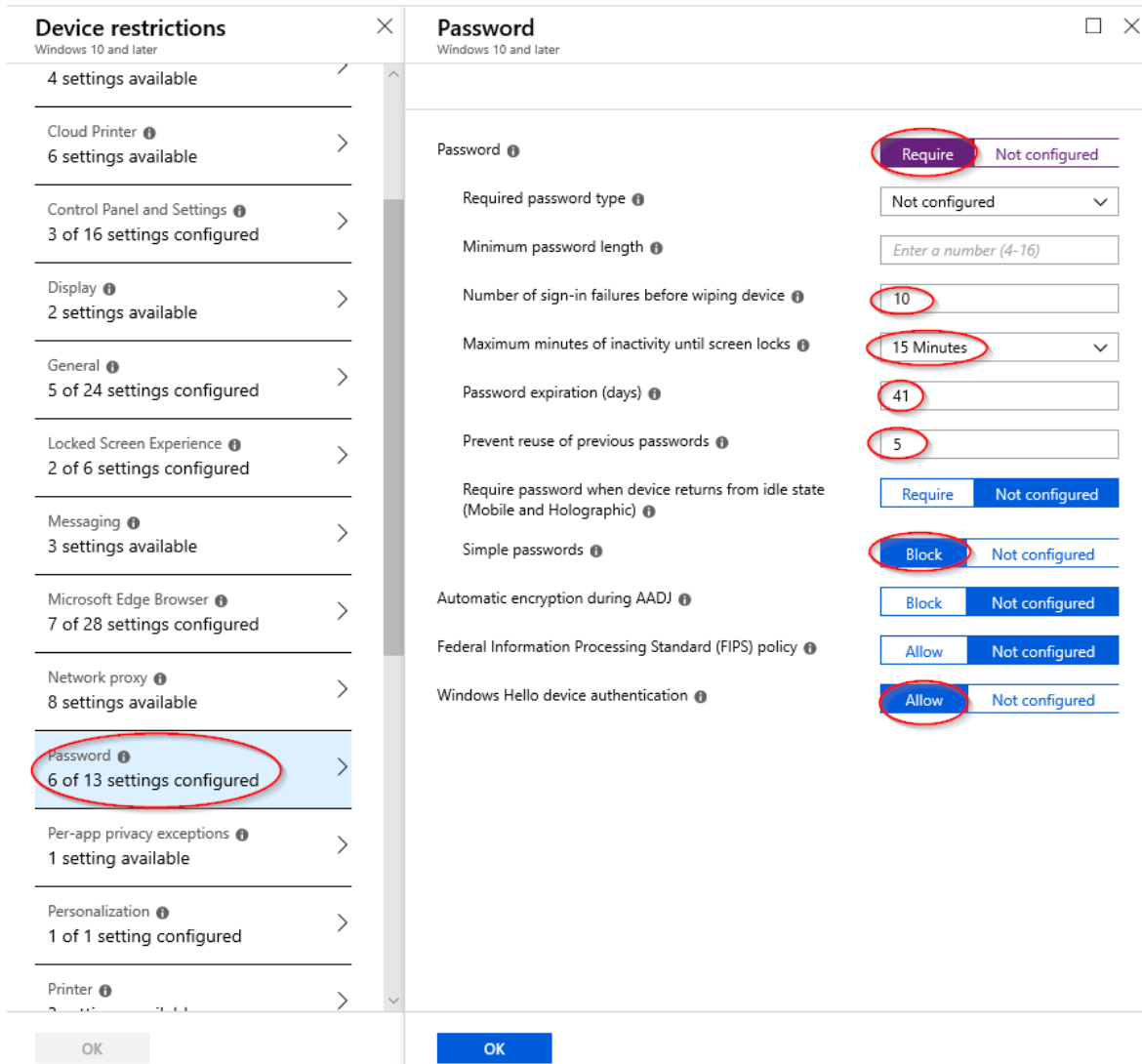
- Screen capture (mobile only) Block Not configured
- Copy and paste (mobile only) Block Not configured
- Manual unenrollment Block Not configured
- Manual root certificate installation (mobile only) Block Not configured
- Camera Block Not configured
- OneDrive file sync Block Not configured
- Removable 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

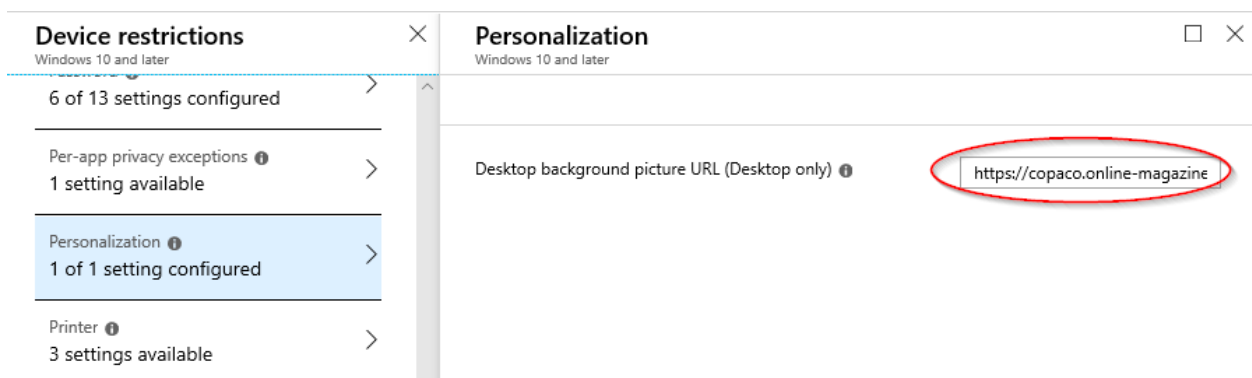
### 2. Configure the settings >

Name	Windows 10 – Device Restrictions
Platform	Windows 10 and later
Profile type	Device restrictions

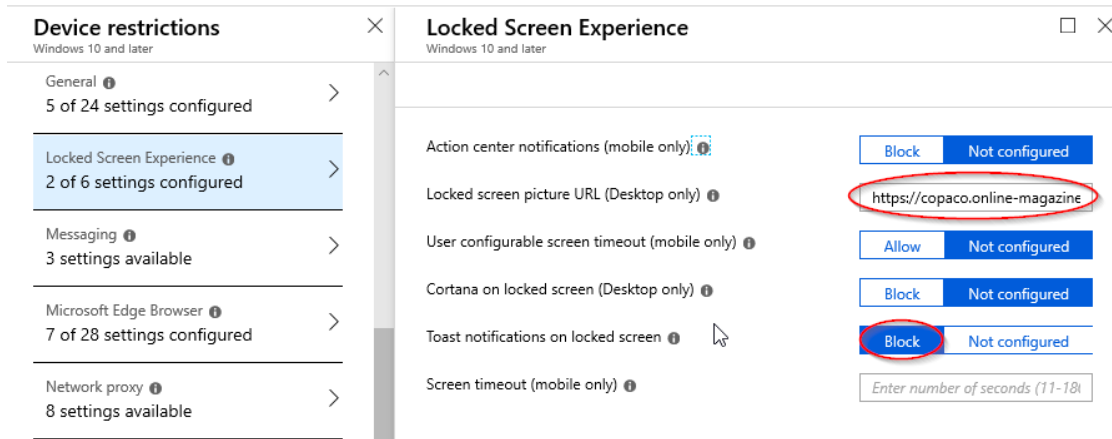
### 3. Configure settings as showed on the screenshot (General)



