



Modern Workplace Hands-on lab

AAD Premium, Intune, Office ProPlus



Microsoft 365 Business Premium

Lab Guide

Thursday, July 30, 2020

Version 4.0

Prepared by

Gido Veekens
Stephan van de Kruis
Hans van Deursen

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
30-7-2020	Stephan van de Kruis	4.0	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.....	Error! Bookmark not defined.
Activity 2: Prepare Modern workplace with Intune	8
Exercise 2: Create an AAD Group.....	8
Exercise 2a: Configure group-based Licensing	9
Exercise 3: Configure MDM and MAM Intune settings	9
Exercise 4: Activate Self Service Password Reset	9
Exercise 5: Company branding.....	11
Activity 3: Add Windows to MDM	17
Exercise 6: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)	Error! Bookmark not defined.
Exercise 6b – Hyper V Win10 VM	19
Exercise 6c Azure steps OPTIONAL	Error! Bookmark not defined.
Activity 4: Configuration Intune.....	25
Exercise 7: Terms of use	Error! Bookmark not defined.
Exercise 8: Device Settings.....	11
Exercise 9: Device Compliance	25
Exercise 10: Conditional Access.....	43
Exercise 10a: Device Configuration - Windows Device Restrictions.....	27
Exercise 10b: Device Configuration - Windows Device Configuration	30
Exercise 11: Windows 10 Update Rings.....	31
Exercise 12: Office ProPlus Deployment via Intune.....	32
Exercise 13: Windows Store for Business	34
Exercise 14: Company portal	36
Exercise 15: MSI app deployment	39

Exercise 16: Windows Hello 43

Activity 5: Selective Wipe 45

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

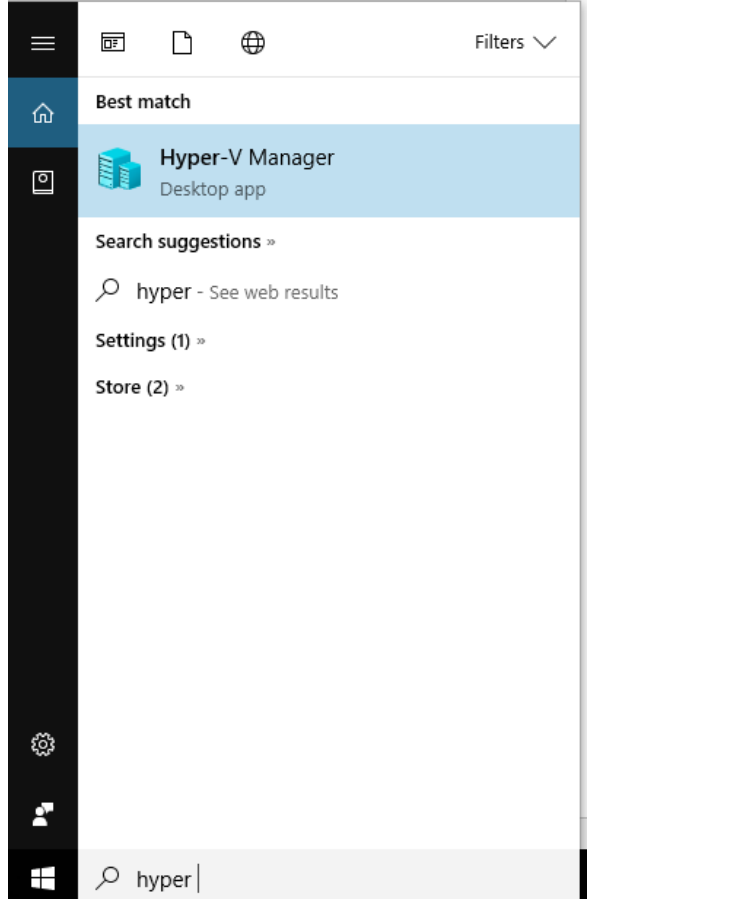
In this activity, you will configure the components necessary to perform this lab:

