



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

Document Revision	2
Change Record	2
Introduction	5
Objectives	5
Student Materials	5
Activity 1: Getting Started.....	6
Objectives	6
Exercise 1a: Create Windows 10 Enterprise VM	6
Exercise 1b OPTIONAL : Create Windows 10 PRO VM in Azure.....	8
Activity 2: Prepare Modern workplace with Intune	13
Exercise 2: Create an AAD Group.....	13
Exercise 2a: Configure group-based Licensing	14
Exercise 3: Configure MDM and MAM Intune settings	15
Exercise 4: Activate Self Service Password Reset	16
Exercise 5: Company branding.....	18
Activity 3: Add Windows to MDM	21
Exercise 6: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)	24
Exercise 6b – Hyper V Win10 VM	24
Exercise 6c Azure steps OPTIONAL	30
Activity 4: Configuration Intune.....	32
Exercise 7: Terms of use	54
Exercise 8: Device Settings.....	23
Exercise 9: Device Compliance	32
Exercise 10: Conditional Access.....	54
Exercise 10a: Device Configuration - Windows Device Restrictions.....	35
Exercise 10b: Device Configuration - Windows Device Configuration	39
Exercise 11: Windows 10 Update Rings.....	40
Exercise 12: Office ProPlus Deployment via Intune.....	41
Exercise 13: Windows Store for Business	43
Exercise 14: Company portal	45
Exercise 15: MSI app deployment	49

Exercise 16: Windows Hello 54

Activity 5: Selective Wipe 58

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

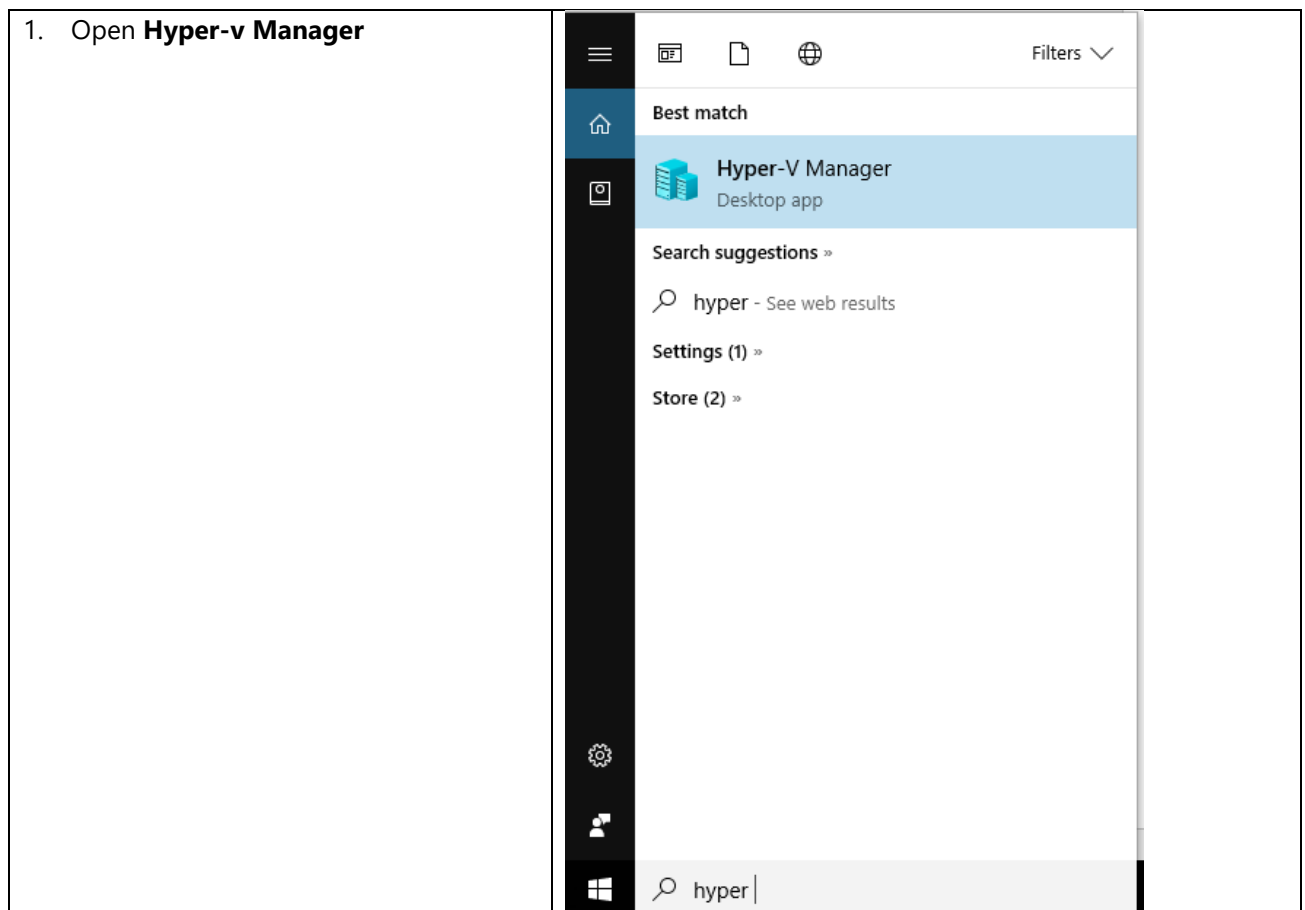
In this activity, you will configure the components necessary to perform this lab:

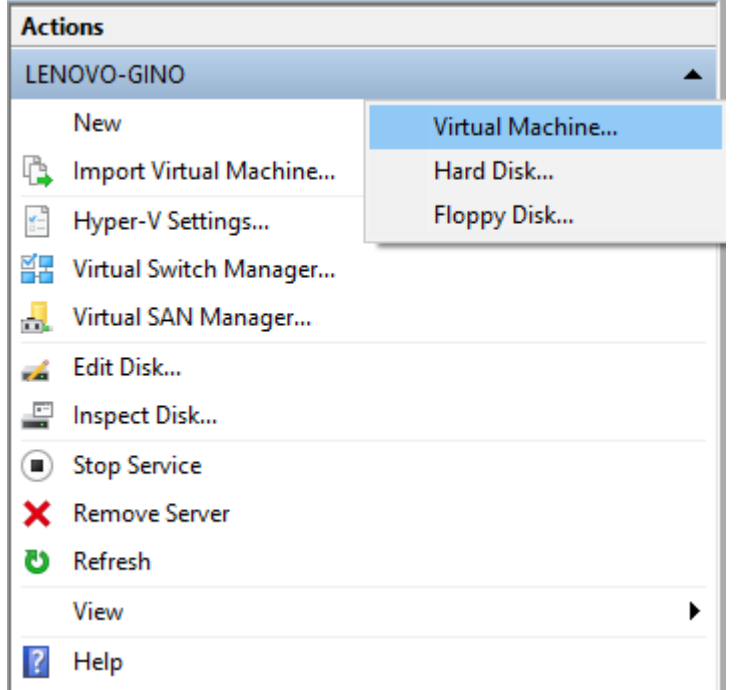
- Windows 10 Enterprise, version 1809 – Hyper-V

When Azure tenant \ subscription is not available

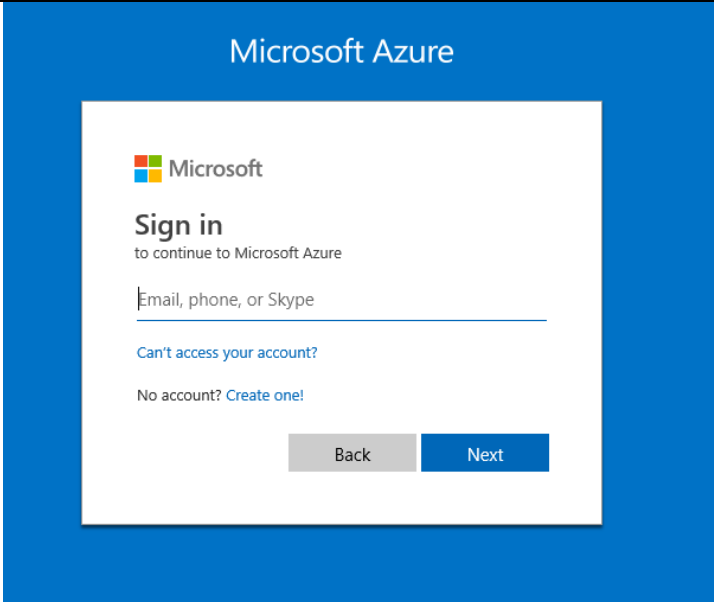
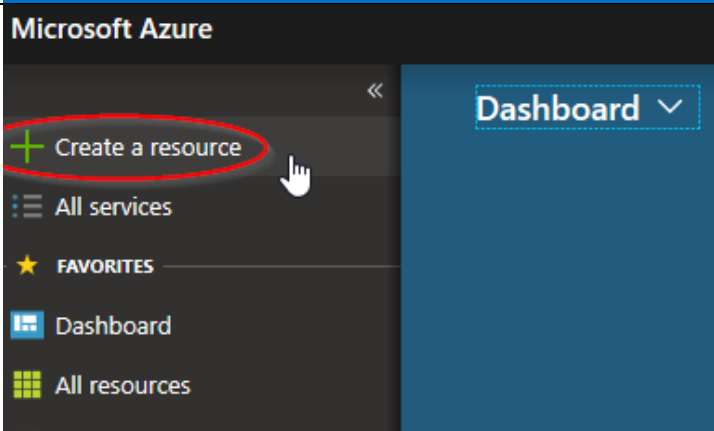
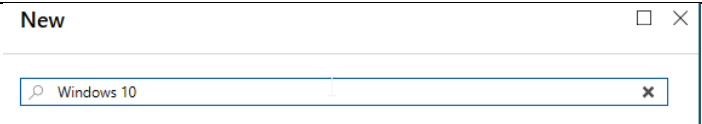

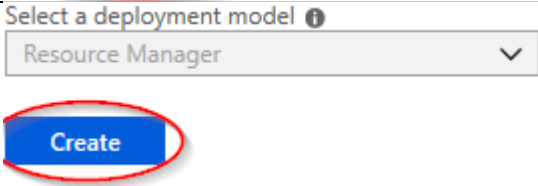
- ISO of Windows 10 Enterprise 1809 handed out by Copaco
- Hyper V Manager VM configuration

Exercise 1a: Create Windows 10 Enterprise VM

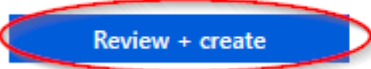


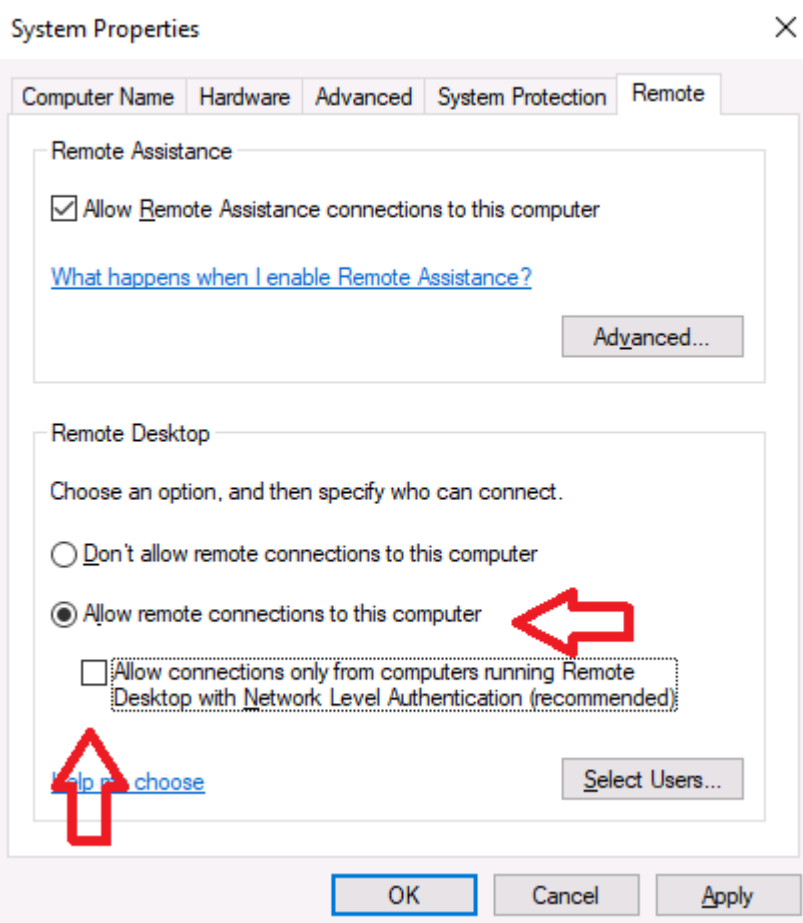
<ol style="list-style-type: none">2. Create New > virtual machine3. Name WIN10ENT-18034. Generation Generation 25. Assign Memory 4096 MB6. Configure Networking Connection External7. Create VHD Standard settings8. Installation Options install an OS from a bootable CD/DVD9. Image file: "Win10.iso"10. Finish / complete the configuration11. DO NOT START THE VM	 <p>Actions</p> <p>LENOVO-GINO ▲</p> <ul style="list-style-type: none">New<ul style="list-style-type: none">Virtual Machine...Hard Disk...Floppy Disk...Import Virtual Machine...Hyper-V Settings...Virtual Switch Manager...Virtual SAN Manager...Edit Disk...Inspect Disk...Stop ServiceRemove ServerRefreshView ►Help
--	--

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

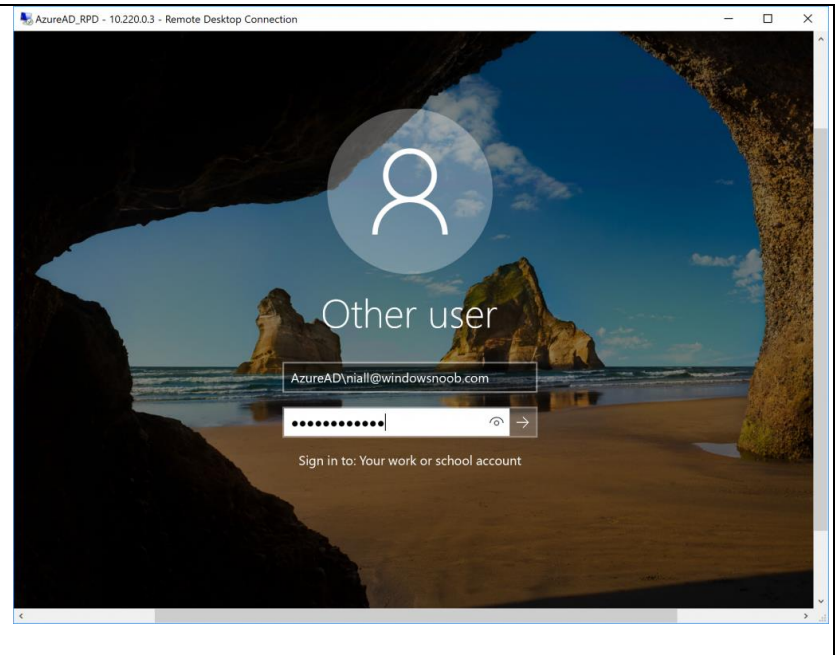
12. Go to https://portal.azure.com and login with your Azure AD Work account"																			
13. Create a resource																			
14. Search for "Windows 10"	 <table><tr><th>NAME</th><th>PUBLISHER</th><th>CATEGORY</th></tr><tr><td>Windows 10 Pro, Version 1709</td><td>Microsoft</td><td>Compute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

<ol style="list-style-type: none"> 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" 	<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 customization. Looking for classic VMs? Create VM from Azure Marketplace</p> <p>PROJECT DETAILS</p> <p>Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage resources.</p> <p>* Subscription Visual Studio Premium with MSDN</p> <p>* Resource group (New) M365HOL Create new</p> <p>INSTANCE DETAILS</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 Browse all images and disks</p> <p>* Size Standard D2s v3 2 vcpus, 8 GB memory Change size</p> <p>ADMINISTRATOR ACCOUNT</p> <p>* Username m365holadmin</p> <p>* Password </p> <p>* Confirm password </p>
<ol style="list-style-type: none"> 11. Go to tab "Networking" 12. Select "Allow selected ports" 13. Select Inbound ports "RDP (3389)" 	<h3>Create a virtual machine</h3> <p>Basics Disks Networking 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.</p> <p>NETWORK INTERFACE</p> <p>When creating a virtual machine, a network interface will be created for you.</p> <p>* Virtual network (new) M365HOL-vnet Create new</p> <p>* Subnet default</p> <p>Public IP (new) m365holwin10vm-ip Create new</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> <p>RDP</p> <p><input type="checkbox"/> HTTP (80)</p> <p><input type="checkbox"/> HTTPS (443)</p> <p><input type="checkbox"/> SSH (22)</p> <p><input checked="" type="checkbox"/> RDP (3389)</p> <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>	<p>Create a virtual machine</p> <p>✓ Validation passed</p> <p>Basics Disks Networking Management Guest config Tags Review + create</p> <p>PRODUCT DETAILS</p> <p>Microsoft Windows 10 by Microsoft Terms of use Privacy policy</p> <p>Standard D2s v3 by Microsoft Terms of use Privacy policy</p> <p>TERMS</p> <p>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.</p> <p>BASICS</p> <table border="0"> <tr> <td>Subscription</td> <td>Visual Studio Premium with MSDN</td> </tr> <tr> <td>Resource group</td> <td>(new) M365HOL</td> </tr> <tr> <td>Virtual machine name</td> <td>m365holwin10vm</td> </tr> <tr> <td>Region</td> <td>West Europe</td> </tr> <tr> <td>Availability options</td> <td>No infrastructure redundancy required</td> </tr> <tr> <td>Username</td> <td>m365holadmin</td> </tr> <tr> <td>Public inbound ports</td> <td>RDP</td> </tr> </table> <p>DISKS</p> <table border="0"> <tr> <td>OS disk type</td> <td>Premium SSD</td> </tr> </table> <p>Pricing not available for this offering</p> <p>Subscription credits apply ⓘ 0.1012 EUR/hr Pricing for other VM sizes</p> <p>Create Previous Next Download a template for automation</p>	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	OS disk type	Premium SSD
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																
OS disk type	Premium SSD																

<p>17. After the VM is ready log in to the VM</p> <p>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</p>	
<p>19. Log out of the VM</p> <p>20. Download the RDP file and save the file on your desktop</p> <p>21. Open the RDP file with Notepad.</p>	
<p>22. Add the following lines to the bottom</p> <p>23. Save the file</p> <p>24. Open to file to Remote desktop to the VM</p>	<pre>enablecredsspsupport:i:0 authentication level:i:2</pre>

25. You can now continue with Activity 2, Exercise 2. When you completed
26. At the login screen you need to use the following format to log in:
- AzureAD\<username@domain.com>**



Activity 2: Prepare Modern workplace with Intune

The most important components in this exercise are:



Azure Active Directory.