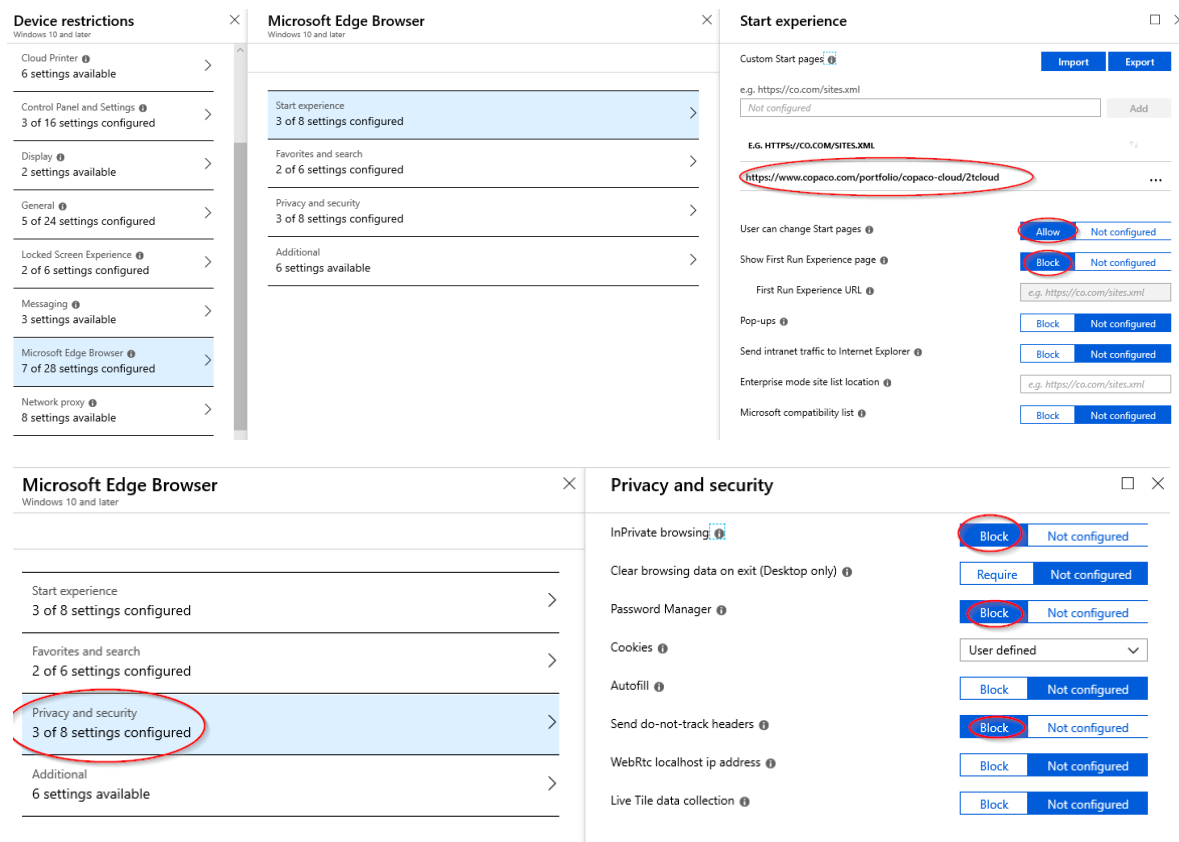
4. Configure settings as showed on the screenshot (Password)