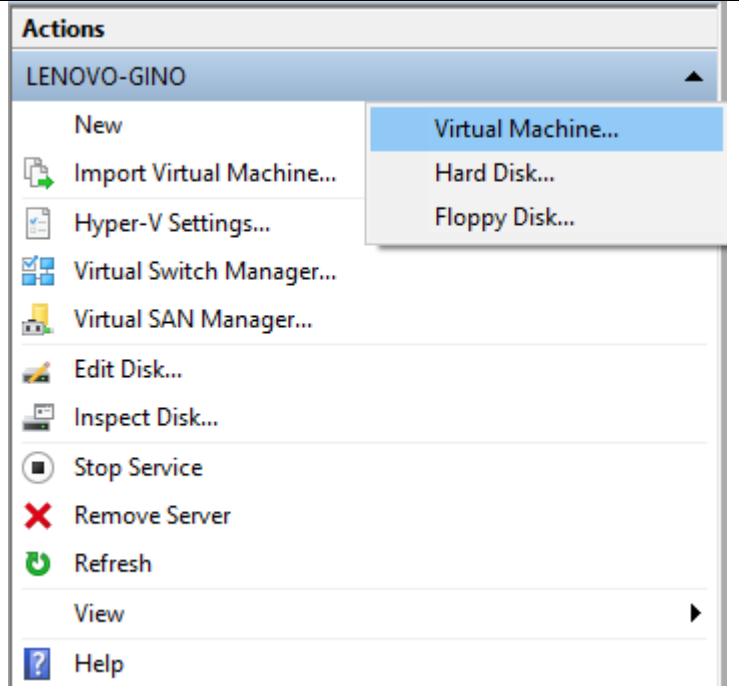
- Windows 10 Enterprise, version 2004 – Hyper-V

When Azure tenant \ subscription is not available

- ISO of Windows 10 Enterprise 2004 handed out by Copaco
- Hyper V Manager VM configuration

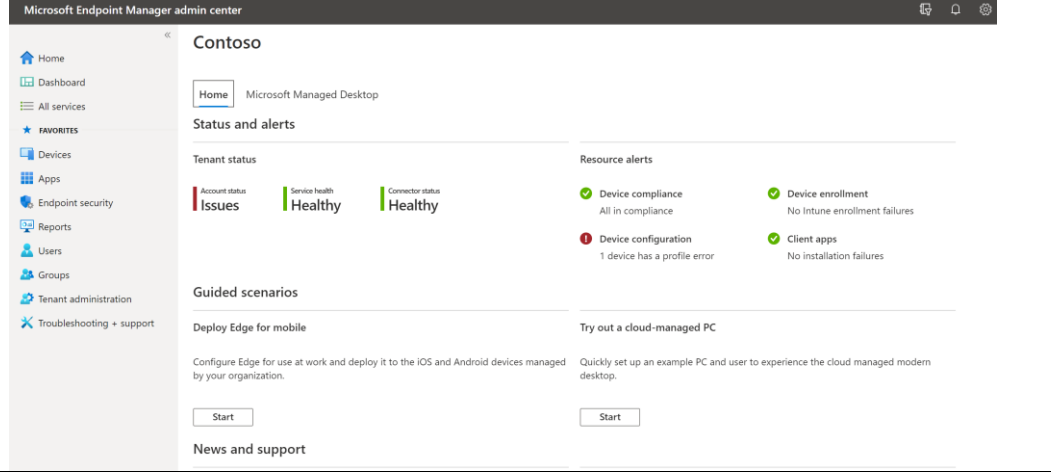
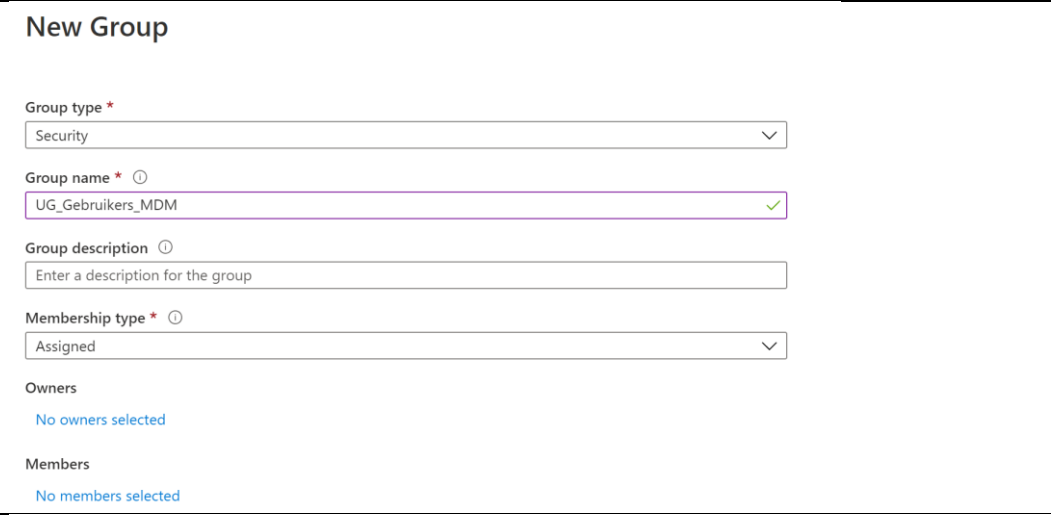
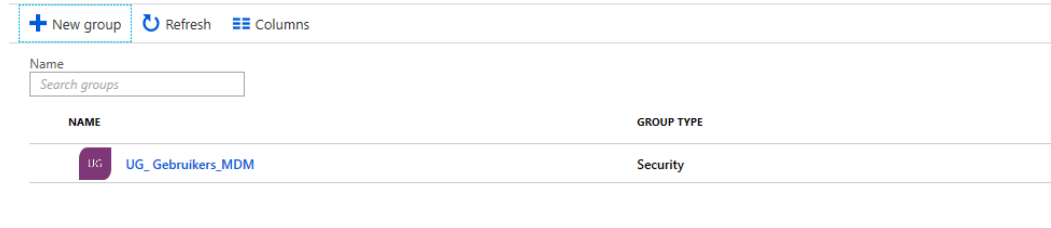
Exercise 1a: Create Windows 10 Enterprise VM