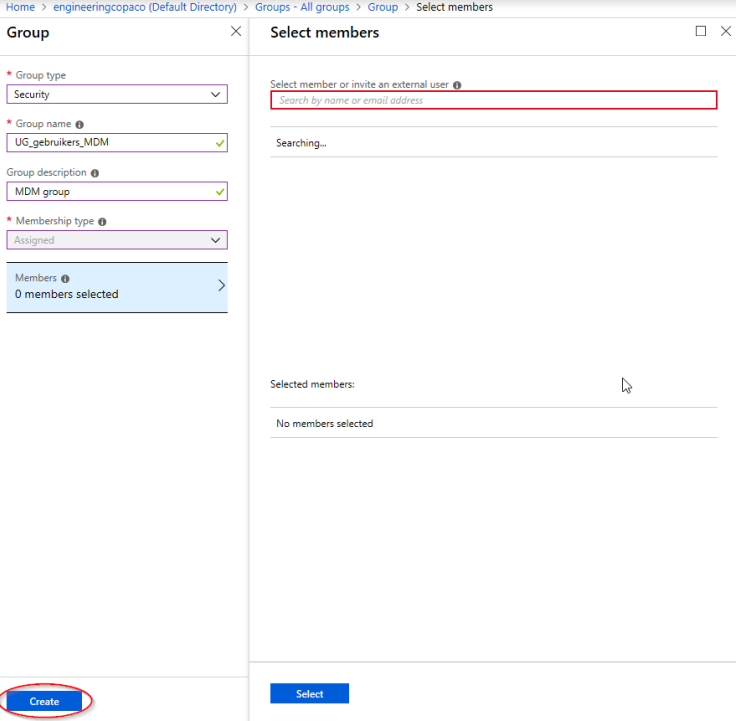
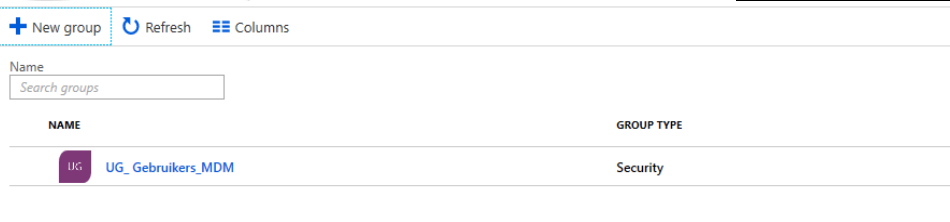
Users and Groups.



Intune.

Exercise 2: Create an AAD Group

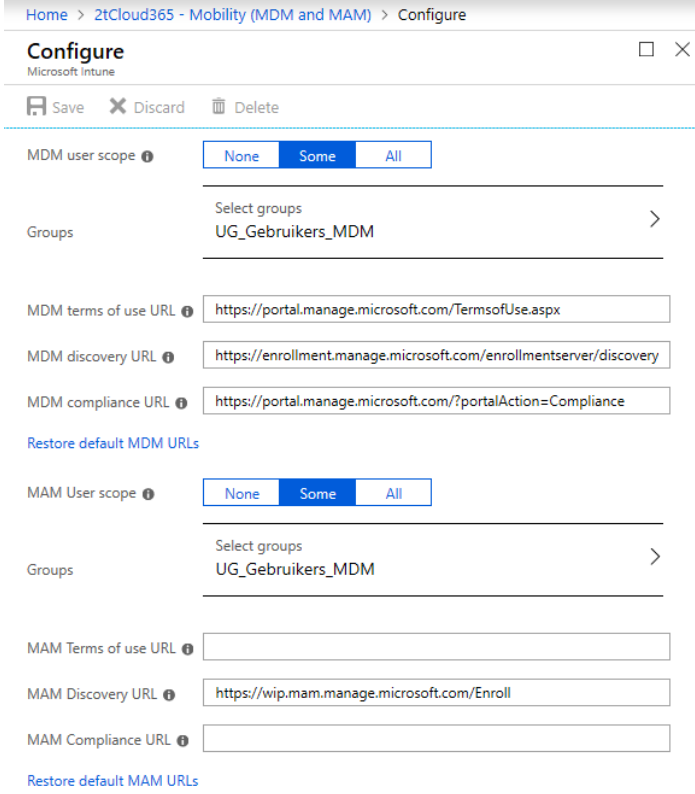
1. Go to : http://portal.azure.com			
Kenmerk	Waarde		
Group type	Security		
Group name	UG_gebruikers_MDM		
Group description	MDM group		
Membership type	Assigned		

<ol style="list-style-type: none"> 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) 					
<ol style="list-style-type: none"> 6. AAD Group "UG_Gebruikers_MDM" is created 	 <table border="1"> <thead> <tr> <th>NAME</th> <th>GROUP TYPE</th> </tr> </thead> <tbody> <tr> <td>UG_Gebruikers_MDM</td> <td>Security</td> </tr> </tbody> </table>	NAME	GROUP TYPE	UG_Gebruikers_MDM	Security
NAME	GROUP TYPE				
UG_Gebruikers_MDM	Security				

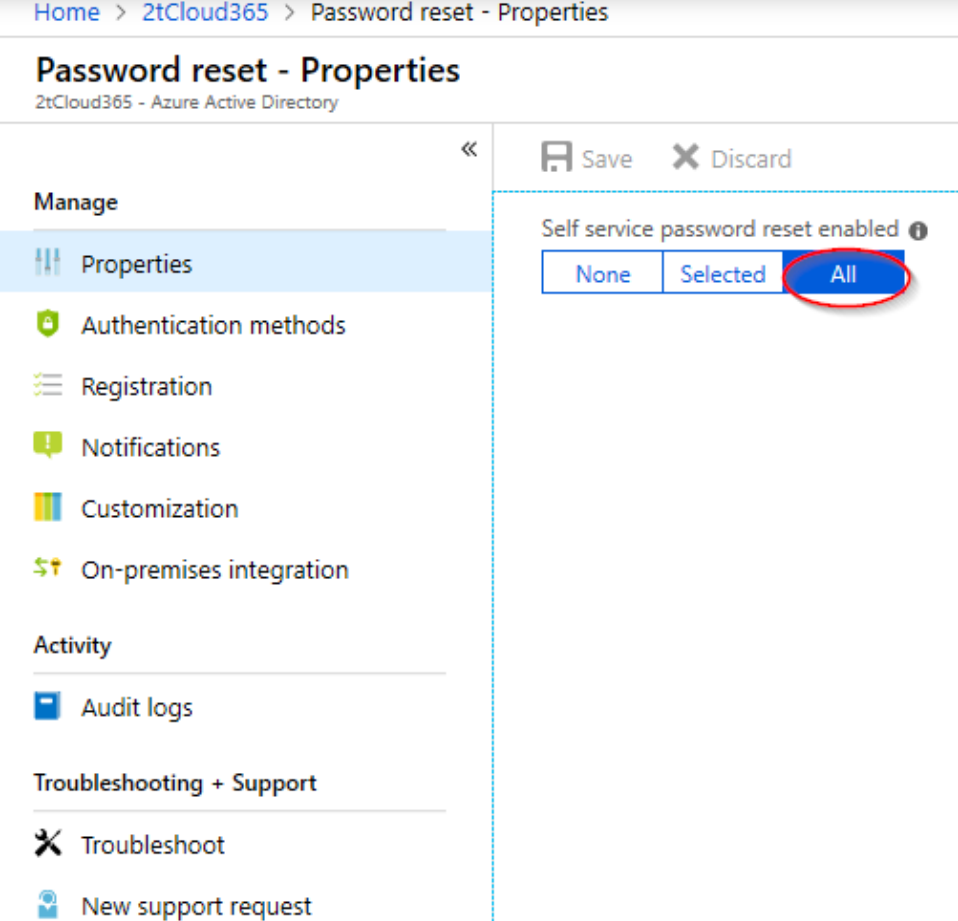
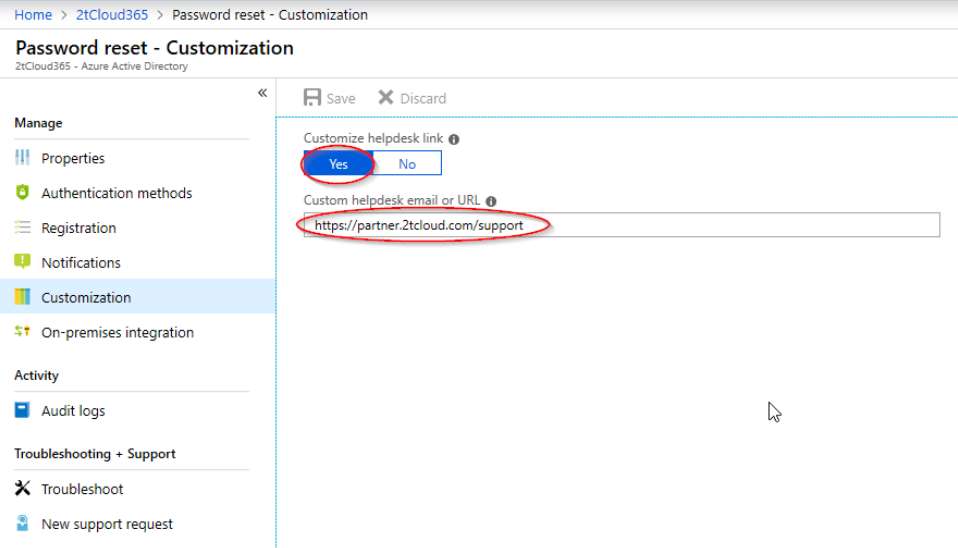
Exercise 2a: Configure group-based Licensing

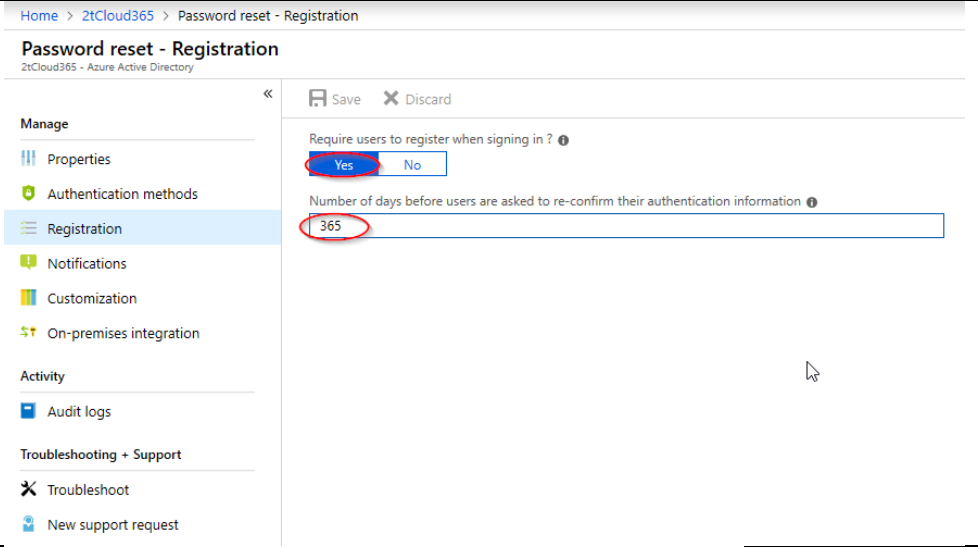
<ol style="list-style-type: none"> 1. Go to: Azure Active Directory → Licenses → All products 2. Select Microsoft 365 E3 3. Select Licensed groups 4. Click the Assign button 5. At users and groups search for UG_gebruikers_MDM and select the group 6. At Assignment options make sure that On is selected and click OK 7. Click Assign 	
--	--

Exercise 3: Configure MDM and MAM Intune settings

<p>1. Go to Azure Active Directory->Mobility (MDM and MAM)->Microsoft Intune.</p>											
<p>2. Configure the settings -></p>	<table border="1"> <thead> <tr> <th>Kenmerk</th><th>Waarde</th></tr> </thead> <tbody> <tr> <td>MDM User scope</td><td>Some</td></tr> <tr> <td>Groups</td><td>UG_Gebruikers_MDM</td></tr> <tr> <td>MAM User scope</td><td>Some</td></tr> <tr> <td>Groups</td><td>UG_Gebruikers_MDM</td></tr> </tbody> </table>	Kenmerk	Waarde	MDM User scope	Some	Groups	UG_Gebruikers_MDM	MAM User scope	Some	Groups	UG_Gebruikers_MDM
Kenmerk	Waarde										
MDM User scope	Some										
Groups	UG_Gebruikers_MDM										
MAM User scope	Some										
Groups	UG_Gebruikers_MDM										
<p>3. Click on Save</p>											

Exercise 4: Activate Self Service Password Reset

<ol style="list-style-type: none"> 1. Go to Azure Active Directory->Password reset->Properties; 2. Set setting to: All 3. Click: Save 					
<ol style="list-style-type: none"> 4. Go to Azure Active Directory-> Password reset-> Customization; 					
<ol style="list-style-type: none"> 5. Configure the settings -> and click Save 	<table border="1"> <tr> <td>Customize helpdesk link</td> <td>Yes</td> </tr> <tr> <td>Custom helpdesk email or URL</td> <td>https://partner.2tcloud.com/support</td> </tr> </table>	Customize helpdesk link	Yes	Custom helpdesk email or URL	https://partner.2tcloud.com/support
Customize helpdesk link	Yes				
Custom helpdesk email or URL	https://partner.2tcloud.com/support				

<p>6. Go to Azure Active Directory-> Password reset-> Registration;</p>	 <p>Home > 2tCloud365 > Password reset - Registration</p> <p>2tCloud365 - Azure Active Directory</p> <p>Manage</p> <ul style="list-style-type: none"> Properties Authentication methods Registration Notifications Customization On-premises integration <p>Activity</p> <ul style="list-style-type: none"> Audit logs <p>Troubleshooting + Support</p> <ul style="list-style-type: none"> Troubleshoot New support request <p>Save Discard</p> <p>Require users to register when signing in ? Yes No</p> <p>Number of days before users are asked to re-confirm their authentication information 365</p>				
<p>7. Configure the settings -> and click Save</p>	<table border="1"> <tr> <td>Require Users to register when Signing in?</td> <td>Yes</td> </tr> <tr> <td>Number of days</td> <td>365</td> </tr> </table>	Require Users to register when Signing in?	Yes	Number of days	365
Require Users to register when Signing in?	Yes				
Number of days	365				