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

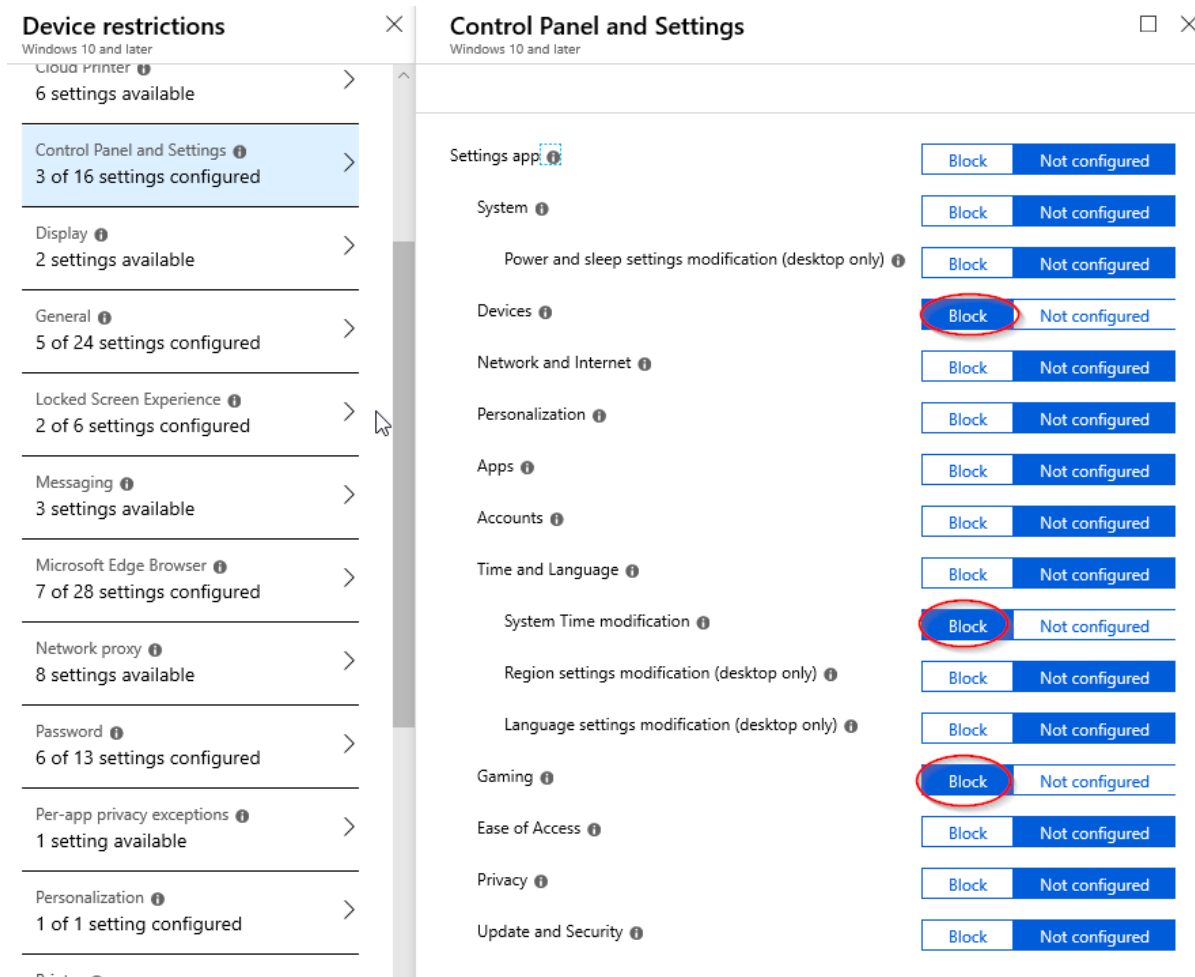


## 6. Configure settings as showed on the screenshot (Lock Screen Experience)

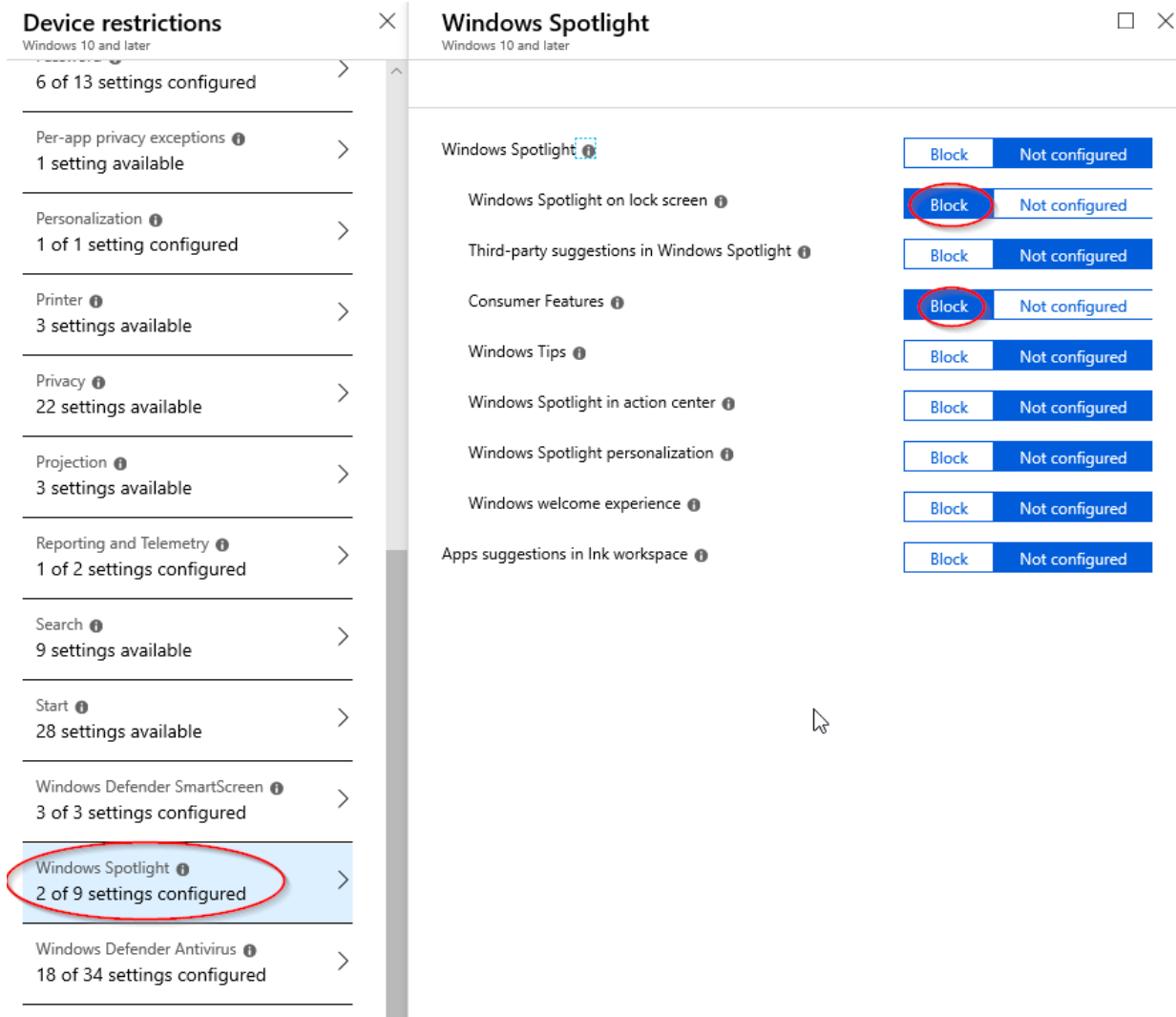


## 7. Configure settings as showed on the screenshots (Edge Browser)





8. Configure settings as showed on the screenshot (Control Panel and Settings)



9. Configure settings as showed on the screenshot (Windows Spotlight)

## Exercise 10b: Device Configuration - Windows Device Configuration

Go to Intune-> Device Configuration->Profiles-> Create Profile

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 Gaa...

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

Configure the settings > Click **Ok**

Name	Windows 10 Encryption
Description	Bitlocker settings for enrolled devices
Platform	Windows 10 and later
Profile type	Endpoint protection

1. Configure settings as showed on the screenshots (2)

## Exercise 11: 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**

Windows 10 Update Ring

Search (Ctrl+/)

Save Discard

**Overview**

**Manage**

Properties

Assignments

**Monitor**

Device status

User status

**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

OK

5. Assign the Windows 10 Update Ring to Group “UG\_Gebruikers\_MDM”

### Windows 10 CBB Update Ring - Assignments

Windows 10 Update Ring

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Save Discard Evaluate

Include Exclude

Assign to

Selected Groups

Select groups to include

UG\_Gebruikers\_MDM

## Exercise 12: Office ProPlus Deployment via Intune

Go to **Microsoft Intune -> Client Apps -> Apps**

Try to create the Office365 Proplus App and assign it to group **UG\_Gebruikers\_MDM**

1. Add a App with App type "Windows 10"
2. Configure the settings
3. 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

### 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

Search (Ctrl+J)

Save Discard

Overview

manage

Properties

Assignments

monitor

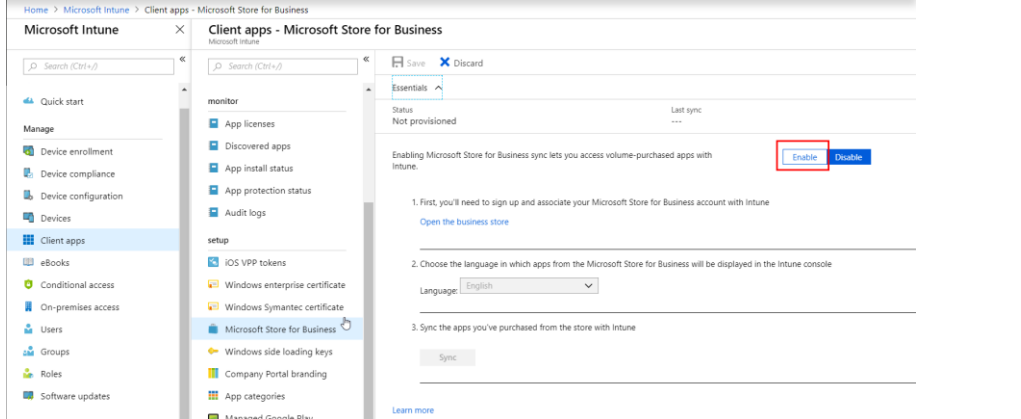
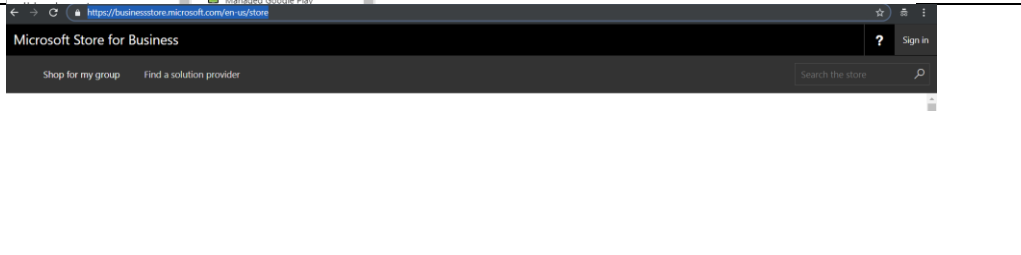
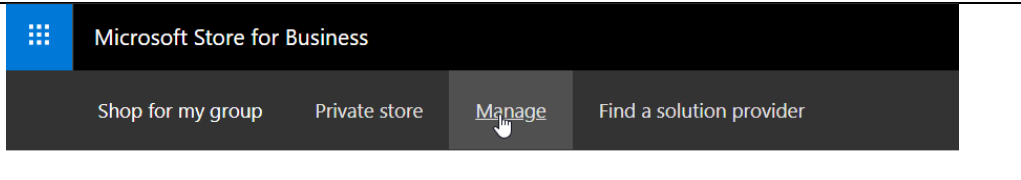
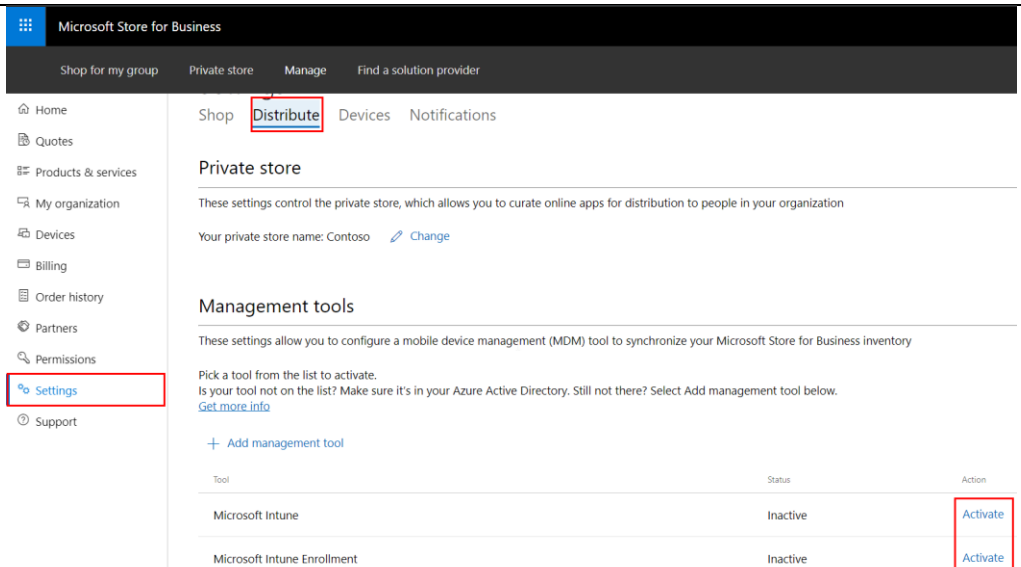
Device install status