<ol style="list-style-type: none">1. IMPORTANT do not power on the VM2. Open Hyper-v Manager	 A screenshot of the Windows 10 search interface. The search bar at the top contains the text 'hyper'. Below the search bar, the results are categorized into 'Best match', 'Search suggestions', 'Settings', and 'Store'. Under 'Best match', 'Hyper-V Manager' is listed as a 'Desktop app' with a blue icon. Under 'Search suggestions', there is a link for 'hyper - See web results'. Under 'Settings', there is a link for 'Settings (1)'. Under 'Store', there is a link for 'Store (2)'. The Windows taskbar is visible at the bottom with the Start button and a search bar containing 'hyper'.
---	---

<ol style="list-style-type: none">3. Create New > virtual machine4. Name WIN10ENT-20045. Generation Generation 26. Assign Memory 4096 MB7. Configure Networking Connection External8. Create VHD Standard settings9. Installation Options install an OS from a bootable CD/DVD10. Image file: "Win10.iso"11. Finish / complete the configuration12. 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
---	--

Activity 2: Prepare Modern workplace with Endpoint Manager

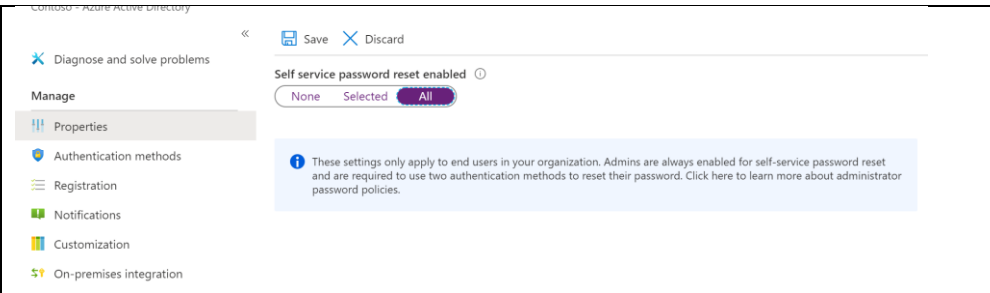
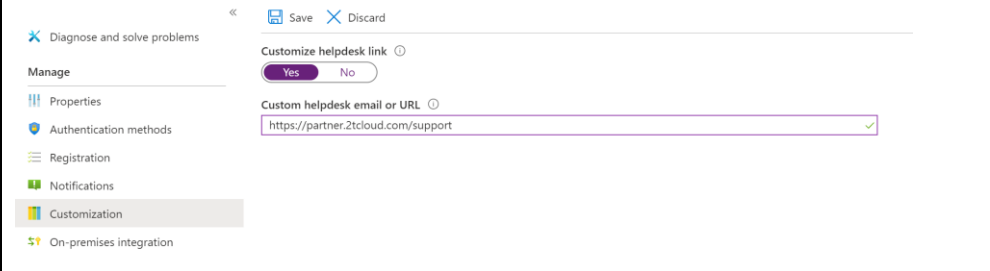
Exercise 2: Create an AAD Group