Exercise 5: Company branding

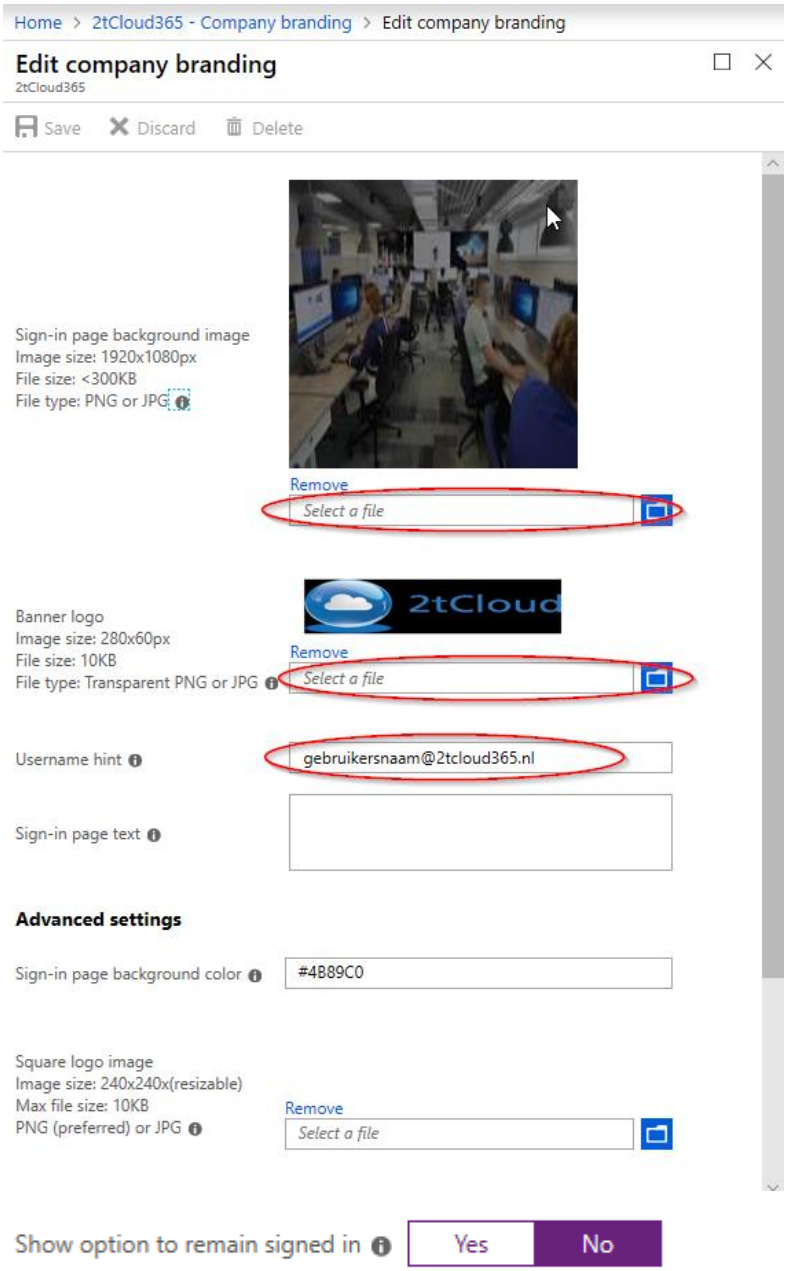
1. Go to **Azure Active Directory**->**Company Branding**->**Edit company branding**;

[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	gebruikersnaam@2tcloud365.nl
Show option to remain signed in	No

<div>3. Go to Intune -> Client apps -> Company Portal Branding</div>	<div><div><div>Home > Microsoft Intune > Client apps - Company Portal branding</div><div><div>Microsoft Intune</div><div><div><div>Search (Ctrl+/,)</div></div><div><div>Overview</div><div>Quick start</div><div>Manage</div><div><div>Device enrollment</div><div>Device compliance</div><div>Device configuration</div><div>Devices</div><div>Client apps</div><div>eBooks</div><div>Conditional access</div><div>On-premises access</div><div>Users</div><div>Groups</div><div>Roles</div><div>Software updates</div></div><div>Help and support</div><div><div>Help and support</div><div>Troubleshoot</div></div></div></div></div><div><div>Client apps - Company Portal</div><div>Microsoft Intune</div><div><div>Search (Ctrl+/,)</div></div><div><div>manage</div><div><div>Apps</div><div>App protection policies</div><div>App configuration policies</div><div>App selective wipe</div><div>iOS app provisioning profiles</div></div><div>monitor</div><div><div>App licenses</div><div>Discovered apps</div><div>App install status</div><div>App protection status</div><div>Audit logs</div></div><div>setup</div><div><div>iOS VPP tokens</div><div>Windows enterprise certificate</div><div>Windows Symantec certificate</div><div>Microsoft Store for Business</div><div>Windows side loading keys</div><div>Company Portal branding</div></div></div></div></div></div>													
<div>4. Configure the settings -> Save</div>	<table><tr><td>Company Name</td><td>2tCloud or your own company</td></tr><tr><td>Contact name</td><td>2tCloud or your own company</td></tr><tr><td>Phone number</td><td>Add picture</td></tr><tr><td>E-mail adress</td><td>2tcloud@copaco.com or gebruikersnaam@x.onmicrosoft.com</td></tr><tr><td>Support website name</td><td>2tCloud Support or your own company</td></tr><tr><td>Support Website URL</td><td>https://partner.2tcloud.com/support/ or your own</td></tr></table>		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
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

Search (Ctrl+/)

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

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

Sample text

More sample text

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"

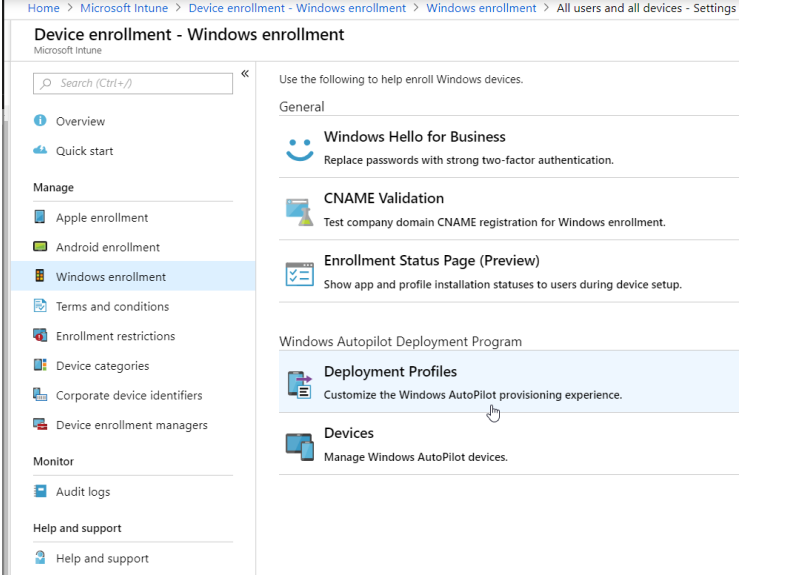
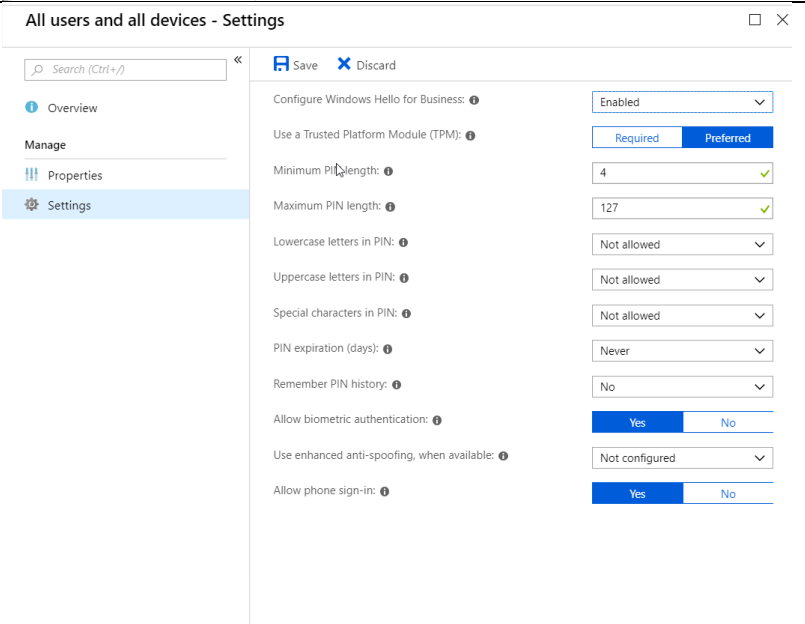


Upload logo to use on light backgrounds:

Select a file

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.

<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"> 1. Select settings 2. At Configure Windows for Business select Enabled. 3. You can leave the default settings 4. And select Save 	

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

<div>1. Go to Azure Active Directory ->Users and groups -> Device Settings;</div>	<div><div><div>Home > 2tCloud365 > Devices - Device settings</div><div>Devices - Device settings</div><div>2tCloud365 - Azure Active Directory</div><div><div>Manage</div><div>All devices</div><div>Device settings</div><div>Enterprise State Roaming</div><div>Activity</div><div>Audit logs</div><div>Troubleshooting + Support</div><div>Troubleshoot</div><div>New support request</div></div><div><div>Save</div><div>Discard</div><div>Users may join devices to Azure AD <div>AllSelectedNone</div></div><div><div>Selected</div><div>1 member selected</div></div><div>Additional local administrators on Azure AD joined devices <div>SelectedNone</div></div><div><div>Selected</div><div>4 members selected</div></div><div>Users may register their devices with Azure AD <div>AllNone</div></div><div><div>Learn more on how this setting works</div></div><div>Require Multi-Factor Auth to join devices <div>YesNo</div></div><div>Maximum number of devices per user <div>5</div></div><div>Enterprise State Roaming</div><div>Manage Enterprise State Roaming settings</div><div>Users may sync settings and app data across devices <div>AllSelectedNone</div></div><div><div>Selected</div><div>1 member selected</div></div></div></div></div>	
<div>2. Configure the settings --> Click Save</div>	<div>Users may join devices to Azure AD</div>	<div>UG_Gebruikers_MDM</div>
	<div>Additional local administrators on Azure AD Joined Devices</div>	<div>Selected -> Admin</div>
	<div>Require Multi-Factor Auth to join devices</div>	<div>Yes</div>
	<div>Maximum number of devices per user</div>	<div>5</div>
	<div>Users may sync settings and enterprise app data</div>	<div>UG_Gebruikers_MDM</div>

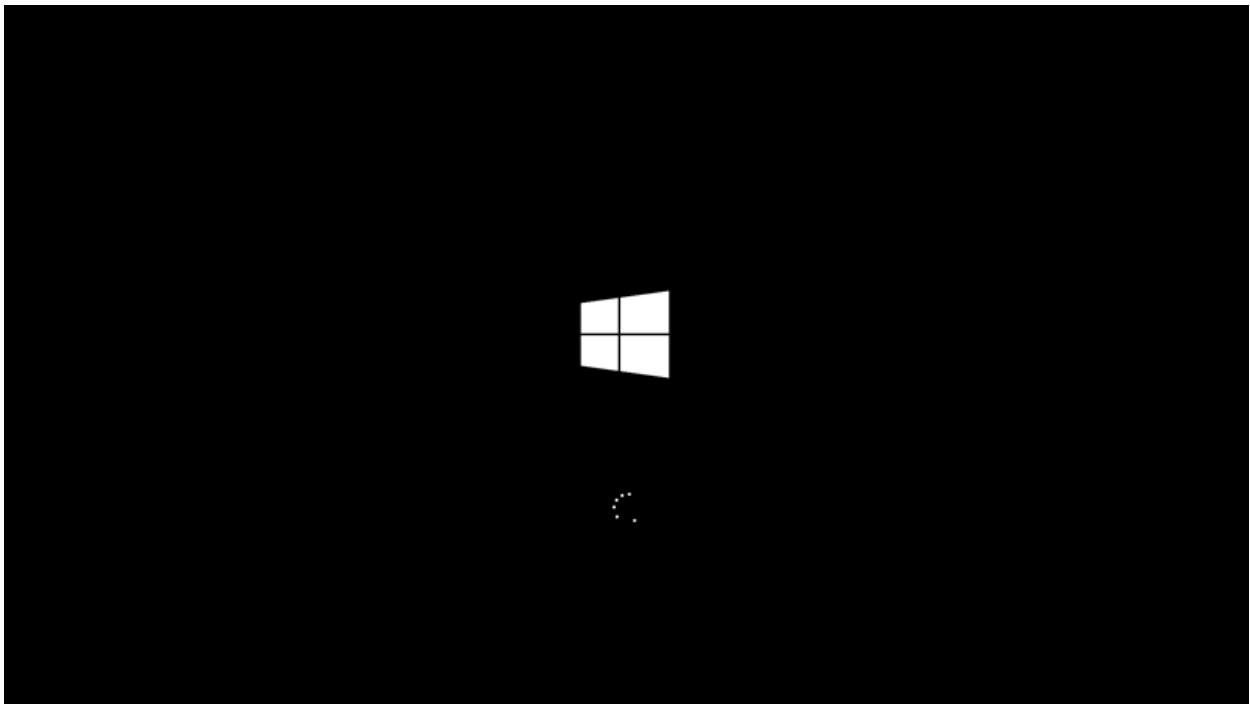
Activity 3: Add Windows to MDM

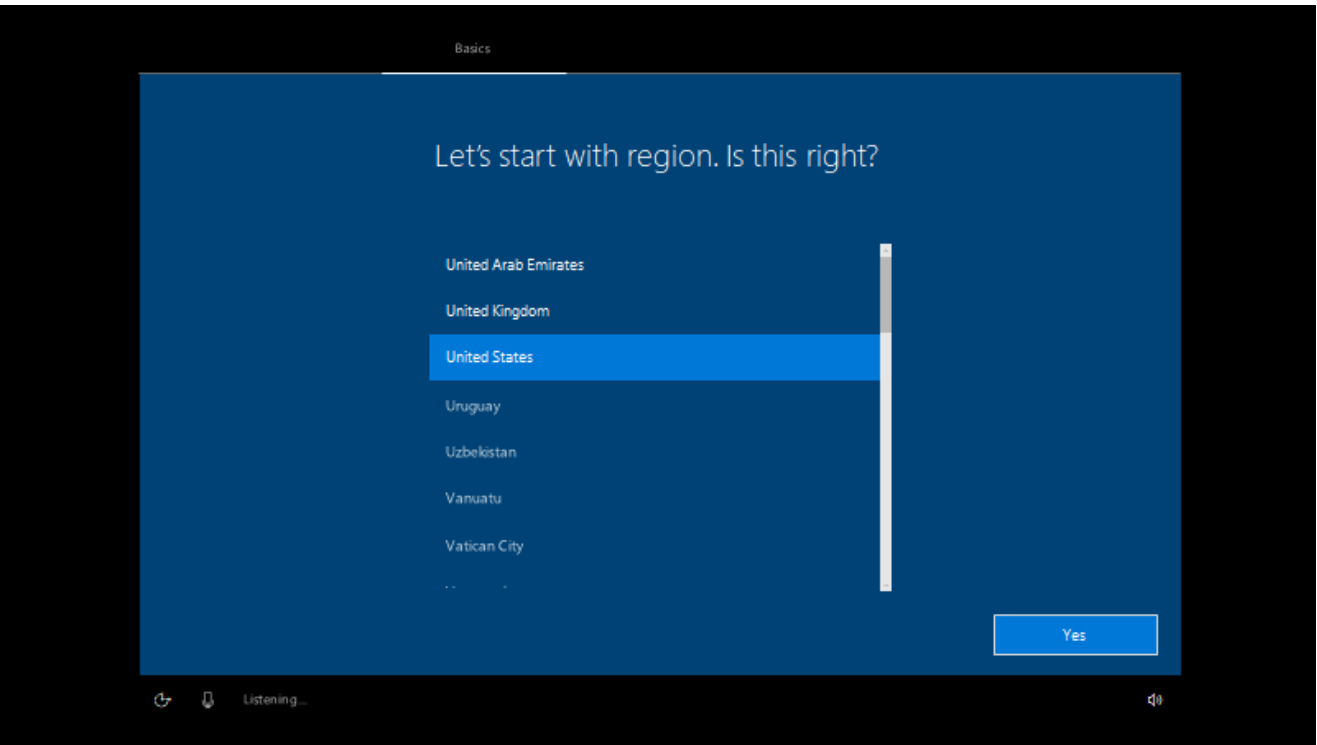
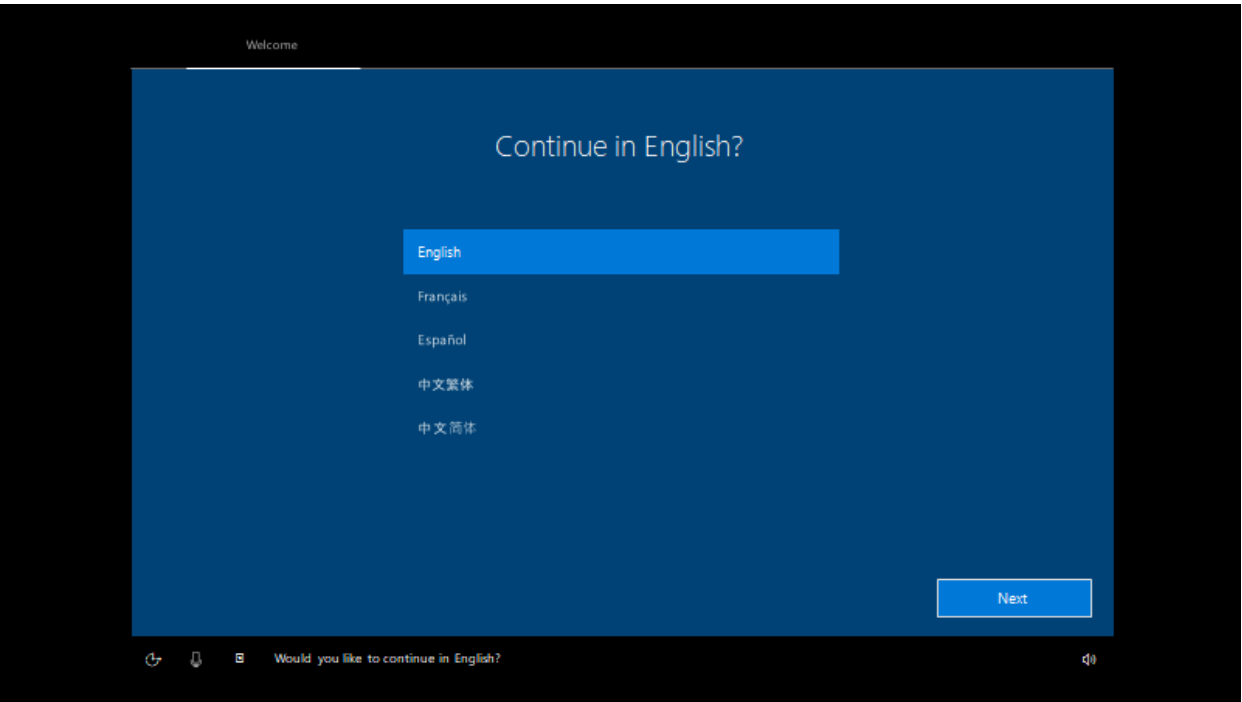
Exercise 9: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)