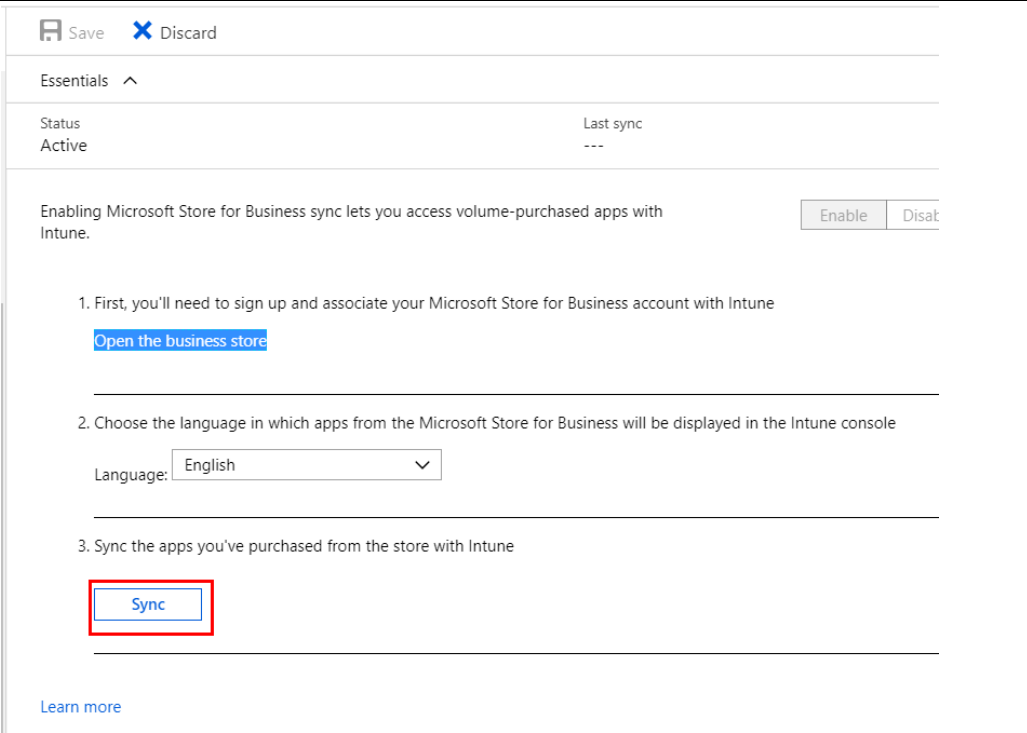
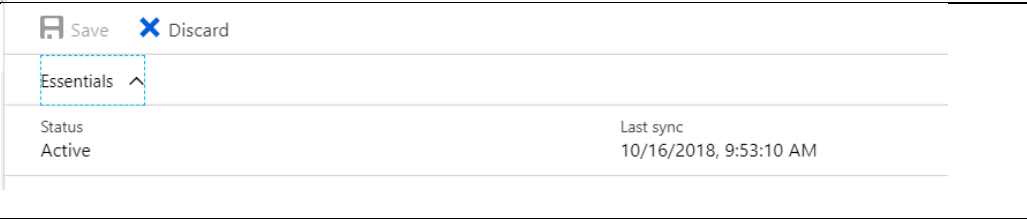
User install status

Add group

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			

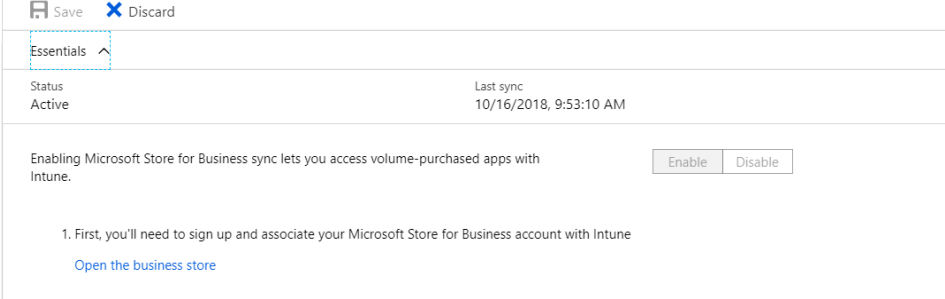
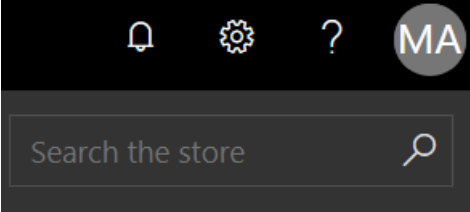
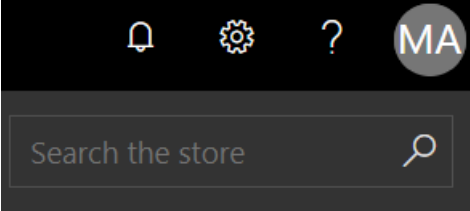
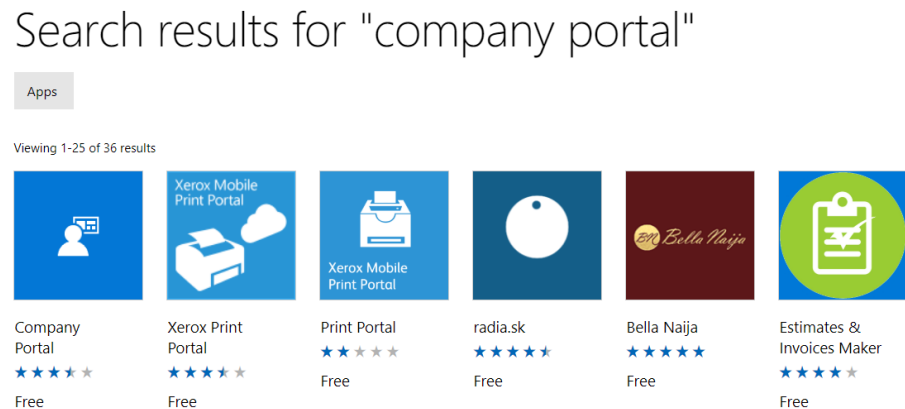
## Exercise 13: Windows Store for Business

<p>Go to Microsoft Intune → Client Apps → Microsoft store for Business</p> <p>1. There you select Enable and press Save</p>	
<p>2. After that you can select the link open</p> <p>3. Sign in with your AAD account</p>	
<p>4. Once your signed in select manage</p> <p>5. Accept any terms and license agreements</p>	
<p>Go to settings → Distribute</p> <p>6. Activate Microsoft Intune and Microsoft Intune Enrollment</p>	




<p>7. Go back to the Intune Portal and Select Sync</p>	 <p>The screenshot shows the Intune Essentials page. At the top, there are 'Save' and 'Discard' buttons. Below them is the 'Essentials' section with a dropdown arrow. The status is 'Active' and the last sync is '---'. A message states: 'Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune.' There are 'Enable' and 'Disable' buttons. A list of steps follows: 1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune. A link 'Open the business store' is provided. 2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console. A dropdown menu shows 'English'. 3. Sync the apps you've purchased from the store with Intune. The 'Sync' button is highlighted with a red box. A 'Learn more' link is at the bottom.</p>
<p>8. The syncing process can take a while. But when completed you should see the last time it was successfully synced</p>	 <p>The screenshot shows the Intune Essentials page. At the top, there are 'Save' and 'Discard' buttons. Below them is the 'Essentials' section with a dropdown arrow. The status is 'Active' and the last sync is '10/16/2018, 9:53:10 AM'.</p>
<p>9. At this point you can deploy apps from the Windows Store for Business</p>	