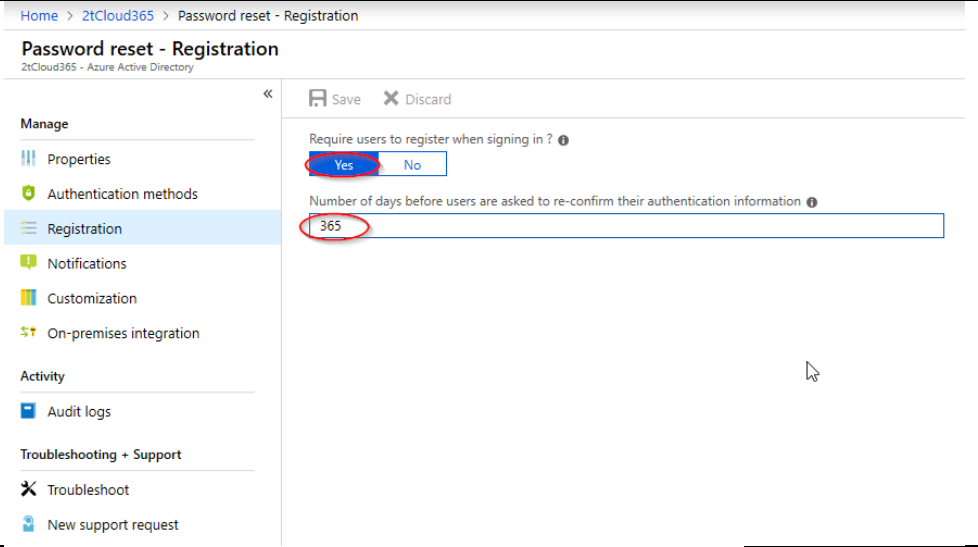
<p>1. Go to : endpoint.microsoft.com</p>	
<p>2. Go to: Groups 3. Click New Group and create a group with the following settings 4. Add Admin account to group "UG_Gebruikers_MDM" 5. Click Create (bottom of screen)</p>	
<p>6. AAD Group "UG_Gebruikers_MDM" is created</p>	

Exercise 2a: Configure group-based Licensing

<ol style="list-style-type: none"> 1. Go to aad.portal.azure.com 2. Go to: Azure Active Directory → Licenses → All products 3. Select Microsoft 365 Business Premium 4. Select Licensed groups 5. Click the Assign button 6. At users and groups search for UG_gebruikers_MDM and select the group 7. At Assignment options make sure that On is selected and click OK 8. Click Assign 	
---	--

Exercise 3: Activate Self Service Password Reset

<ol style="list-style-type: none"> 1. Go to Azure Active Directory->Users ->Password reset 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>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 4: Device Settings

<div>1. Go to Azure Active Directory ->Devices -> Device Settings;</div>	<div><div><div><div><div>Dashboard > Contoso ></div><div>Devices Device settings</div><div>Contoso - Azure Active Directory</div></div><div><div>Save</div><div>Discard</div><div>Got feedback?</div></div><div><div>All devices</div><div>Device settings</div><div>Enterprise State Roaming</div><div>Diagnose and solve problems</div></div><div>Activity</div><div><div>Audit logs</div><div>Troubleshooting + Support</div><div>New support request</div></div></div><div><div>Users may join devices to Azure AD</div><div>AllSelectedNone</div><div>Selected</div><div>No member selected</div><div>Additional local administrators on Azure AD joined devices</div><div>SelectedNone</div><div>Selected</div><div>No member selected</div><div>Users may register their devices with Azure AD</div><div>AllNone</div><div>Learn more on how this setting works</div><div>Require Multi-Factor Auth to join devices</div><div>YesNo</div><div>Maximum number of devices per user</div><div>5</div><div>Enterprise State Roaming</div><div>Manage Enterprise State Roaming settings</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>