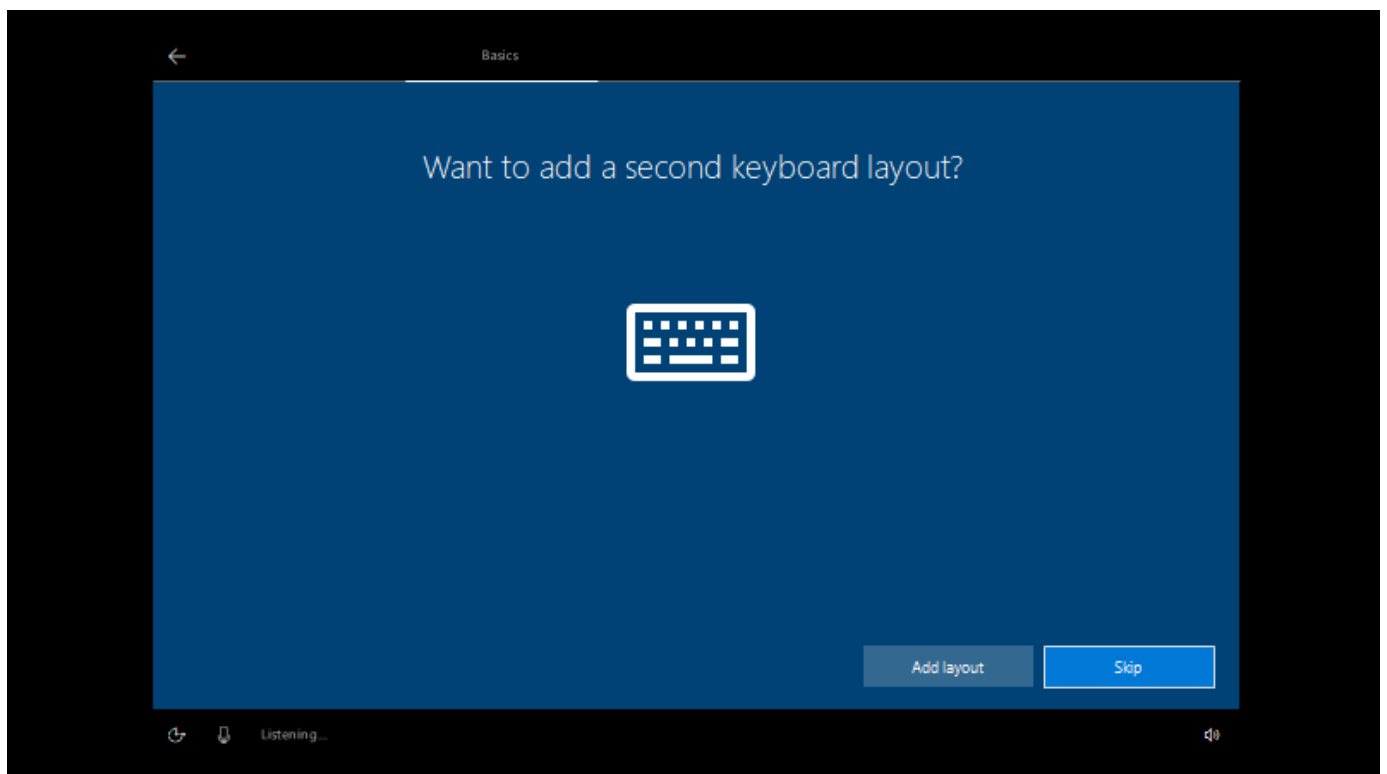
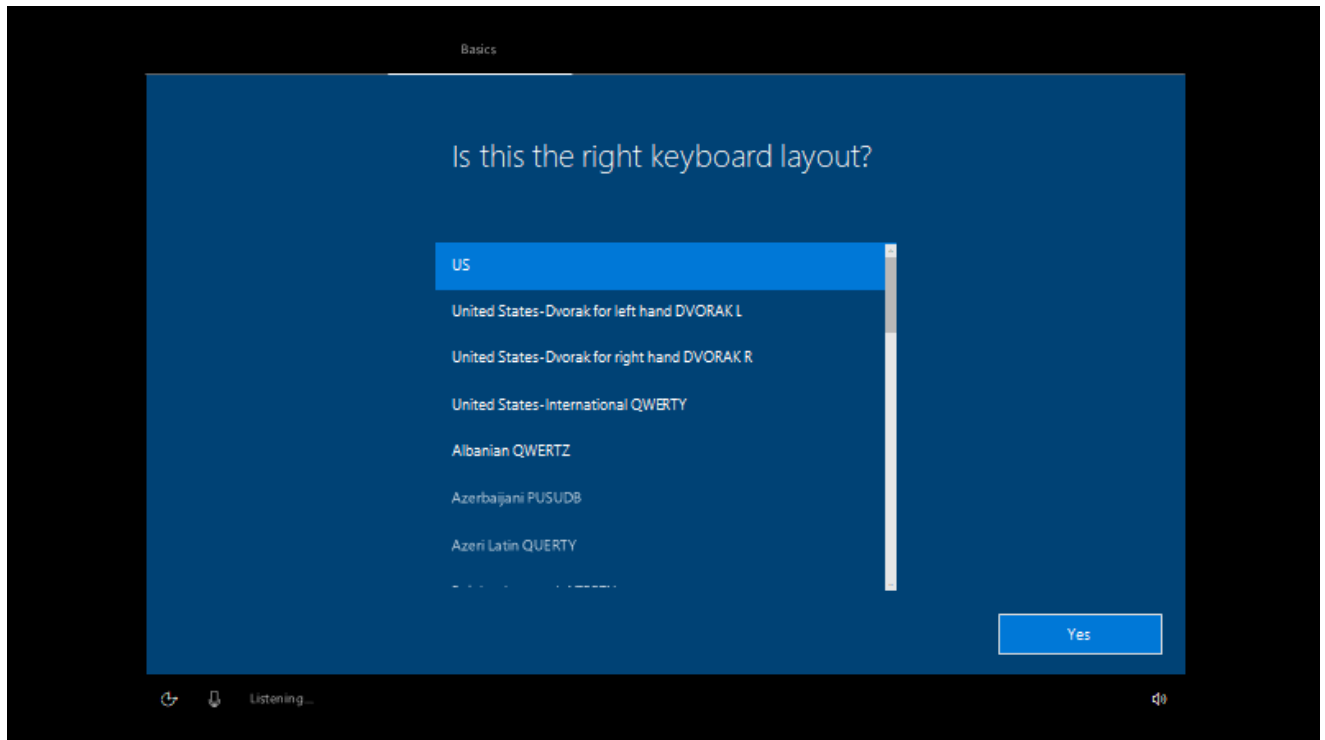
Go to the Win10 VM (Azure or Hyper-V Manager)

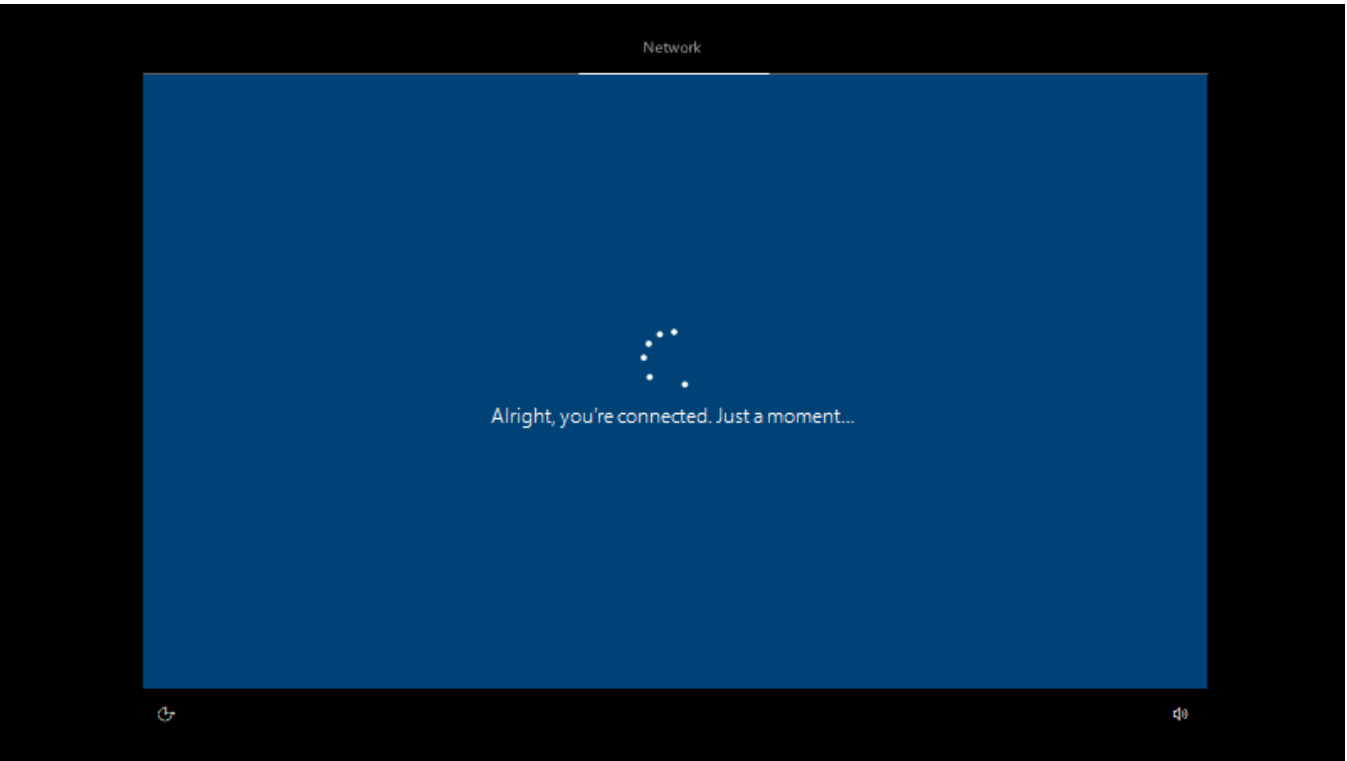
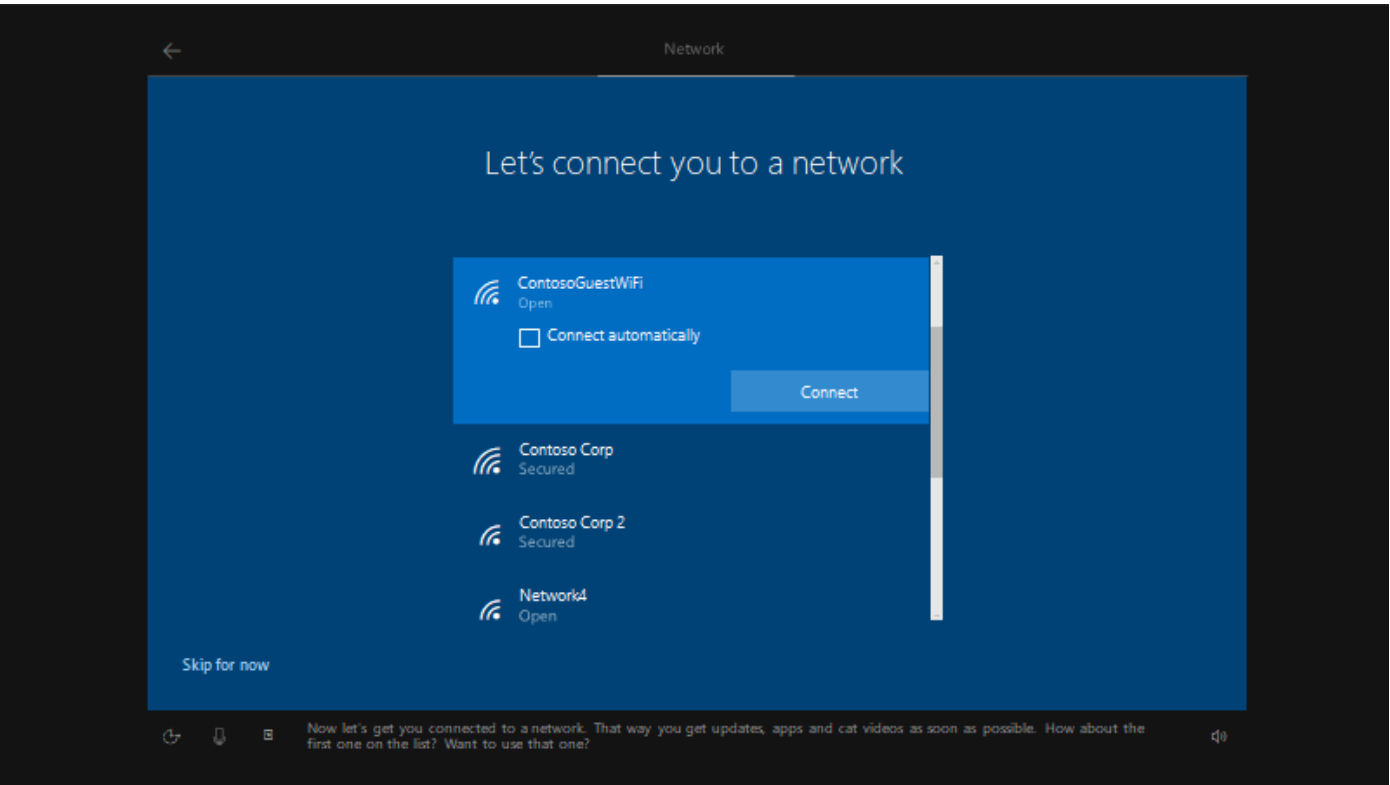
Exercise 9b (Optional) – Hyper V Win10 VM