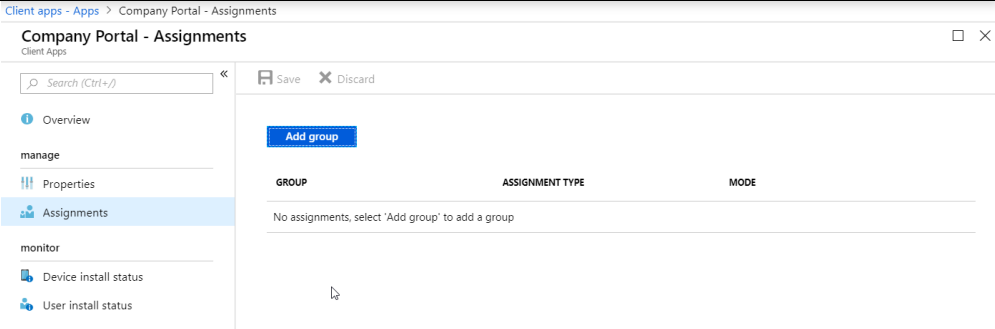
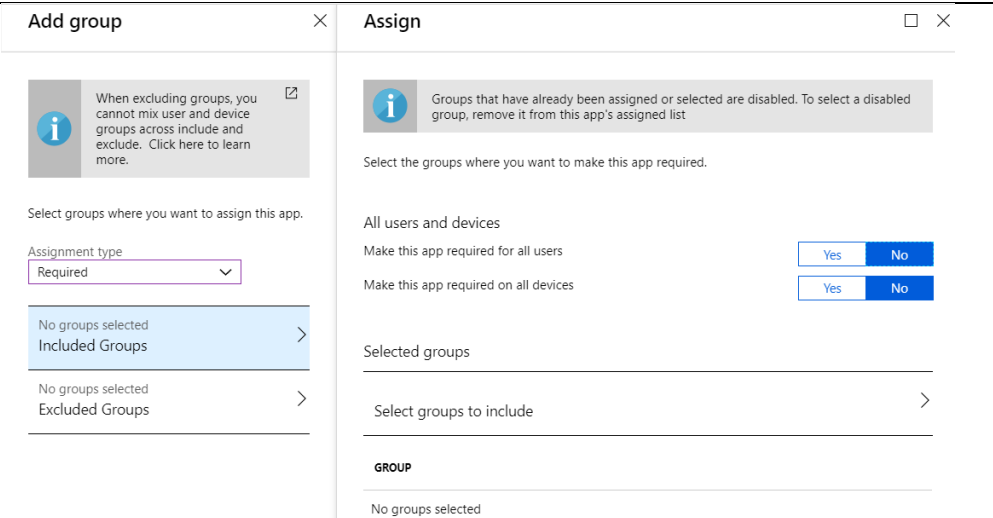
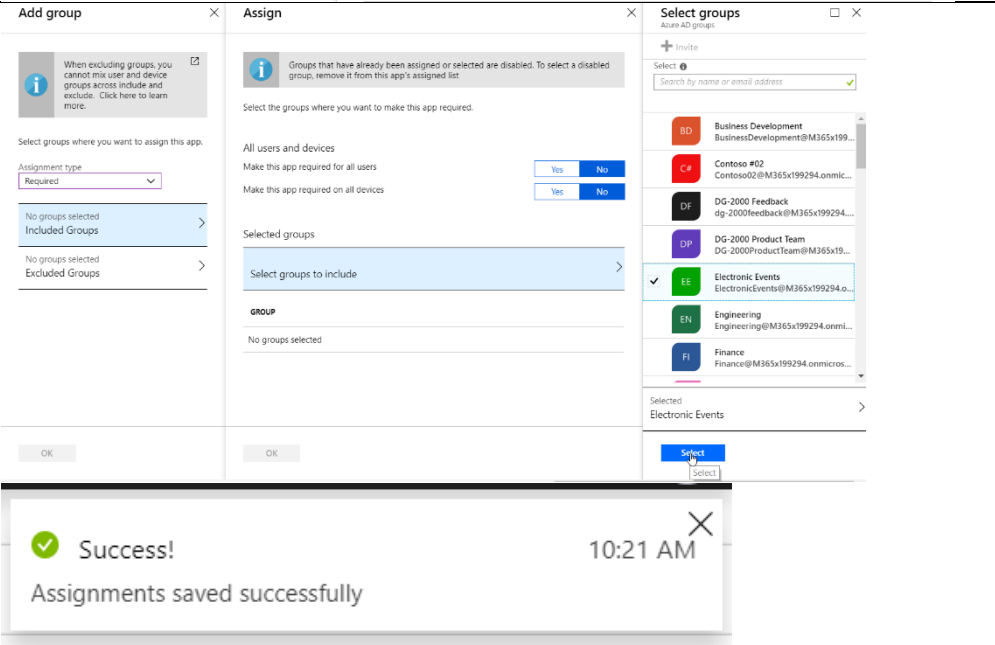
## Exercise 14: Company portal

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

<p>Go to Microsoft Intune → Client Apps → Microsoft store for Business</p> <p>1. Select open the business store</p>	
<p>2. Check if you are signed in. If not sign in with your account</p>	
<p>3. Use the search bar to search for company portal (bedrijfs portaal)</p>	
<p>4. Select Company Portal</p>	

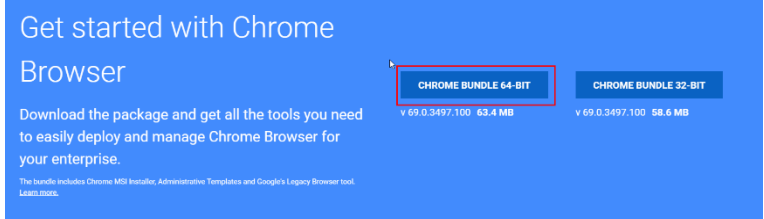
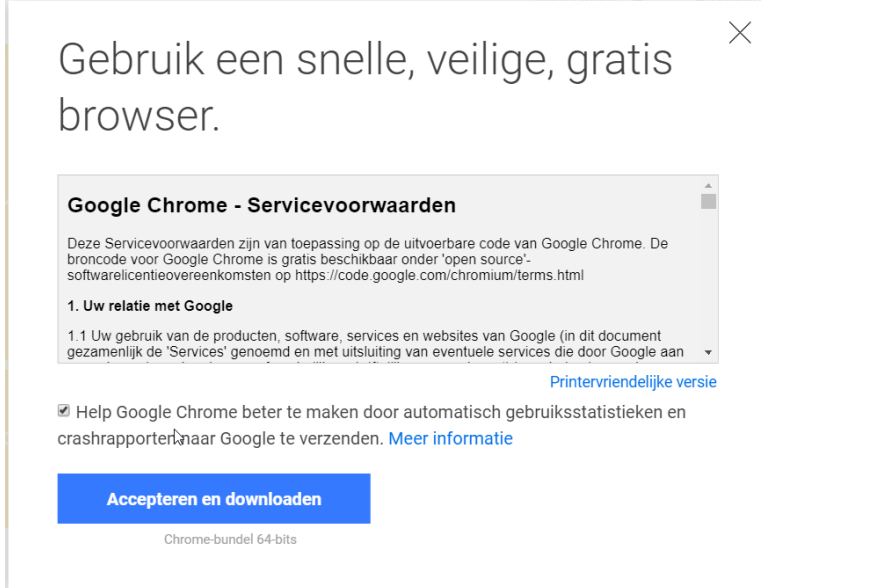
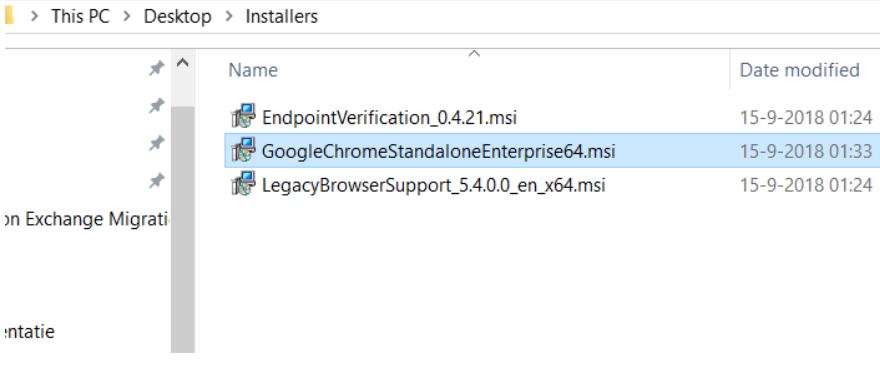
5. Select Get the app	
6. Accept the agreement	<p>Review and accept the services agreement to sign up for the Microsoft Store for Bu</p>