Exercise 5: Company branding

<p>1. Go to Azure Active Directory->Company Branding->Edit the default branding policy to your likings</p>	<div data-bbox="667 376 933 412">Edit company branding</div> <div data-bbox="667 412 791 430">Azure Active Directory</div> <div data-bbox="673 443 815 465"> <div>Save</div> <div>Discard</div> </div> <div data-bbox="667 499 866 577"> <p>Sign-in page background image</p> <p>Image size: 1920x1080px</p> <p>File size: <300KB</p> <p>File type: PNG, JPG, or JPEG</p> </div> <div data-bbox="930 495 1150 712"> </div> <div data-bbox="930 719 976 736">Remove</div> <div data-bbox="930 736 1007 757">Select a file</div> <div data-bbox="667 799 916 889"> <p>Banner logo</p> <p>Image size: 280x60px</p> <p>File size: 10KB</p> <p>File type: Transparent PNG, JPG, or JPEG</p> </div> <div data-bbox="930 799 1142 835"> </div> <div data-bbox="930 848 976 866">Remove</div> <div data-bbox="930 866 1007 887">Select a file</div> <div data-bbox="667 927 780 947">Username hint</div> <div data-bbox="930 927 1501 947"> <input type="text"/> </div> <div data-bbox="667 969 798 990">Sign-in page text</div> <div data-bbox="930 969 1501 990"> <input type="text" value="Contoso"/> </div> <div data-bbox="667 1059 794 1077">Advanced settings</div> <div data-bbox="667 1095 882 1115">Sign-in page background color</div> <div data-bbox="930 1095 1501 1115"> <input type="color"/> </div> <div data-bbox="667 1137 866 1214"> <p>Square logo image</p> <p>Image size: 240x240x (resizable)</p> <p>Max file size: 50KB</p> <p>PNG (preferred), JPG, or JPEG</p> </div> <div data-bbox="930 1144 1070 1180"> </div> <div data-bbox="930 1202 976 1220">Remove</div> <div data-bbox="930 1220 1007 1240">Select a file</div> <div data-bbox="667 1281 861 1301">Square logo image, dark theme</div> <div data-bbox="930 1281 1070 1301"> </div>								
<p>2. Configure the settings -> Click Save</p>	<table border="1"> <tr> <td>Sign-in page image</td><td>Add image</td></tr> <tr> <td>Banner image</td><td>Add image</td></tr> <tr> <td>User name hint</td><td>gebruikersnaam@2tcloud365.nl</td></tr> <tr> <td>Show option to remain signed in</td><td>No</td></tr> </table>	Sign-in page image	Add image	Banner image	Add image	User name hint	gebruikersnaam@2tcloud365.nl	Show option to remain signed in	No
Sign-in page image	Add image								
Banner image	Add image								
User name hint	gebruikersnaam@2tcloud365.nl								
Show option to remain signed in	No								

3. Go to **Endpoint Manager -> Tenant Administration -> Customization**
4. Edit the details to your liking

Home > Tenant admin | Customization

This is the default customization that is applied to all users and devices. It can be edited, but not deleted.

Search (Ctrl+ /) << Edit

Branding

Organization name	--
Theme color	#0072c6
Show in header	Organization name only

Support information

Contact name	--
Phone number	--
Email address	--
Website name	--
Website URL	--
Additional information	--

Configuration

Device enrollment	Available, with prompts
Privacy message in Company Portal for iOS/iPadOS	Default
Privacy statement URL	--
Send a push notification to users when their device ownership type changes from personal to corporate (Android and	No

Exercise 6 Set MDM authority to Intune

This step is optional, most likely this is already the case. To confirm go to Azure Active Directory → Mobility (MDM and MAM)

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.