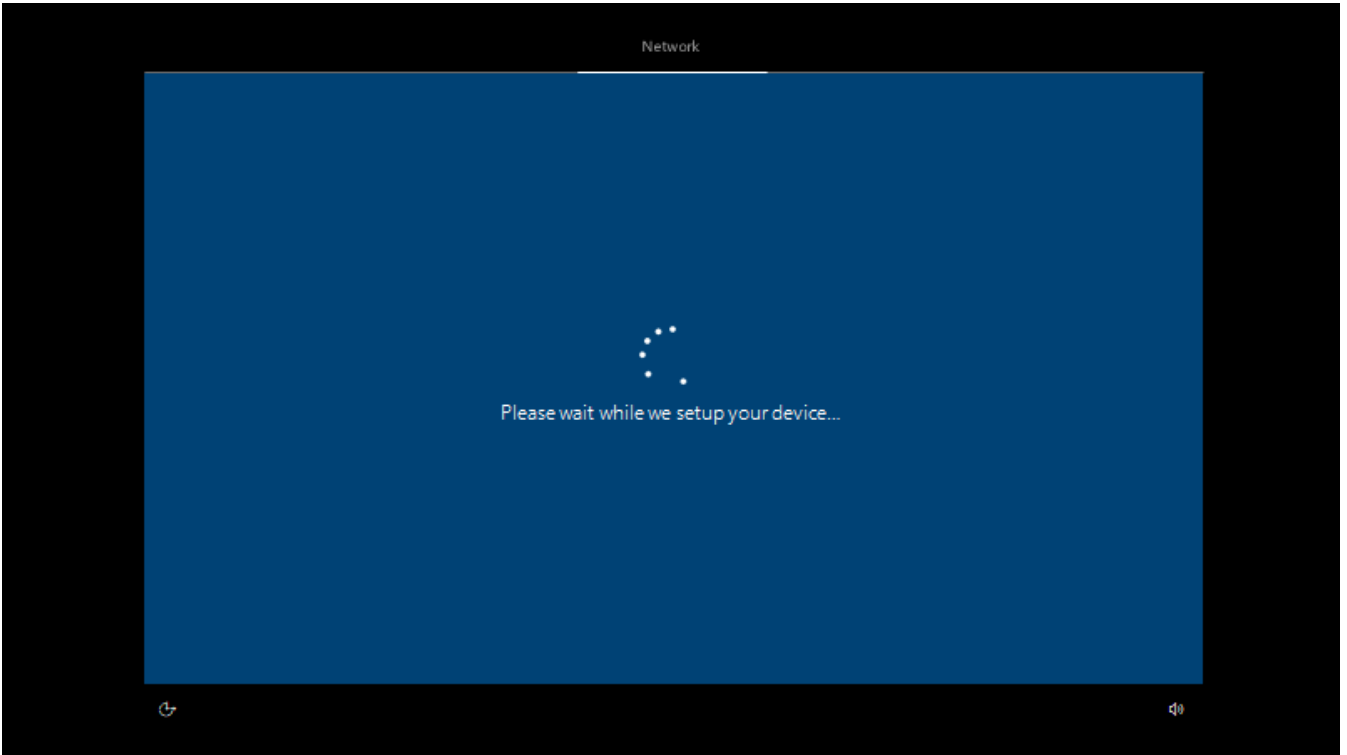
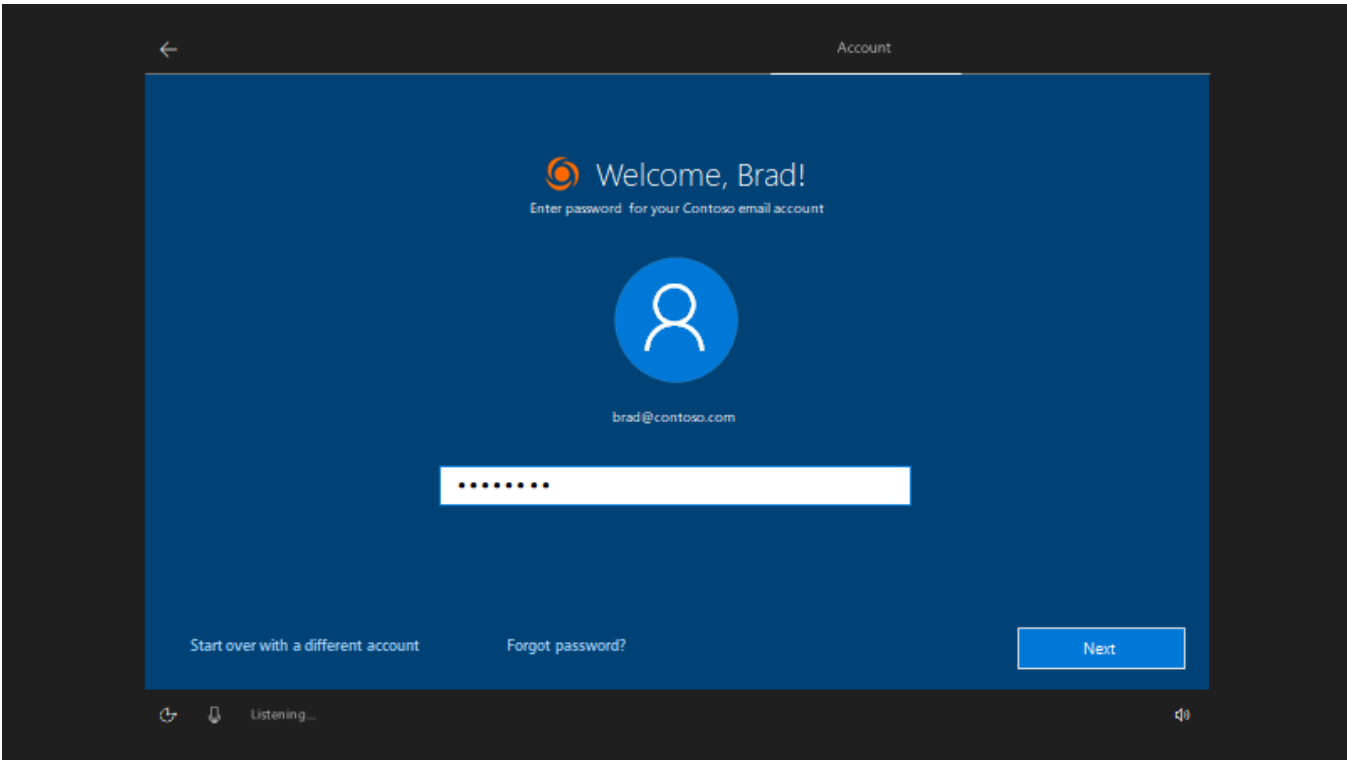
Start the setup of the Windows 10 Enterprise OS, and sign in with your test account











We're getting everything ready for you.

Don't turn off your PC

We're getting everything ready for you.

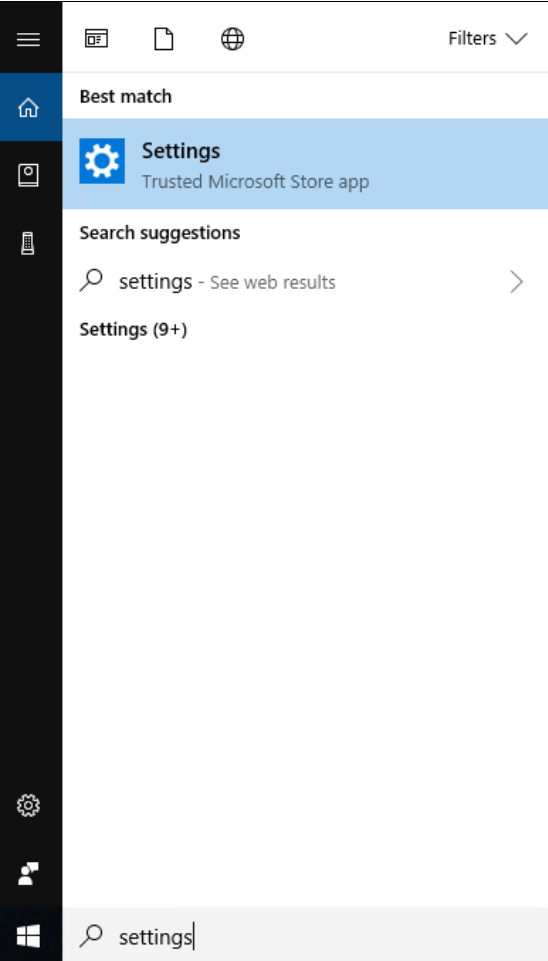
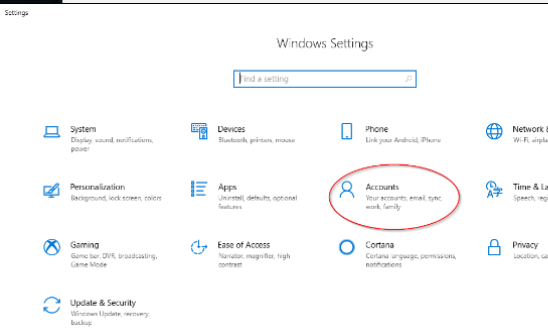
Don't turn off your PC

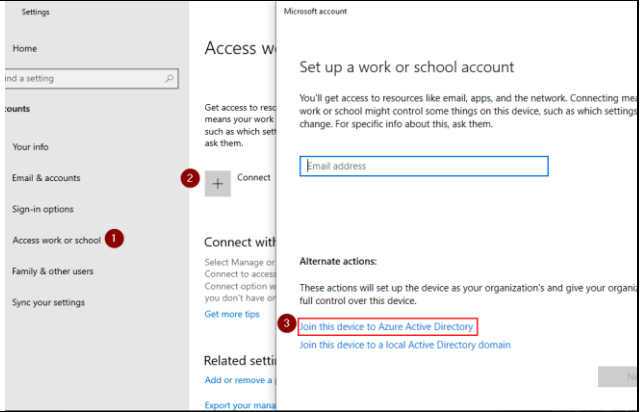
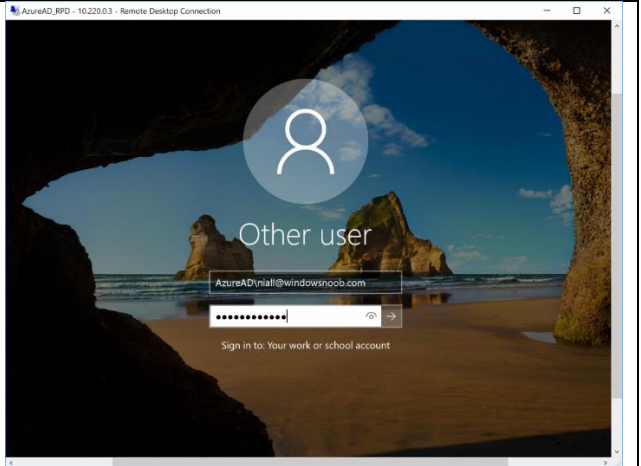
Exercise 9c (Optional) - Azure steps OPTIONAL

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

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

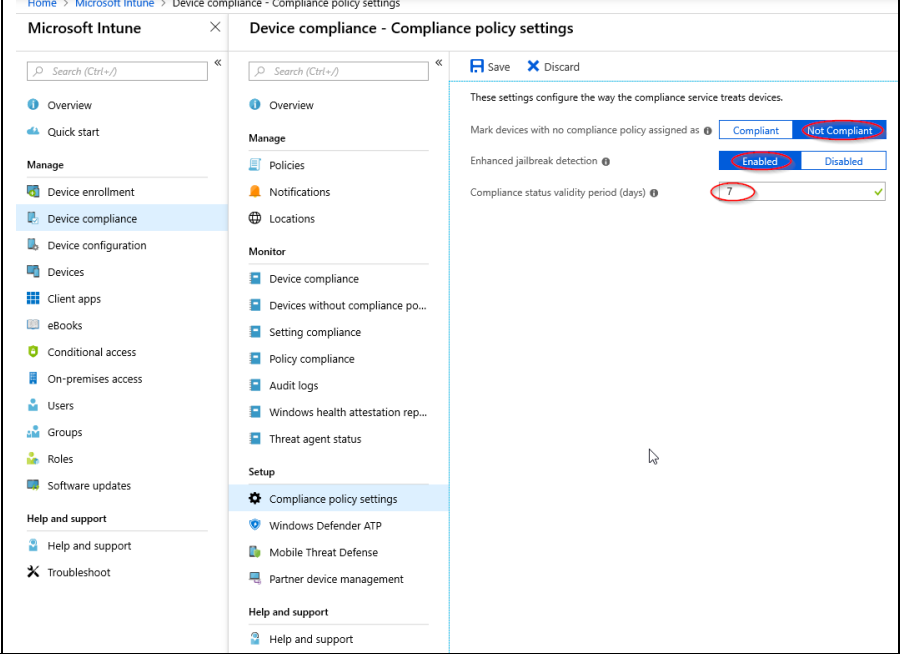
Complete these steps on the M365holwin10vm virtual machine.

<p>Enroll a Windows 10 Device in Intune</p> <ol style="list-style-type: none"> 1. Login to the virtual machine and go to Start > Settings. 	 <p>The screenshot shows the Windows Start menu 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', which is highlighted in blue. Below this, there are 'Search suggestions' including 'settings - See web results'. At the bottom, there is a search bar with the text 'settings' and a magnifying glass icon.</p>
<ol style="list-style-type: none"> 2. In the Settings app, browse to Accounts > Access work or school. 	 <p>The screenshot shows the Windows Settings app. The 'Accounts' category is highlighted with a red circle. The 'Accounts' category is located in the middle row, second column of the settings grid. The 'Accounts' category is labeled 'Accounts' and has a sub-label 'Your accounts, email, sync, work, family'.</p>

<ol style="list-style-type: none"> Click Connect. The Setup a work or school account dialog box will show, asking for your account to enroll the device. Select Join this device to Azure Active Directory. Provide the Azure AD account and click Next. In the Microsoft Intune Enrollment page, enter the password then click Sign in. Click Got it. In the Settings app, you should see that the device is now connected to the corporate MDM. <p>Click Sync and confirm that the sync was successful.</p> <ol style="list-style-type: none"> Reboot the device 	
<ol style="list-style-type: none"> At the login screen you need to use the following format to log in (this is your test account): AzureAD\<username@domain.com> 	

Activity 4: Configuration Intune

Exercise 10: Device Compliance

<p>1. Go to Intune->Device Compliance -> Compliance policy settings</p>			
<p>2. Configure the settings > Click Save</p>	<p>Mark devices with no compliance</p> <p>Enhanced Jailbreak detection</p> <p>Compliance status validity period</p>	<p>Not Compliant</p> <p>Enabled</p> <p>7</p>	

<p>3. Go to Intune->Device Compliance->Policies->Create Policy;</p>	<div> <div> <div>Create Policy</div> <div> <div>* Name</div> <div>CP_2tC365_PIN_ ✓</div> </div> <div> <div>Description</div> <div>Enter a description... ✓</div> </div> <div> <div>* Platform</div> <div>Windows 10 and later ▾</div> </div> <div> <div>Settings</div> <div>Configure ></div> </div> <div> <div>Actions for noncompliance</div> <div>1 configured ></div> </div> <div> <div>Scope (Tags)</div> <div>0 scope(s) selected ></div> </div> <div>Create</div> </div> <div> <div>Windows 10 compliance policy</div> <div>Windows 10 and later</div> <div>Select a category to configure settings.</div> <div> <div>Device Health ⓘ</div> <div>3 settings available ></div> </div> <div> <div>Device Properties ⓘ</div> <div>5 settings available ></div> </div> <div> <div>System Security ⓘ</div> <div>16 settings available ></div> </div> <div> <div>Windows Defender ATP ⓘ</div> <div>1 setting available ></div> </div> <div>OK</div> </div> <div> <div>System Security</div> <div>Windows 10 and later</div> <div>Password</div> <div>Require a password to unlock mobile device ⓘ</div> <div>Simple passwords ⓘ</div> <div>Password type ⓘ</div> <div>Number of non-alphanumeric characters ⓘ</div> <div>Minimum password length ⓘ</div> <div>Maximum minutes of inactivity before password required ⓘ</div> <div>Password expiration (days) ⓘ</div> <div>Number of previous passwords to prevent reuse ⓘ</div> <div>Require password when device returns from sleep (Mobile and Holographic) ⓘ</div> <div>Encryption</div> <div>Encryption of data storage on device. ⓘ</div> <div>Device Security</div> <div>Firewall ⓘ</div> <div>Antivirus ⓘ</div> <div>AntiSpyware ⓘ</div> <div>OK</div> </div> </div>				
<p>4. Configure the settings ></p>	<table> <tr> <td>Name</td><td>CP_2tC365_PIN</td></tr> <tr> <td>Platform</td><td>Windows 10 and later</td></tr> </table>	Name	CP_2tC365_PIN	Platform	Windows 10 and later
Name	CP_2tC365_PIN				
Platform	Windows 10 and later				
<p>5. Repeat steps 1 / 4 for another policy (Bitlocker)</p>	<div> <div> <div>CP_2tC365_Bitlocker - Properties</div> <div>Device compliance policy</div> <div>Search (Ctrl+F)</div> <div>Save Discard</div> <div> <div>Overview</div> <div>Manage</div> <div>Properties</div> <div>Assignments</div> <div>Monitor</div> <div>Device status</div> <div>User status</div> <div>Per-setting status</div> </div> <div> <div>* Name</div> <div>CP_2tC365_Bitlocker</div> </div> <div> <div>Description</div> <div>Afdwingen van Bitlocker</div> </div> <div> <div>* Platform</div> <div>Windows 10 and later ▾</div> </div> <div> <div>Settings</div> <div>1 configured ></div> </div> <div> <div>Actions for noncompliance</div> <div>1 configured ></div> </div> <div> <div>Scope (Tags)</div> <div>0 scope(s) selected ></div> </div> <div>OK</div> </div> <div> <div>Windows 10 compliance policy</div> <div>Windows 10 and later</div> <div>Select a category to configure settings.</div> <div> <div>Device Health ⓘ</div> <div>4 or 3 settings configured ></div> </div> <div> <div>Device Properties ⓘ</div> <div>5 settings available ></div> </div> <div> <div>System Security ⓘ</div> <div>16 settings available ></div> </div> <div> <div>Windows Defender ATP ⓘ</div> <div>1 setting available ></div> </div> <div>OK</div> </div> <div> <div>Device Health</div> <div>Windows 10 and later</div> <div>Windows Health</div> <div>Require BitLocker</div> <div>Require Secure Boot</div> <div>Require code integrity</div> <div>OK</div> </div> </div>				