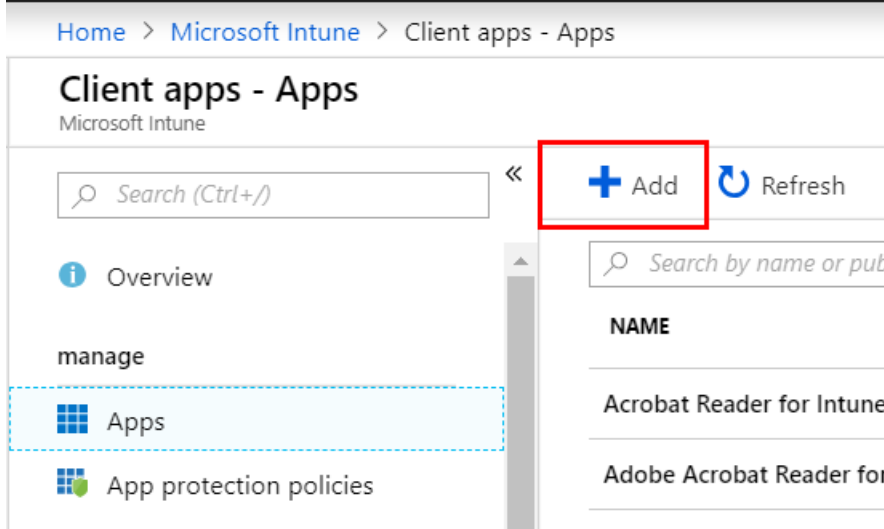
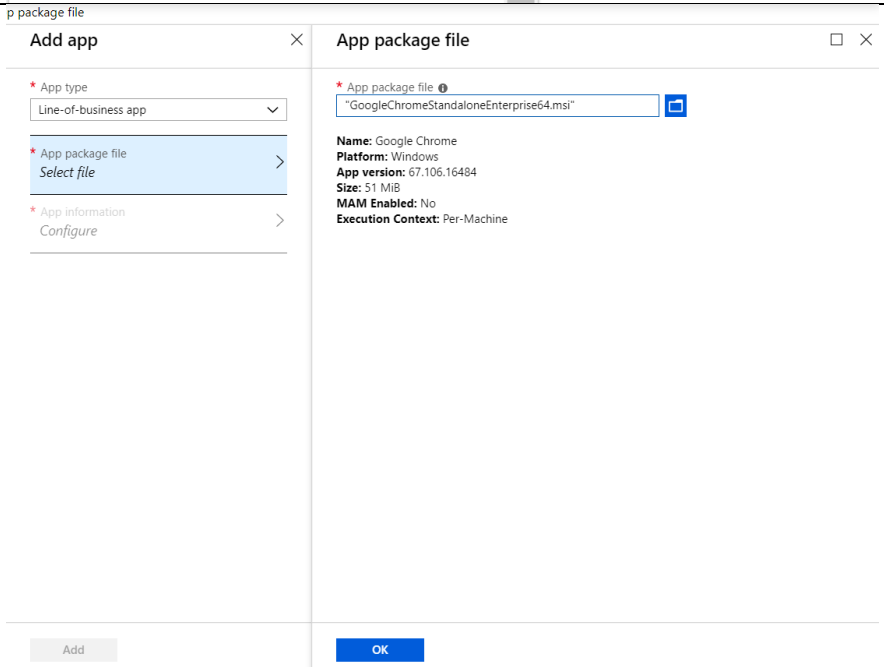
<p>7. After that the app is added</p>	<div data-bbox="555 367 841 409">Thanks for your order</div> <div data-bbox="616 490 691 564"></div> <div data-bbox="694 495 1099 557">Company Portal has been purchased and added to your inventory.</div> <div data-bbox="976 978 1034 1008">Close</div>
<p>8. Go back to the Intune Portal and Select Sync</p>	<div data-bbox="561 1061 746 1090"> Save  Discard</div> <div data-bbox="561 1113 667 1137">Essentials ^</div> <div data-bbox="561 1158 616 1202">Status Active</div> <div data-bbox="1102 1158 1176 1196">Last sync ---</div> <div data-bbox="561 1243 1198 1290">Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune.</div> <div data-bbox="1345 1247 1482 1272"><div>Enable</div><div>Disat</div></div> <div data-bbox="598 1335 1311 1361">1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune</div> <div data-bbox="616 1370 798 1397"><a href="#">Open the business store</a></div> <div data-bbox="598 1453 1441 1480">2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console</div> <div data-bbox="616 1496 967 1532">Language: <div>English</div></div> <div data-bbox="598 1576 1046 1603">3. Sync the apps you've purchased from the store with Intune</div> <div data-bbox="652 1635 697 1659"><div>Sync</div></div> <div data-bbox="561 1736 651 1760"><a href="#">Learn more</a></div>

<p>After the sync is completed go to Microsoft Intune → Client apps – Apps</p> <p>There you should find The company portal. Note that the Type is Microsoft Store for Business app</p> <p>9. Select Company Portal and click on Assignments</p>	
<p>10. Select Add group</p> <p>11. On Assignment Type choose required</p> <p>12. Then select group and select the MDM group that you have created.</p>	
<p>13. Then select group and select the MDM group that you have created.</p> <p>14. Then click OK</p> <p>15. Then Click OK again</p> <p>16. Click Save</p>	



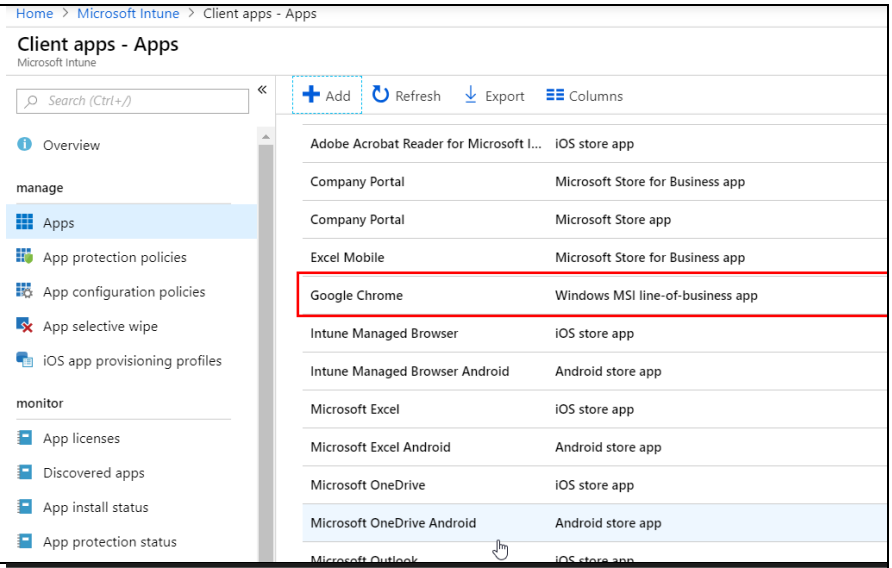
## Exercise 15: MSI app deployment

<p>Go to <a href="https://enterprise.google.com/chrome/chrome-browser/">https://enterprise.google.com/chrome/chrome-browser/</a></p> <ol style="list-style-type: none"> <li>1. Search the page for Chrome Bundle 64-bit</li> </ol>	
<ol style="list-style-type: none"> <li>2. Accept and download the MSI</li> </ol>	
<ol style="list-style-type: none"> <li>3. This will download a zip file</li> <li>4. Extract the files to your desktop</li> <li>5. There you can find the GoogleChromeStandAloneEnterprise64.msi</li> </ol> <p>Desktop\Installers\GoogleChromeStandAloneEnterprise64.msi</p>	