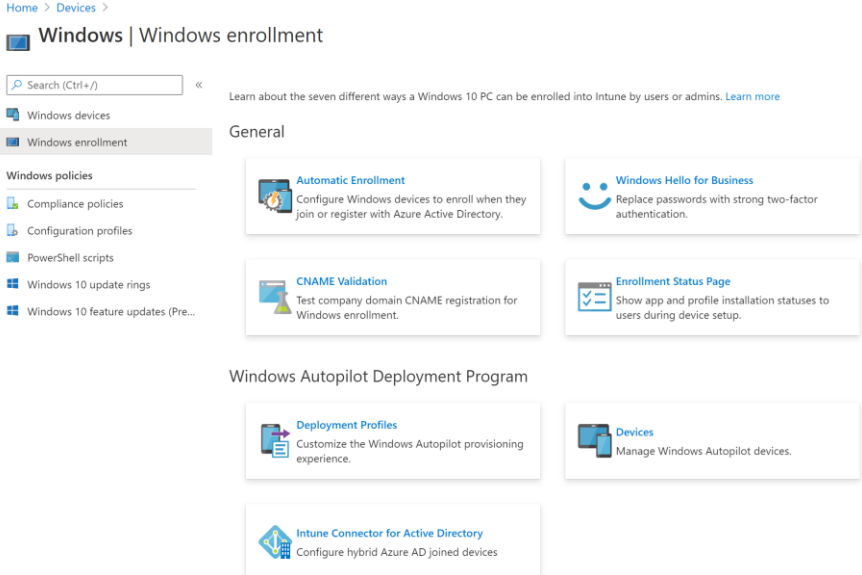
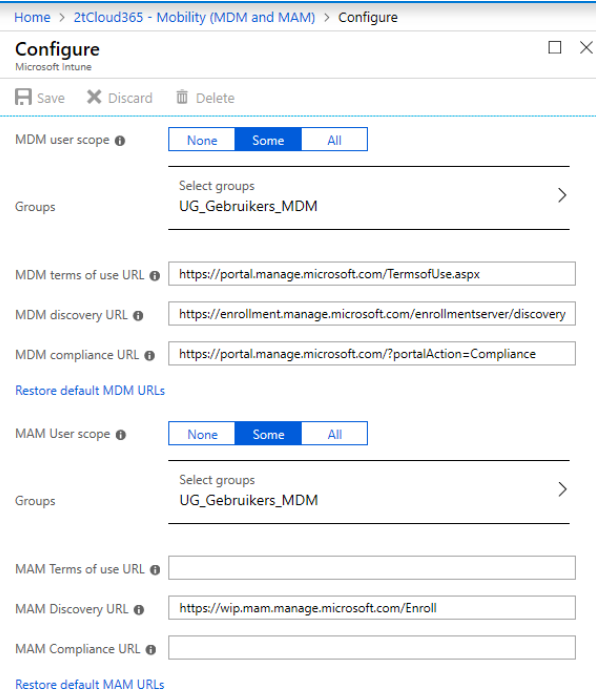
Choose Configuration Manager as your MDM authority to manage mobile devices with System Center Configuration Manager and Microsoft Intune.

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

Learn more about [choosing your MDM Authority](#).