6. Configure the settings -> Click Ok	Name		CP_2TC365_Bitlocker
7. Click on Configure	Description		Afdwingen van Bitlocker
8. Configure settings as showed on the screenshot -> Click Save	Platform		Windows 10 and later
9.			
10. Go to Intune->Device Compliance->Policies-> CP_2TC365_Bitlocker -> Assignments-> Select groups	<div><div><div>CP_2TC365_Bitlocker - Assignments</div><div>Device compliance policy</div><div><div>Search (Ctrl+/)</div><div>«</div></div><div><div>Overview</div><div>Manage</div><div>Properties</div><div>Assignments</div><div>Monitor</div></div><div><div>Device status</div><div>User status</div><div>Per-setting status</div></div></div><div><div>Save</div><div>Discard</div><div>Evaluate</div></div><div><div>Approximately 3 users will be impacted.</div><div><div>Include</div><div>Exclude</div></div><div>Assign to</div><div>Selected Groups</div><div>Select groups to include</div><div>UG_Gebruikers_MDM</div></div></div>		
11. Configure the settings > Click Save	Groups	UG_Gebruikers_MDM	
12. Go to Intune->Device Compliance -> Policies-> CP_2tC365_PIN -> Assignments-> Select groups;	<div><div><div>CP_2TC365_PIN - Assignments</div><div>Device compliance policy</div><div><div>Search (Ctrl+/)</div><div>«</div></div><div><div>Overview</div><div>Manage</div><div>Properties</div><div>Assignments</div><div>Monitor</div></div><div><div>Device status</div><div>User status</div><div>Per-setting status</div></div></div><div><div>Save</div><div>Discard</div><div>Evaluate</div></div><div><div>Include</div><div>Exclude</div></div><div>Assign to</div><div>Selected Groups</div><div>Select groups to include</div><div>UG_Gebruikers_MDM</div></div>		
13. Configure the settings > Click Save	Groups	UG_Gebruikers_MDM	

Exercise 11a: Device Configuration - Windows Device Restrictions

<p>1. Go to Intune->Device Configuration->Profiles-> Create Profile;</p>									
<p>2. Configure the settings ></p>	<table border="1"> <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>	Name	Windows 10 – Device Restrictions	Platform	Windows 10 and later	Profile type	Device restrictions		
Name	Windows 10 – Device Restrictions								
Platform	Windows 10 and later								
Profile type	Device restrictions								
<p>3. Configure settings as showed on the screenshot (Password)</p>									

<p>4. Configure settings as showed on the screenshot (Personalization)</p>	<div> <div> Device restrictions <small>Windows 10 and later</small> 6 of 13 settings configured </div> <div> Per-app privacy exceptions 1 setting available </div> <div> Personalization 1 of 1 setting configured </div> <div> Printer 3 settings available </div> </div> <div> Personalization <small>Windows 10 and later</small> Desktop background picture URL (Desktop only) https://copaco.online-magazine </div>
<p>5. Configure settings as showed on the screenshot (Lock Screen Experience)</p>	<div> <div> Device restrictions <small>Windows 10 and later</small> General 5 of 24 settings configured </div> <div> Locked Screen Experience 2 of 6 settings configured </div> <div> Messaging 3 settings available </div> <div> Microsoft Edge Browser 7 of 28 settings configured </div> <div> Network proxy 8 settings available </div> </div> <div> Locked Screen Experience <small>Windows 10 and later</small> 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): <input type="text" value="Enter number of seconds (11-180)"/> </div>
<p>6. Configure settings as showed on the screenshot (Edge)</p>	<div> <div> Device restrictions <small>Windows 10 and later</small> Cloud Printer 6 settings available </div> <div> Control Panel and Settings 3 of 16 settings configured </div> <div> Display 2 settings available </div> <div> General 5 of 24 settings configured </div> <div> Locked Screen Experience 2 of 6 settings configured </div> <div> Messaging 3 settings available </div> <div> Microsoft Edge Browser 7 of 28 settings configured </div> <div> Network proxy 8 settings available </div> </div> <div> Microsoft Edge Browser <small>Windows 10 and later</small> 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 </div> <div> Start experience Custom Start pages: Import Export e.g. https://co.com/sites.xml Not configured e.g. https://co.com/sites.xml https://www.copaco.com/portfolio/copaco-cloud/2cloud 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 </div> <div> Microsoft Edge Browser <small>Windows 10 and later</small> 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 </div> <div> 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 </div>

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

Control Panel and Settings

Windows 10 and later

Settings app

System

Power and sleep settings modification (desktop only)

Devices

Network and Internet

Personalization

Apps

Accounts

Time and Language

System Time modification

Region settings modification (desktop only)

Language settings modification (desktop only)

Gaming

Ease of Access

Privacy

Update and Security

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

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

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

Windows Spotlight

Windows Spotlight on lock screen

Third-party suggestions in Windows Spotlight

Consumer Features

Windows Tips

Windows Spotlight in action center

Windows Spotlight personalization

Windows welcome experience

Apps suggestions in Ink workspace

9. Save the Configuration and assign the Configuration to the UG_gebruikers_MD M 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

The image displays three screenshots from the Windows Device Configuration console, illustrating the configuration of BitLocker settings for enrolled devices.

Top Left Screenshot: Shows the 'Profiles' list on the left sidebar. The 'Name' field is set to 'Windows 10 Encryption' and the 'Description' is 'Bitlocker settings for enrolled devices'. The 'Platform' is 'Windows 10 and later' and the 'Profile type' is 'Endpoint protection'. The 'Settings' section shows '2 configured'.

Top Right Screenshot: Shows the 'Windows Encryption' settings page. The 'Encrypt devices' and 'Encrypt storage card (mobile only)' options are both set to 'Require'. The 'BitLocker base settings' section shows 'Warning for other disk encryption' set to 'Block' and 'Configure encryption methods' set to 'Enable'. The 'Encryption for operating system drives', 'Encryption for fixed data drives', and 'Encryption for removable data drives' are all set to 'XTS-AES 128-bit'. The 'BitLocker OS drive settings' section shows 'Additional authentication at startup' set to 'Require', 'BitLocker with non-compatible TPM chip' set to 'Block', 'Compatible TPM startup' set to 'Allow TPM', 'Compatible TPM startup PIN' set to 'Allow startup PIN with TPM', 'Compatible TPM startup key' set to 'Allow startup key with TPM', and 'Compatible TPM startup key and PIN' set to 'Allow startup key and PIN with TPM'. The 'Minimum PIN Length' is set to 'Enable'.

Bottom Left Screenshot: Shows the 'Endpoint protection' settings page. The 'Windows Encryption' category is selected, showing '1 of 37 settings configured'.

Bottom Right Screenshot: Shows the 'Windows Encryption' settings page with the 'OS drive recovery' section expanded. The 'OS drive recovery' option is set to 'Enable'. The 'Certificate-based data recovery agent' is set to 'Block'. The 'User creation of recovery password' is set to 'Allow 48-digit recovery password'. The 'User creation of recovery key' is set to 'Allow 256-bit recovery key'. The 'Recovery options in the BitLocker setup wizard' are set to 'Block'. The 'Save BitLocker recovery information to Azure Active Directory' is set to 'Enable'. The 'BitLocker recovery information stored to Azure Active Directory' is set to 'Backup recovery passwords and key packages'. The 'Store recovery information in Azure Active Directory before enabling BitLocker' is set to 'Require'. The 'Pre-boot recovery message and URL' is set to 'Enable'. The 'Pre-boot recovery message' is set to 'Use default recovery message and URL'. The 'BitLocker fixed data-drive settings' section shows 'Write access to fixed data-drive not protected by BitLocker' set to 'Block'. The 'Fixed drive recovery' is set to 'Enable'. The 'Data recovery agent' is set to 'Block'. The 'User creation of recovery password' is set to 'Allow 48-digit recovery password'. The 'User creation of recovery key' is set to 'Allow 256-bit recovery key'. The 'Recovery options in the BitLocker setup wizard' are set to 'Block'.

3. Save the Configuration and assign the Configuration to the UG_gebruikers_MD M 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

Windows 10 Update Ring

Search (Ctrl+/)

Save Discard

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Name: Windows 10 CBB Update Ring

Description: Enter a description...

Settings: 10 configured

Scope (Tags): 0 scope(s) selected

Settings

Update settings

Servicing channel: Semi-Annual Channel

Microsoft product updates: Allow Block

Windows drivers: Allow Block

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 Skip

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

Search (Ctrl+/)

Save Discard Evaluate

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Include Exclude

Assign to: Selected Groups

Select groups to include

UG_Gebruikers_MDM

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

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

5. Assign the app to MDM users

2tCloud Support - Assignments

Client Apps

Search (Ctrl+V) Save Discard

Overview

manage

- Properties
- Assignments

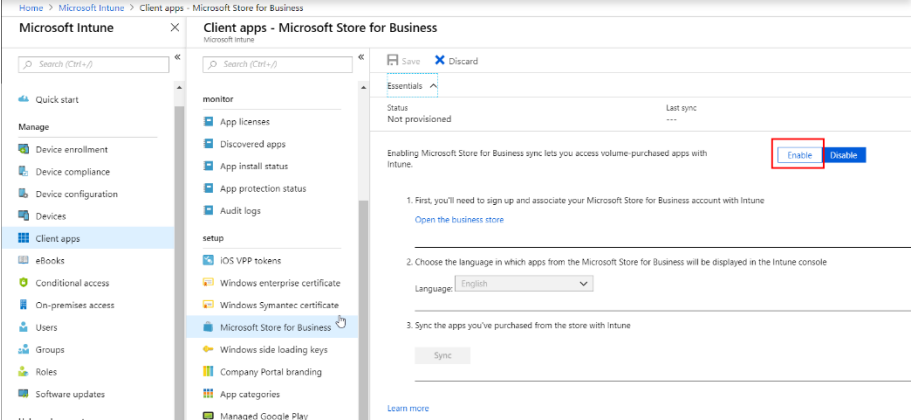
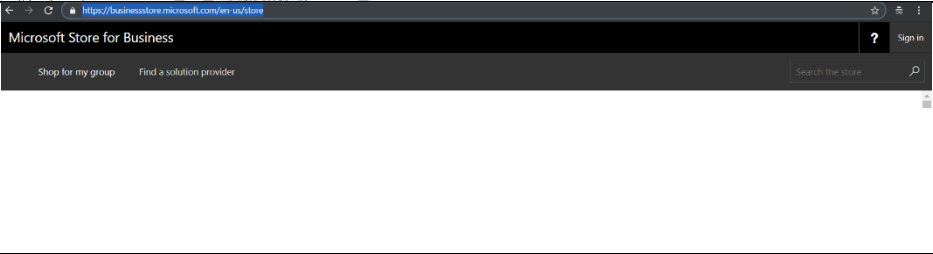
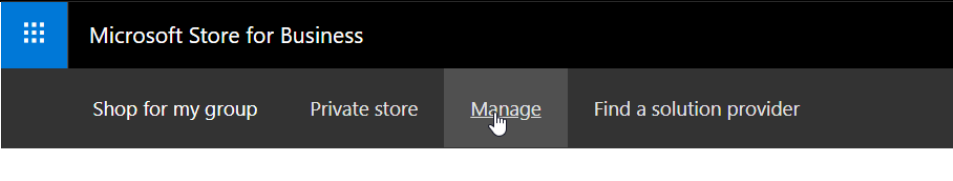
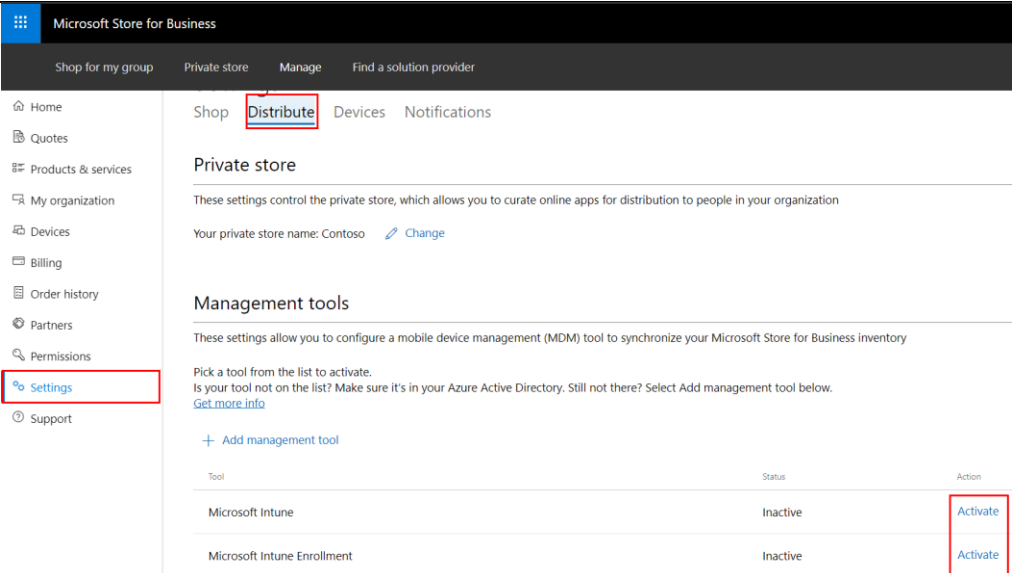
monitor

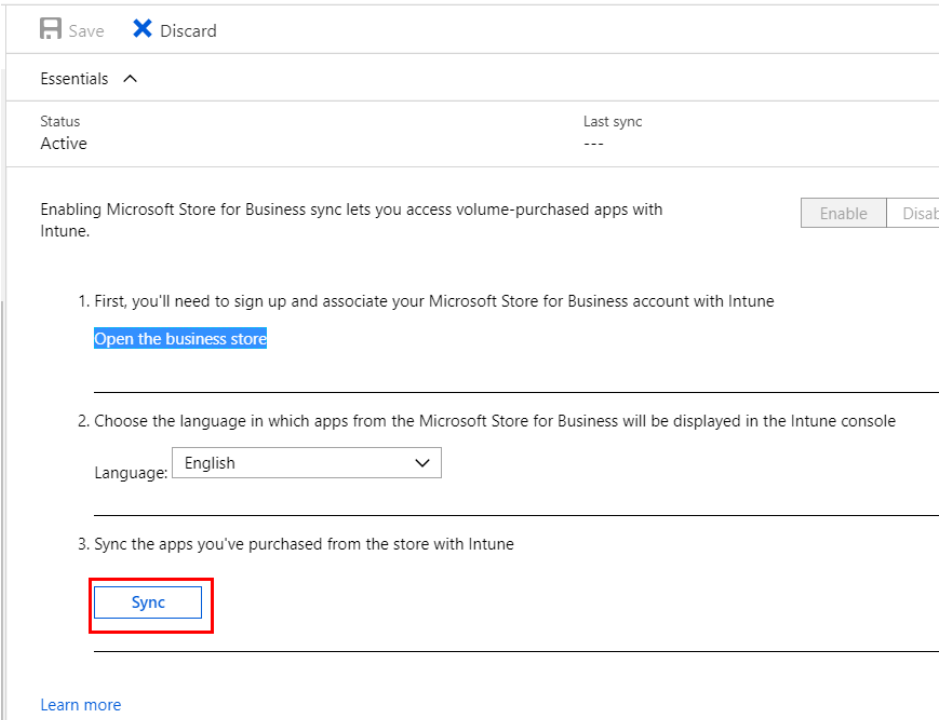

- Device install status
- User install status

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		

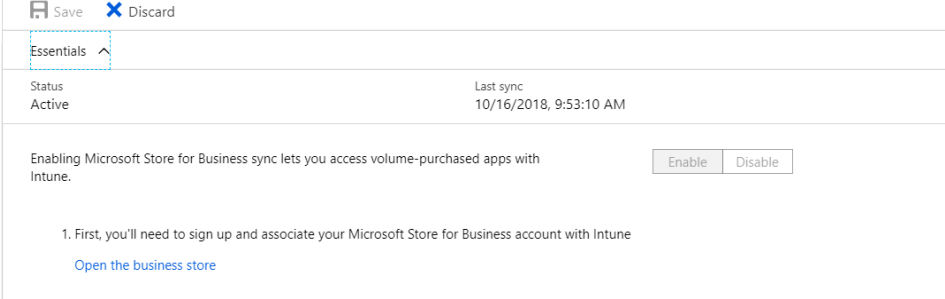
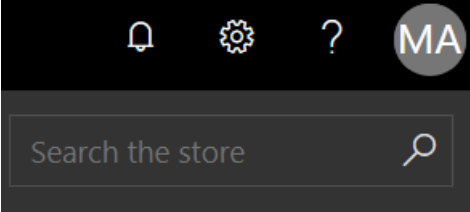
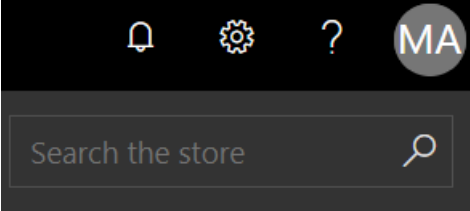
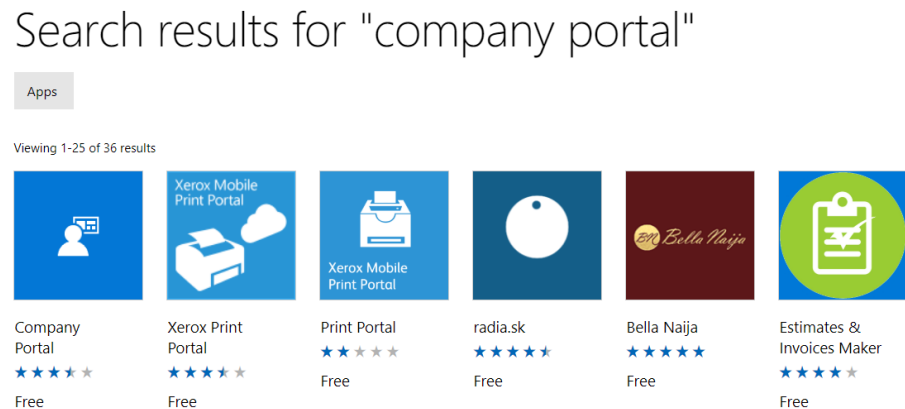
Exercise 14: Windows Store for Business