<p>Go to portal.office.com</p> <p>Choose Microsoft Intune → Client Apps → Apps</p> <p>1. Select Add</p>	 <p>Home &gt; Microsoft Intune &gt; Client apps - Apps</p> <h2>Client apps - Apps</h2> <p>Microsoft Intune</p> <p>Search (Ctrl+/) &lt;&lt; <b>+ Add</b> Refresh</p> <p>Overview</p> <p>manage</p> <p><b>Apps</b></p> <p>App protection policies</p> <p>Search by name or pub</p> <p>NAME</p> <p>Acrobat Reader for Intune</p> <p>Adobe Acrobat Reader for</p>
<p>2. At App Type choos Line-of-business app</p> <p>3. At App package file select GoogleChromeStandaloneEnterprise64.msi from your desktop and click OK</p>	 <p>App package file</p> <h3>Add app</h3> <p>* App type Line-of-business app</p> <p>* App package file Select file</p> <p>* App information Configure</p> <p>Add</p> <h3>App package file</h3> <p>* App package file</p> <p>"GoogleChromeStandaloneEnterprise64.msi"</p> <p>Name: Google Chrome Platform: Windows App version: 67.106.16484 Size: 51 MiB MAM Enabled: No Execution Context: Per-Machine</p> <p>OK</p>

<p>4. Select App information</p> <p>5. Enter a Description</p> <p>6. Enter a Publisher</p> <p>7. Select OK</p> <p>8. Select ADD</p>	<div> <div> Add app </div> <div> <div> <div>* App type</div> <div>Line-of-business app</div> </div> <div> <div>* App package file</div> <div>GoogleChromeStandaloneEnterp...</div> </div> <div> <div>* App information</div> <div>Configure</div> </div> </div> <div> <div>Add</div> </div> </div> <div> <div> App information </div> <div> <div> <div>* Name</div> <div>Google Chrome</div> </div> <div> <div>* Description</div> <div>Google Chrome</div> </div> <div> <div>* Publisher</div> <div>Google</div> </div> <div> <div>* App install context</div> <div>Device context</div> </div> <div> <div>Ignore app version</div> <div> <div>Yes</div> <div>No</div> </div> </div> <div> <div>Category</div> <div>0 selected</div> </div> <div> <div>Display this as a featured app in the Company Portal</div> <div> <div>Yes</div> <div>No</div> </div> </div> <div> <div>Information URL</div> <div>Enter a valid url</div> </div> <div> <div>Privacy URL</div> <div>Enter a valid url</div> </div> </div> <div> <div>OK</div> </div> </div>
---	--

10. After Chrome is reader you need to select the app



Home > Microsoft Intune > Client apps - Apps

### Client apps - Apps

Microsoft Intune

Search (Ctrl+/)

+ Add Refresh Export Columns

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

Overview

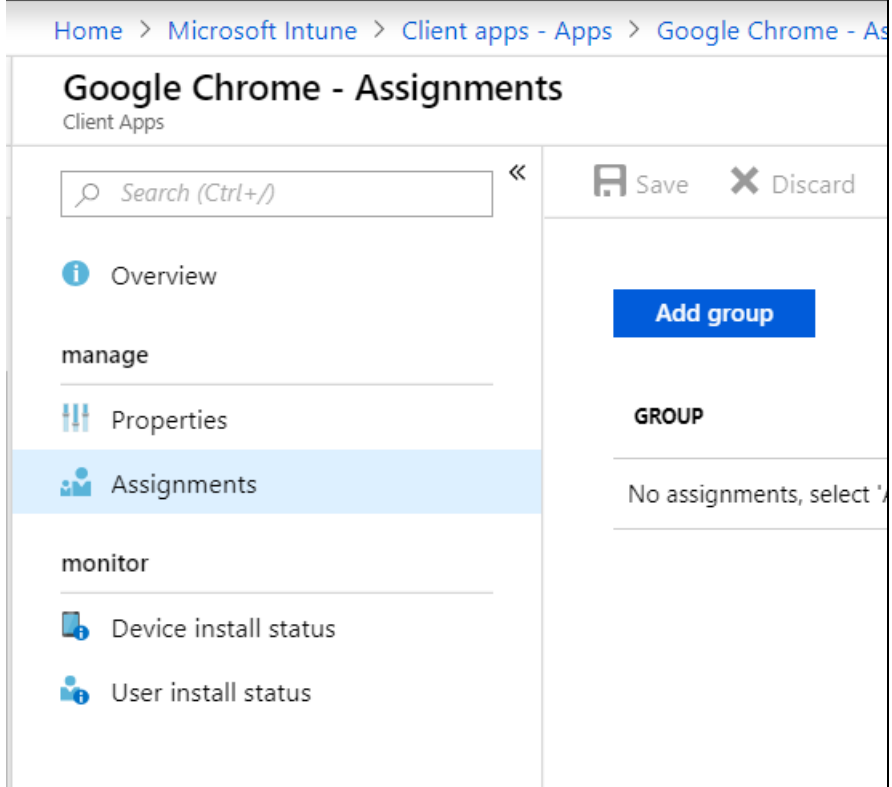
manage

- Apps
- App protection policies
- App configuration policies
- App selective wipe
- iOS app provisioning profiles

monitor

- App licenses
- Discovered apps
- App install status
- App protection status

11. Select Assignments and add group



Home > Microsoft Intune > Client apps - Apps > Google Chrome - As

### Google Chrome - Assignments

Client Apps

Search (Ctrl+/)

Save Discard

Overview

manage

- Properties
- Assignments

monitor

- Device install status
- User install status

**Add group**

**GROUP**

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

Invite

Select

Search by name or email address

BD

Business Development

Busi...Development@M365x199...

C#

Contoso #02

Contoso02@M365x199294.onmic...

DF

DG-2000 Feedback

dig-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...

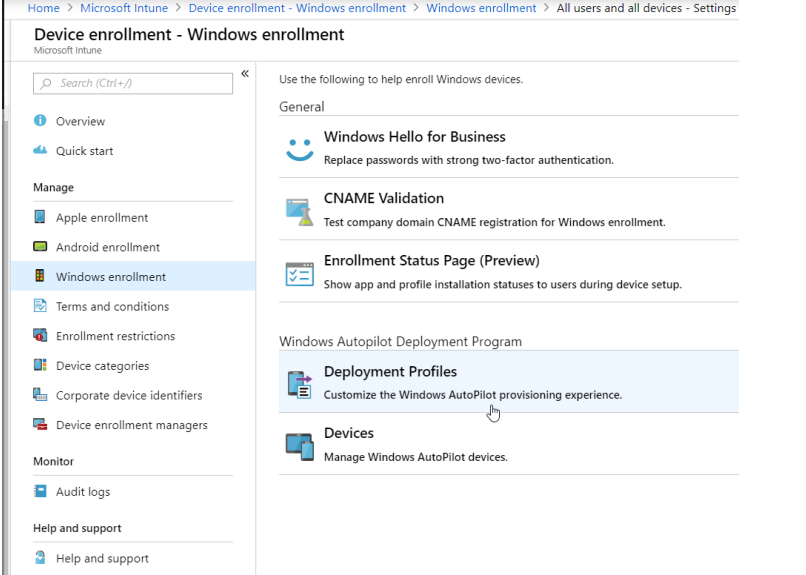
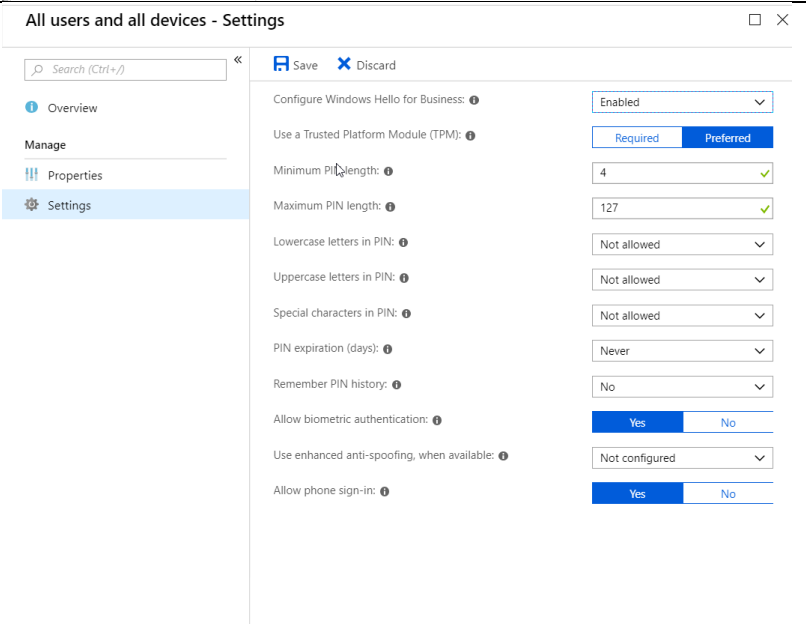
Selected