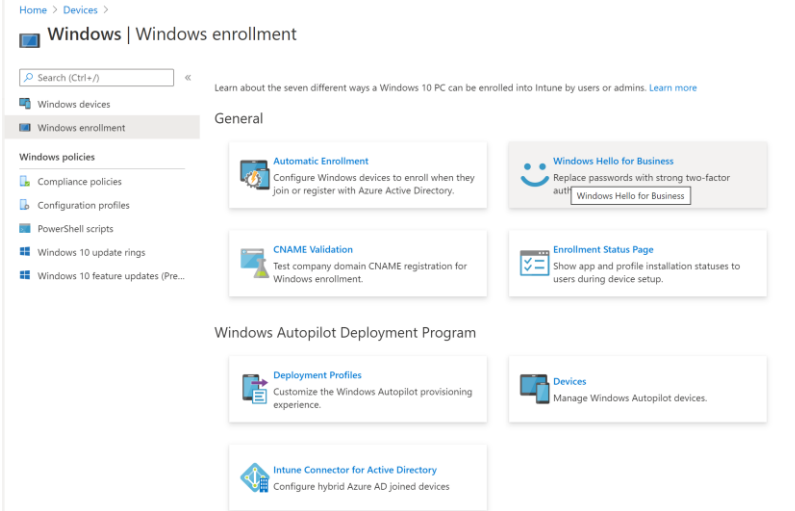
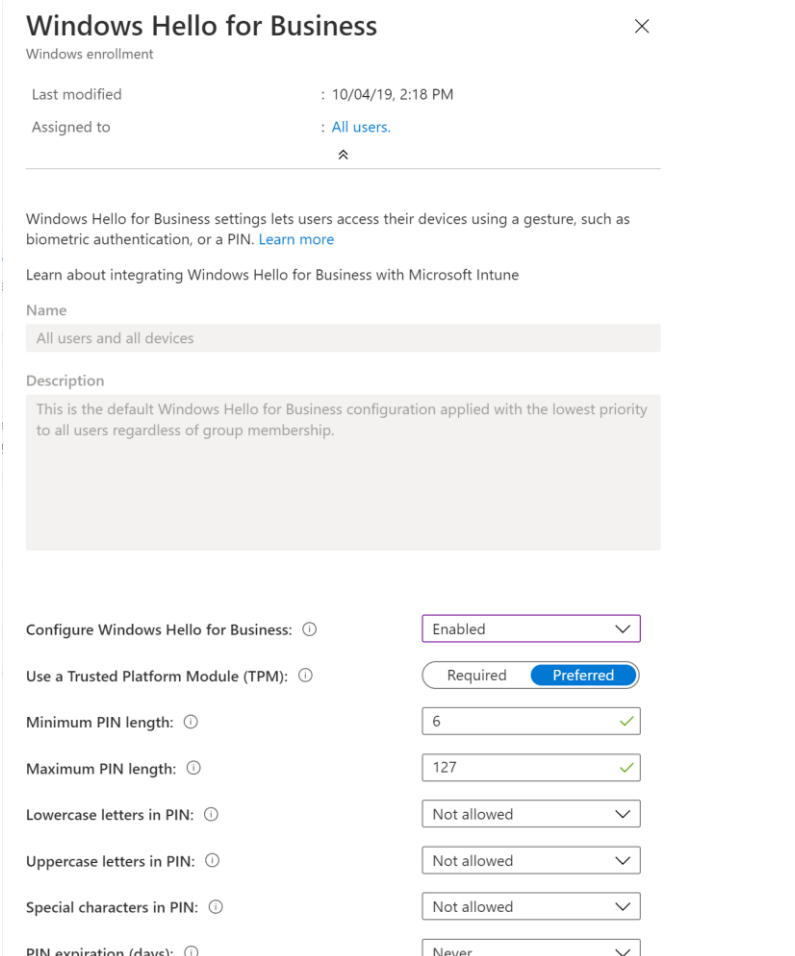
- ☒ Intune MDM Authority
- ☐ Configuration Manager MDM Authority
- ☐ None

Exercise 7: Configure MDM and MAM Intune settings

<ol style="list-style-type: none"> Go to endpoint.microsoft.com Go to Devices -> Windows -> Windows Enrollment. Select Automatic Enrollment Go to Azure Active Directory->Mobility (MDM and MAM)->Microsoft Intune. 											
<ol style="list-style-type: none"> Configure the settings -> Click on Save 	<table border="1" data-bbox="619 936 1284 1182"> <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										