<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 'Essentials' section of the Intune portal. At the top, there are 'Save' and 'Discard' buttons. Below them, the 'Status' is 'Active' and the 'Last sync' is '---'. A section titled 'Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune.' has '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. Below this is a link 'Open the business store'. 2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console. Below this is a dropdown menu for 'Language' set to 'English'. 3. Sync the apps you've purchased from the store with Intune. Below this is a 'Sync' button, which is highlighted with a red rectangular box. At the bottom left of the section is a 'Learn more' link.</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>This screenshot shows the 'Essentials' section after a successful sync. The 'Status' remains 'Active', but the 'Last sync' is now '10/16/2018, 9:53:10 AM'. The 'Sync' button is no longer visible in this view.</p>
<p>9. At this point you can deploy apps from the Windows Store for Business</p>	

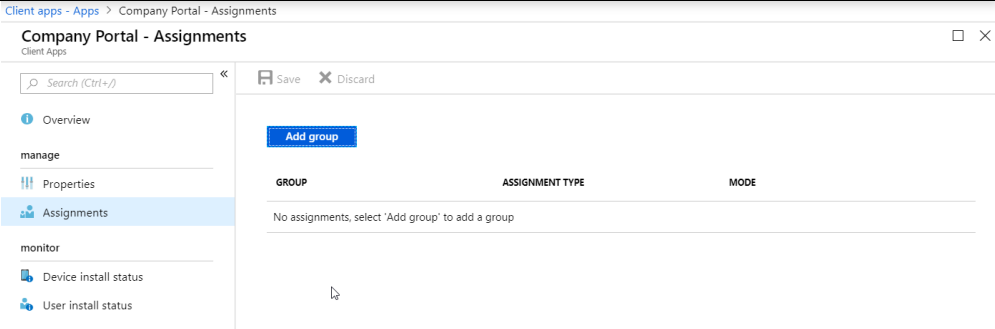
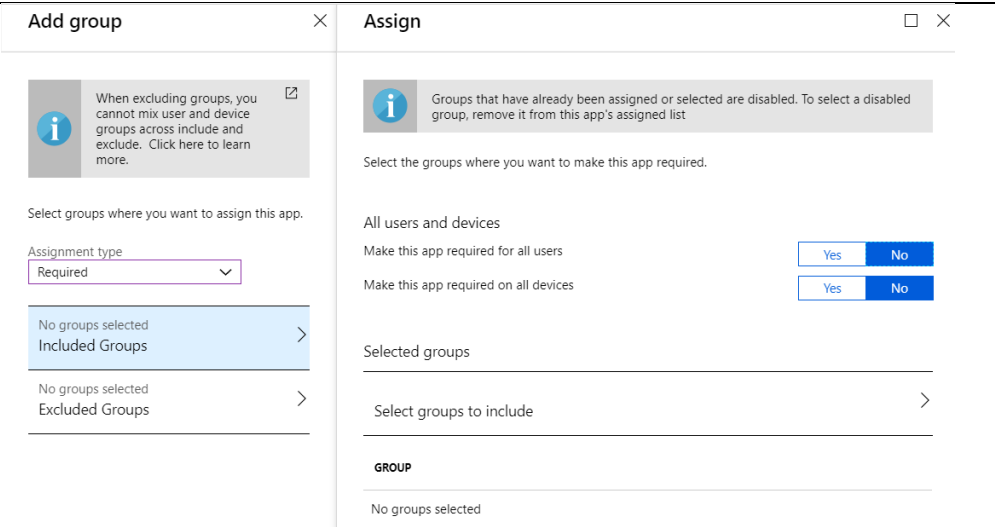
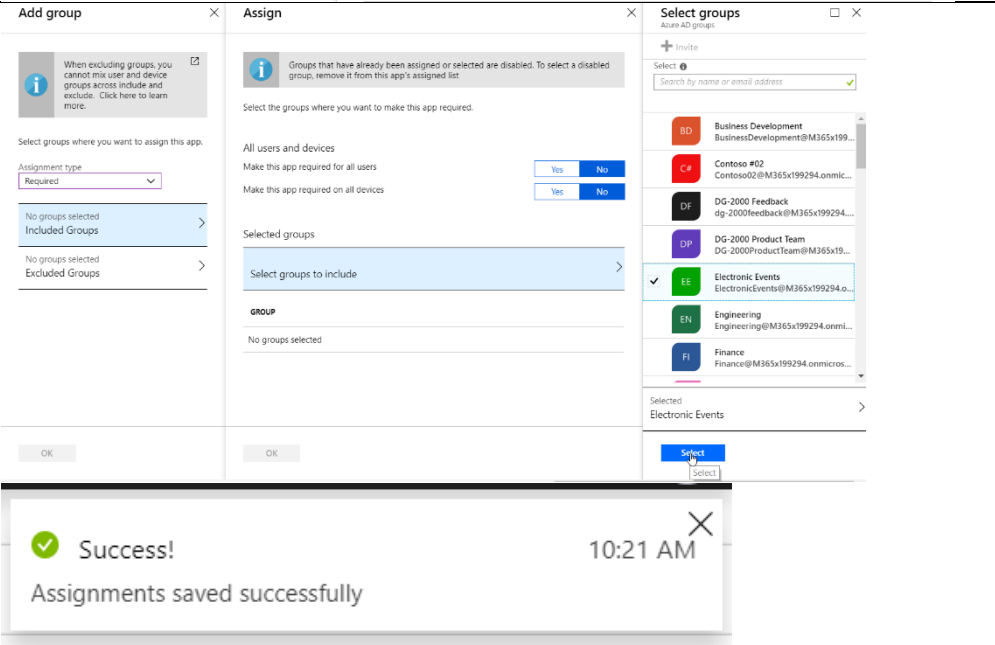
Exercise 15: Company portal

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

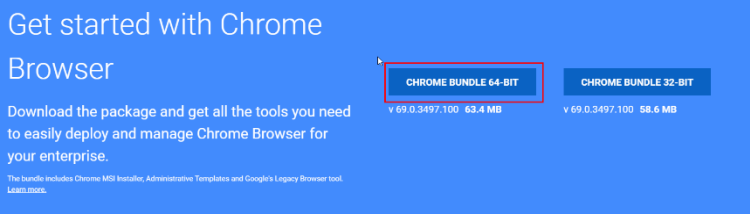
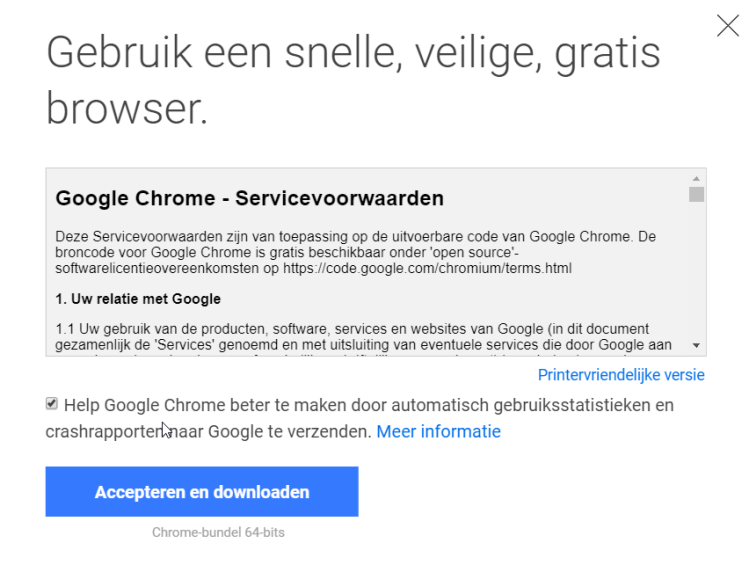
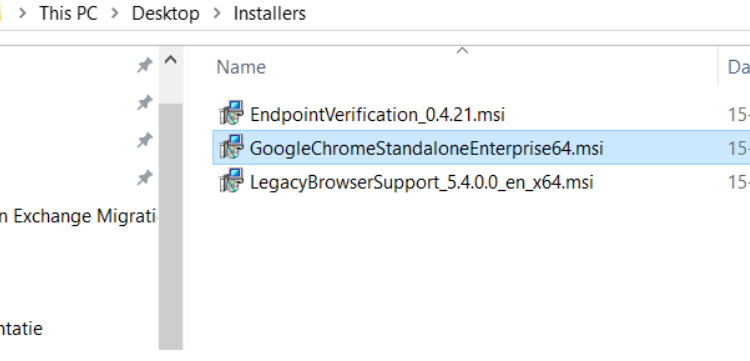
<p>Go to Microsoft Intune → Client Apps → Microsoft store for Business</p> <p>1. Select open the business store</p>	
<p>2. Check if you are signed in. If not sign in with your account</p>	
<p>3. Use the search bar to search for company portal (bedrijfs portaal)</p>	
<p>4. Select Company Portal</p>	

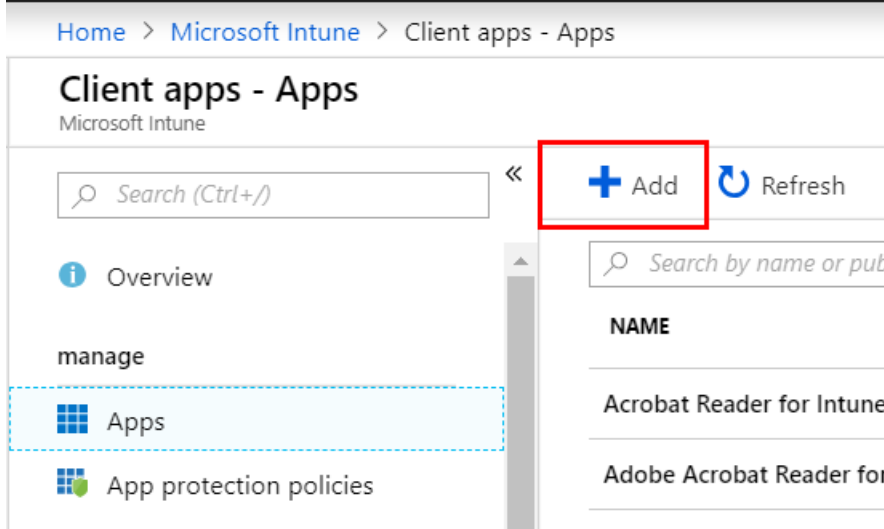
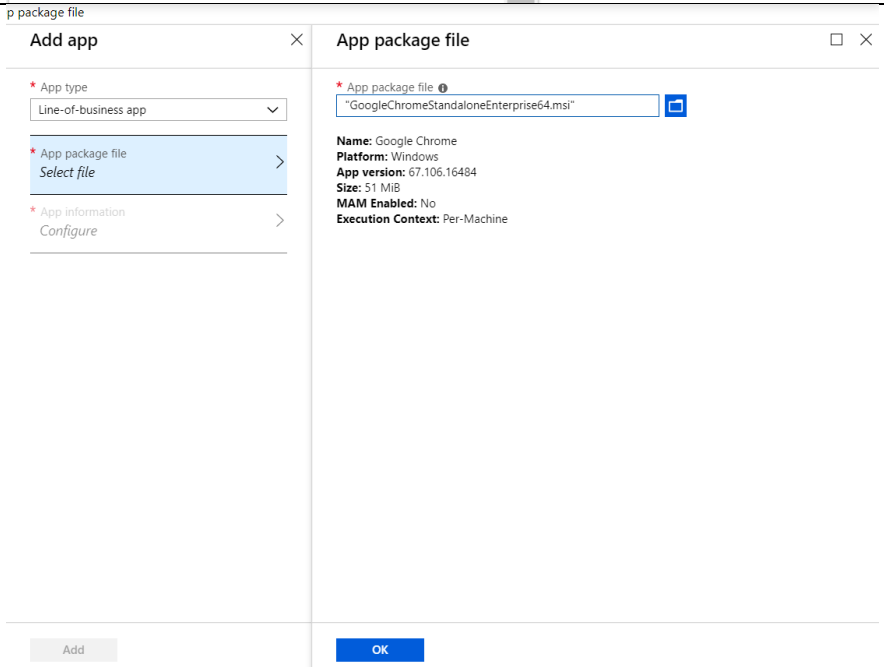
<p>5. Select Get the app</p>	
<p>6. Accept the agreement</p>	<p>Review and accept the services agreement to sign up for the Microsoft Store for Bu</p>

<p>7. After that the app is added</p>	<div data-bbox="555 367 841 407">Thanks for your order</div> <div data-bbox="616 490 691 562"></div> <div data-bbox="694 495 1099 555"><p>Company Portal has been purchased and added to your inventory.</p></div> <div data-bbox="975 978 1034 1005"><p>Close</p></div>
<p>8. Go back to the Intune Portal and Select Sync</p>	<div data-bbox="561 1059 746 1090"><p> Save  Discard</p></div> <div data-bbox="561 1111 667 1135"><p>Essentials ^</p></div> <div data-bbox="561 1155 617 1200"><p>Status Active</p></div> <div data-bbox="1101 1155 1176 1196"><p>Last sync ---</p></div> <div data-bbox="561 1240 1198 1288"><p>Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune.</p></div> <div data-bbox="1343 1245 1482 1270"><p><input type="button" value="Enable"/> <input type="button" value="Disable"/></p></div> <div data-bbox="598 1330 1311 1359"><p>1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune</p></div> <div data-bbox="614 1366 798 1397"><p>Open the business store</p></div> <div data-bbox="598 1449 1442 1478"><p>2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console</p></div> <div data-bbox="614 1491 963 1529"><p>Language: <input type="text" value="English"/></p></div> <div data-bbox="598 1572 1046 1601"><p>3. Sync the apps you've purchased from the store with Intune</p></div> <div data-bbox="651 1632 699 1659"><p><input type="button" value="Sync"/></p></div> <div data-bbox="561 1733 651 1760"><p>Learn more</p></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>	

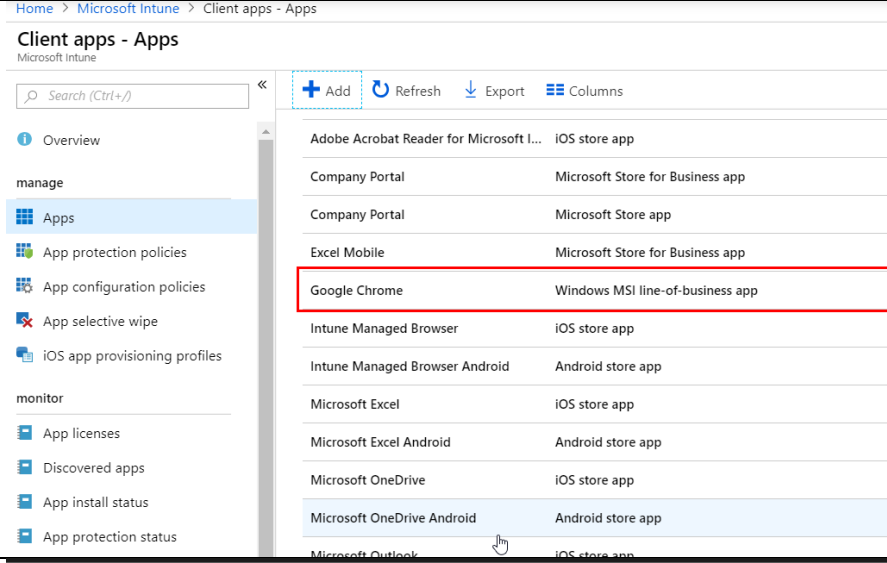
Exercise 16: MSI app deployment

<p>Go to https://enterprise.google.com/chrome/chrome-browser/</p> <ol style="list-style-type: none"> 1. Search the page for Chrome Bundle 64-bit 	 <p>Get started with Chrome Browser</p> <p>Download the package and get all the tools you need to easily deploy and manage Chrome Browser for your enterprise.</p> <p>CHROME BUNDLE 64-BIT v 69.0.3497.100 63.4 MB</p> <p>CHROME BUNDLE 32-BIT v 69.0.3497.100 58.6 MB</p>								
<ol style="list-style-type: none"> 2. Accept and download the MSI 	 <p>Gebruik een snelle, veilige, gratis browser.</p> <p>Google Chrome - Servicevoorwaarden</p> <p>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</p> <p>1. Uw relatie met Google</p> <p>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</p> <p>Printvriendelijke versie</p> <p><input checked="" type="checkbox"/> Help Google Chrome beter te maken door automatisch gebruiksstatistieken en crashrapporten naar Google te verzenden. Meer informatie</p> <p>Accepteren en downloaden</p> <p>Chrome-bundel 64-bits</p>								
<ol style="list-style-type: none"> 3. This will download a zip file 4. Extract the files to your desktop 5. There you can find the GoogleChromeStandAloneEnterprise64.msi <p>Desktop\Installers\GoogleChromeStandAloneEnterprise64.msi</p>	 <p>This PC > Desktop > Installers</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Date modified</th> </tr> </thead> <tbody> <tr> <td>EndpointVerification_0.4.21.msi</td> <td>15-9-2018 01:24</td> </tr> <tr> <td>GoogleChromeStandAloneEnterprise64.msi</td> <td>15-9-2018 01:33</td> </tr> <tr> <td>LegacyBrowserSupport_5.4.0.0_en_x64.msi</td> <td>15-9-2018 01:24</td> </tr> </tbody> </table>	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
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								