Business Development

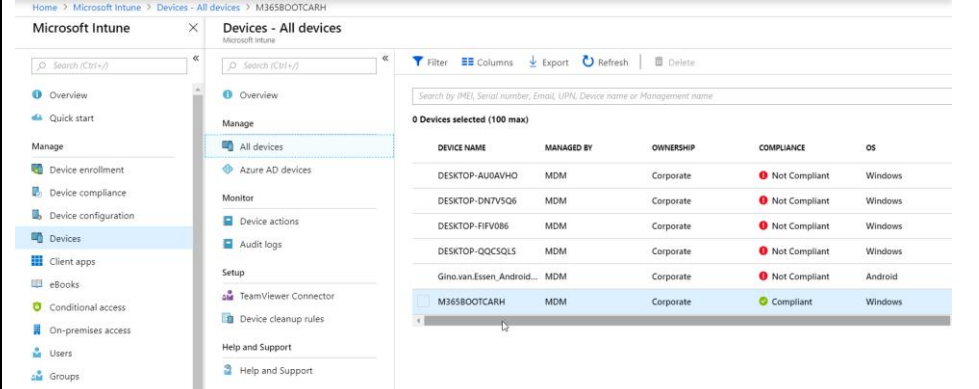
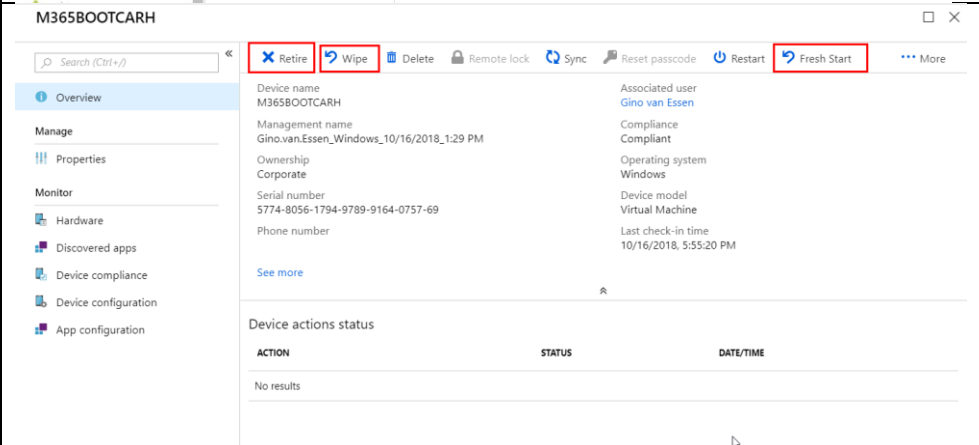
Select

## Exercise 16: Windows Hello

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

<p>Go to portal.azure.com and select Microsoft Intune.</p> <p>Then select Device Enrollment → Windows enrollment. There you can select Windows Hello For Business</p>	
<ol style="list-style-type: none"> <li>1. Select settings</li> <li>2. At Configure Windows for Business select Enabled.</li> <li>3. You can leave the default settings</li> <li>4. And select Save</li> </ol>	

## Activity 5: Selective Wipe

<p>Go to Microsoft Intune → Devices → All devices</p> <p>1. Here you can select the device that you want to wipe</p>	 <p>Microsoft Intune - Devices - All devices</p> <p>0 Devices selected (100 max)</p> <table><tr><th>DEVICE NAME</th><th>MANAGED BY</th><th>OWNERSHIP</th><th>COMPLIANCE</th><th>OS</th></tr><tr><td>DESKTOP-AUGAVHO</td><td>MDM</td><td>Corporate</td><td>Not Compliant</td><td>Windows</td></tr><tr><td>DESKTOP-DNTV5Q6</td><td>MDM</td><td>Corporate</td><td>Not Compliant</td><td>Windows</td></tr><tr><td>DESKTOP-FIFV086</td><td>MDM</td><td>Corporate</td><td>Not Compliant</td><td>Windows</td></tr><tr><td>DESKTOP-QQC5QL5</td><td>MDM</td><td>Corporate</td><td>Not Compliant</td><td>Windows</td></tr><tr><td>Gino.van.Essen_Android...</td><td>MDM</td><td>Corporate</td><td>Not Compliant</td><td>Android</td></tr><tr><td><b>M365BOOTCARH</b></td><td><b>MDM</b></td><td><b>Corporate</b></td><td><b>Compliant</b></td><td><b>Windows</b></td></tr></table>	DEVICE NAME	MANAGED BY	OWNERSHIP	COMPLIANCE	OS	DESKTOP-AUGAVHO	MDM	Corporate	Not Compliant	Windows	DESKTOP-DNTV5Q6	MDM	Corporate	Not Compliant	Windows	DESKTOP-FIFV086	MDM	Corporate	Not Compliant	Windows	DESKTOP-QQC5QL5	MDM	Corporate	Not Compliant	Windows	Gino.van.Essen_Android...	MDM	Corporate	Not Compliant	Android	<b>M365BOOTCARH</b>	<b>MDM</b>	<b>Corporate</b>	<b>Compliant</b>	<b>Windows</b>
DEVICE NAME	MANAGED BY	OWNERSHIP	COMPLIANCE	OS																																
DESKTOP-AUGAVHO	MDM	Corporate	Not Compliant	Windows																																
DESKTOP-DNTV5Q6	MDM	Corporate	Not Compliant	Windows																																
DESKTOP-FIFV086	MDM	Corporate	Not Compliant	Windows																																
DESKTOP-QQC5QL5	MDM	Corporate	Not Compliant	Windows																																
Gino.van.Essen_Android...	MDM	Corporate	Not Compliant	Android																																
<b>M365BOOTCARH</b>	<b>MDM</b>	<b>Corporate</b>	<b>Compliant</b>	<b>Windows</b>																																
<p>2. On the overview page you can find Retire, Wipe and Fresh Start.</p> <p>3. You can click on them to read what they will do.</p> <p>4. For demonstrating purposes you can choose Retire.</p>	 <p>Microsoft Intune - M365BOOTCARH</p> <p>Overview</p> <p>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: [redacted] 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</p> <p>Device actions status</p> <table><tr><th>ACTION</th><th>STATUS</th><th>DATE/TIME</th></tr><tr><td colspan="3">No results</td></tr></table>	ACTION	STATUS	DATE/TIME	No results																															
ACTION	STATUS	DATE/TIME																																		
No results																																				
<p>5. Go back to your test device and monitor any changes</p>																																				

**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>