<p>Go to portal.office.com</p> <p>Choose Microsoft Intune → Client Apps → Apps</p> <p>1. Select Add</p>	 <p>Home > Microsoft Intune > Client apps - Apps</p> <h2>Client apps - Apps</h2> <p>Microsoft Intune</p> <p>Search (Ctrl+/) << + Add Refresh</p> <p>Overview</p> <p>manage</p> <p>Apps</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

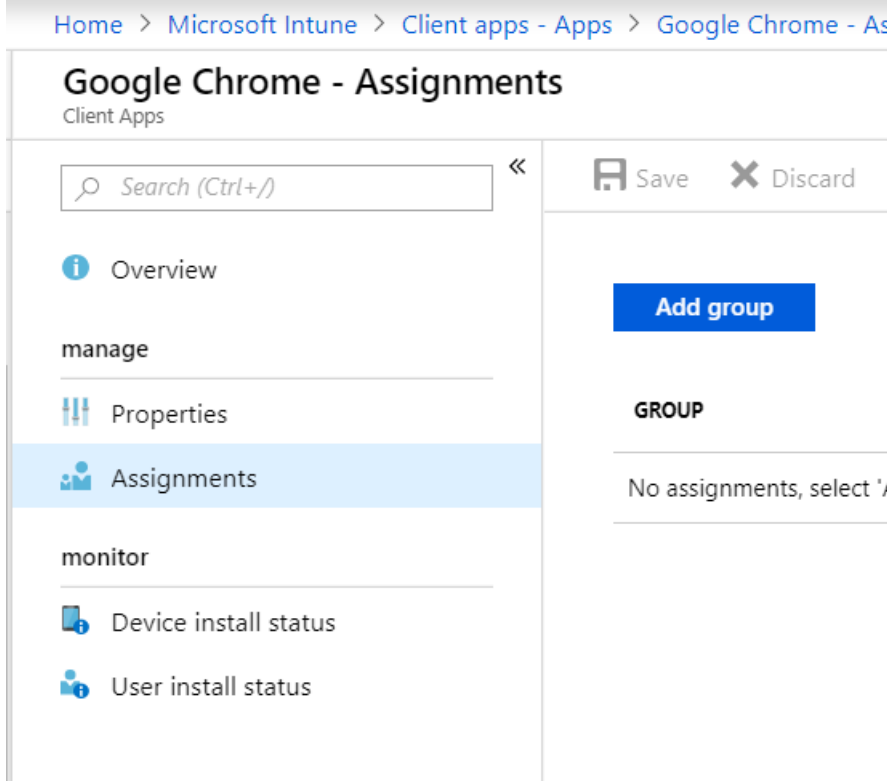
manage

- 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

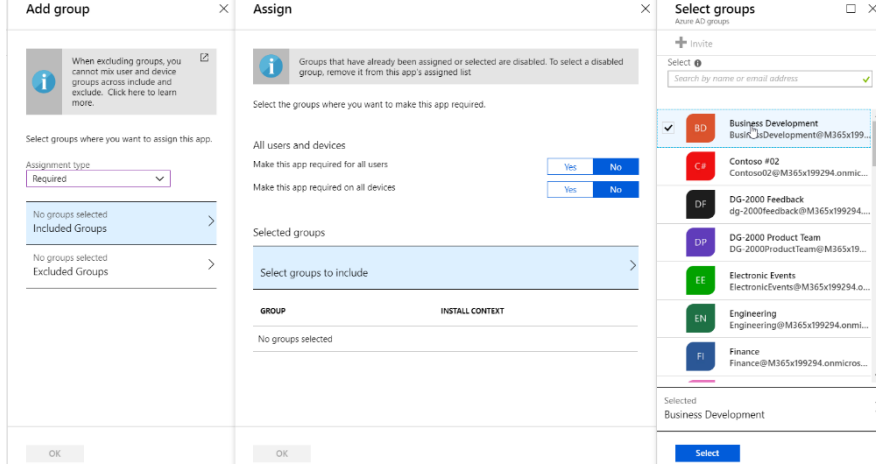
monitor

- Device install status
- User install status

Add group

GROUP

No assignments, select %

<p>12. At assignment type choose Required</p> <p>13. Select the group you created and choose Select</p> <p>14. Choose OK</p> <p>15. And OK again</p> <p>16. Finally press Save</p>	 <p>The screenshot displays the Microsoft Intune assignment wizard in three panels:</p> <ul style="list-style-type: none"> Add group: Shows the 'Assignment type' dropdown set to 'Required'. Below it are 'Included Groups' and 'Excluded Groups' sections, both currently empty. Assign: Shows options for 'All users and devices' with 'Yes' buttons for 'Make this app required for all users' and 'Make this app required on all devices'. The 'Selected groups' section is empty. Select groups: A list of groups is shown, including 'Business Development', 'Contoso #02', 'DG-2000 Feedback', 'DG-2000 Product Team', 'Electronic Events', 'Engineering', and 'Finance'. The 'Business Development' group is selected, and the 'Select' button at the bottom is highlighted.
--	---

Exercise 17: 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. 

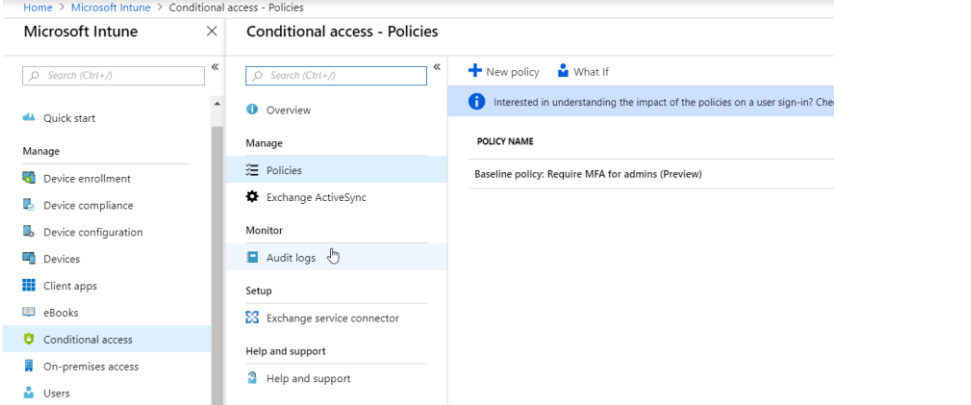
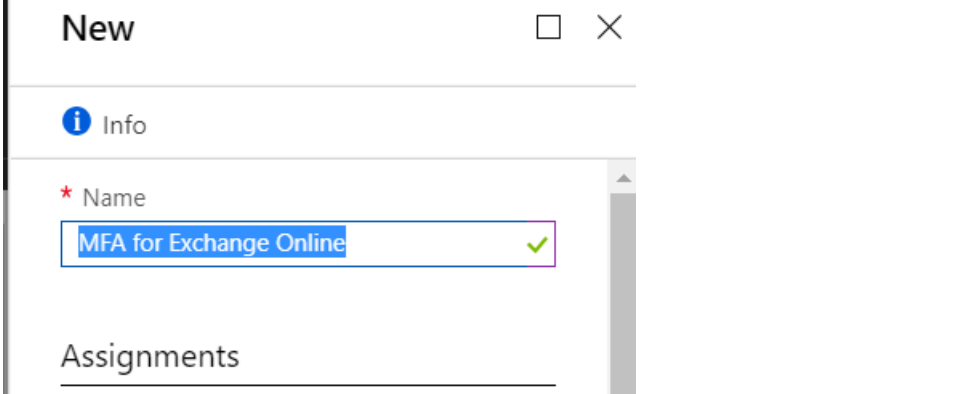
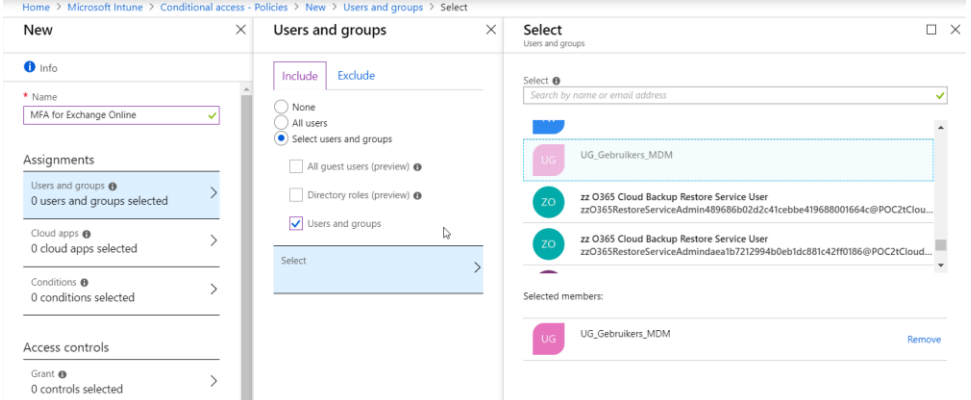
[Create](#)

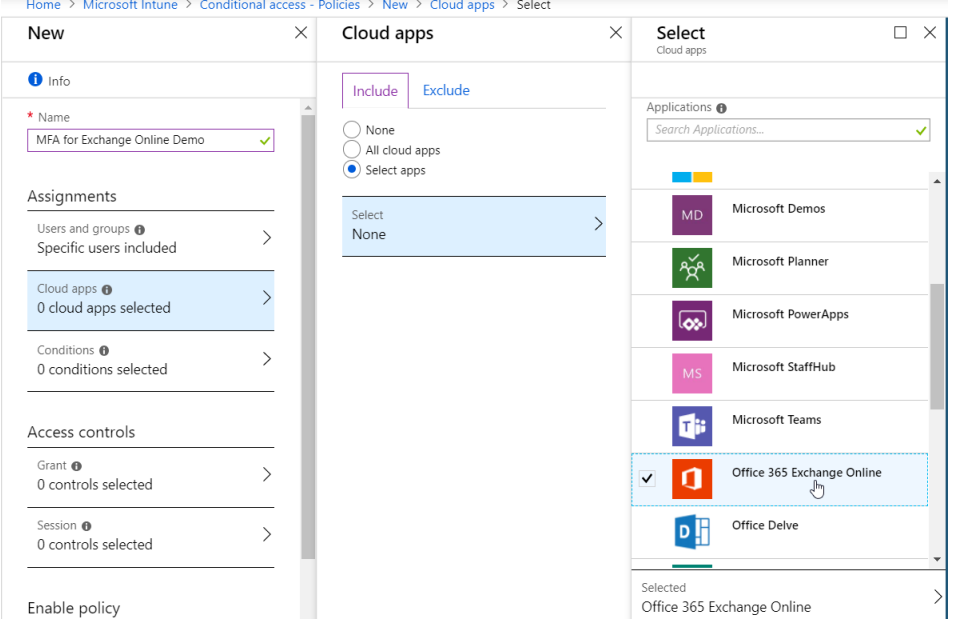
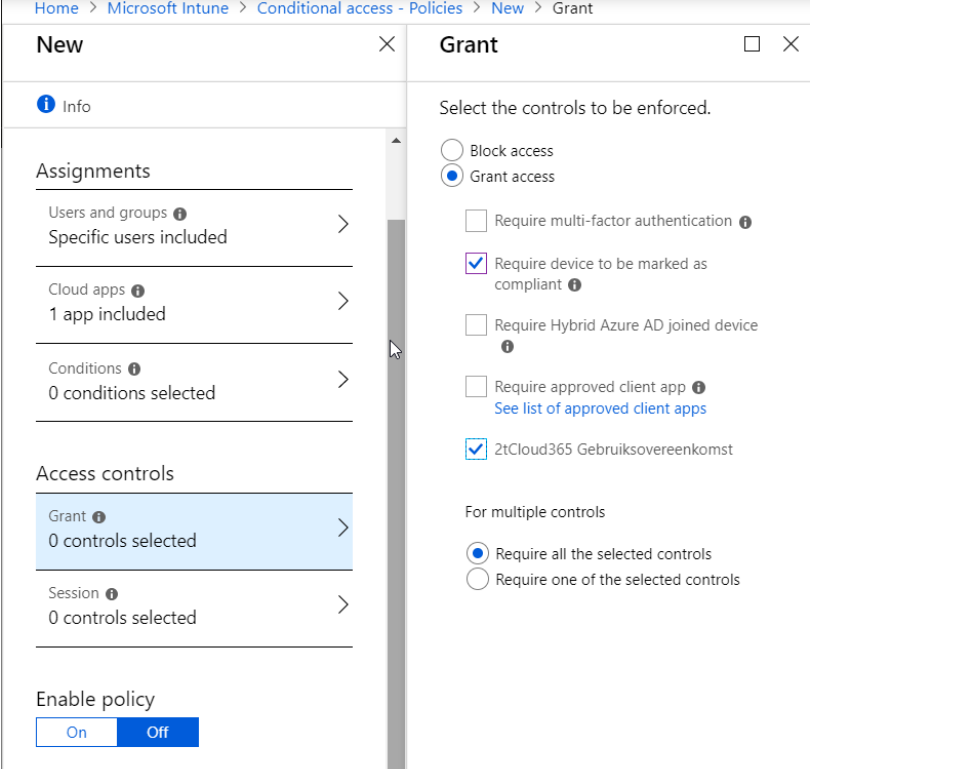
2. Create new -> Configure the settings -> Click **Create**

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

<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

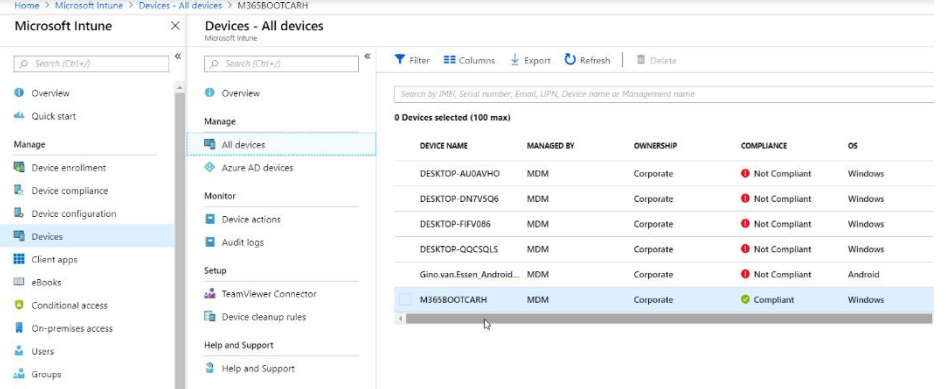
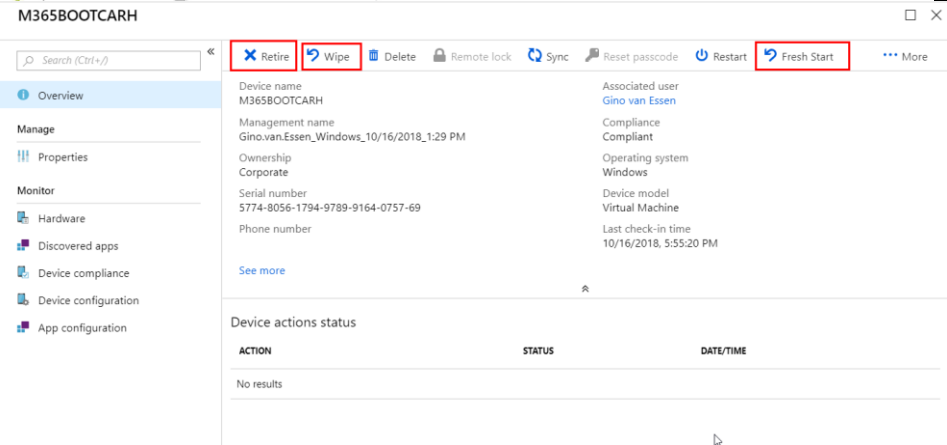
Enable policy

On

Off

Create

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>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>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>