Exercise 8: Windows Hello for Business

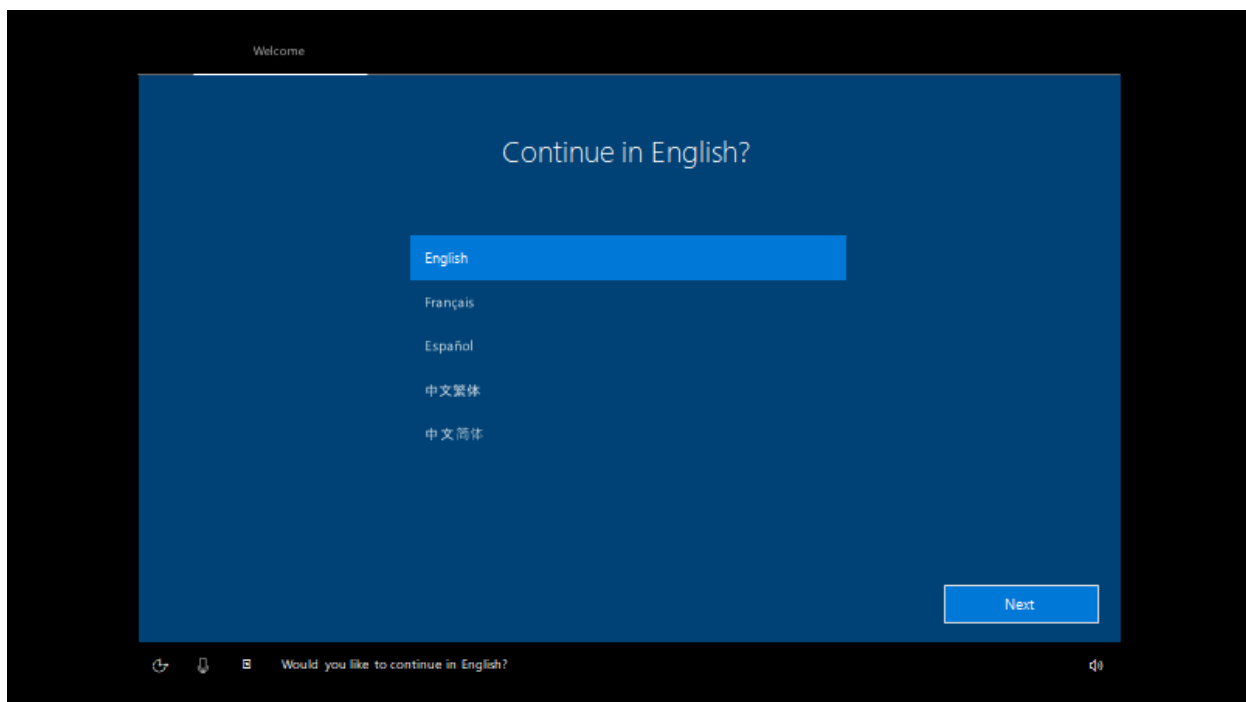
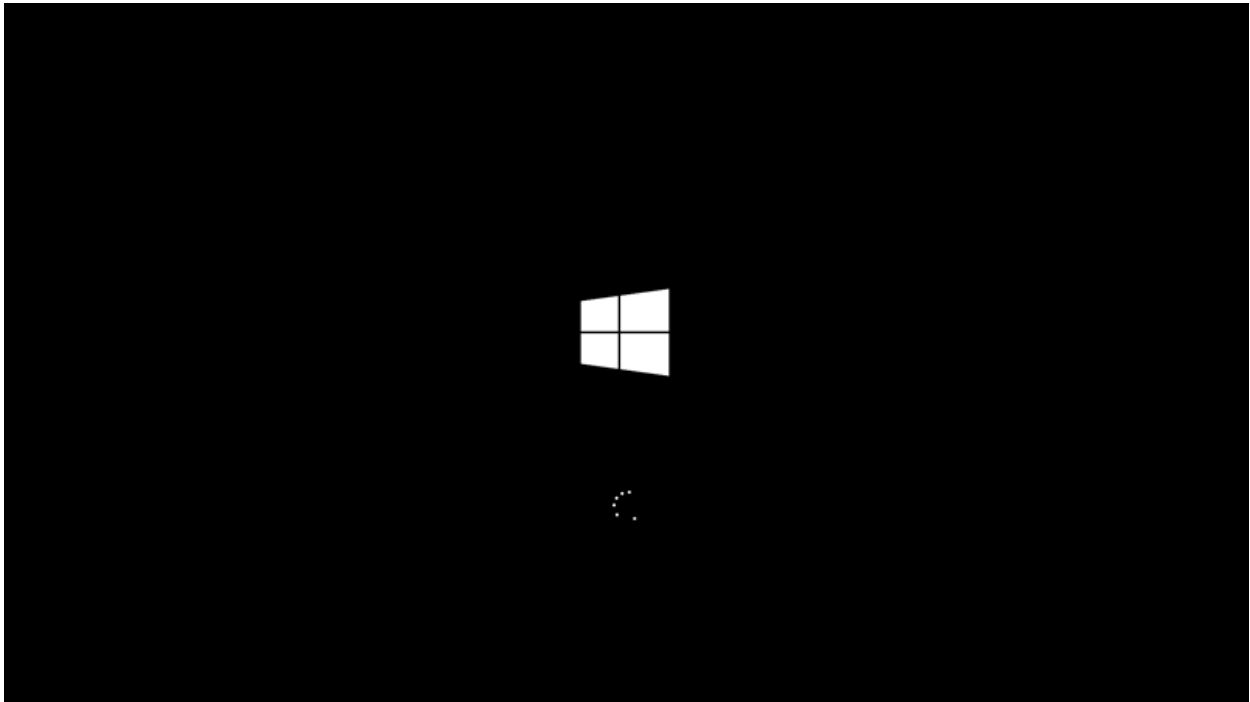
With Windows Hello you can allow user to access their devices using a gesture, such as biometric authentication, or a PIN.

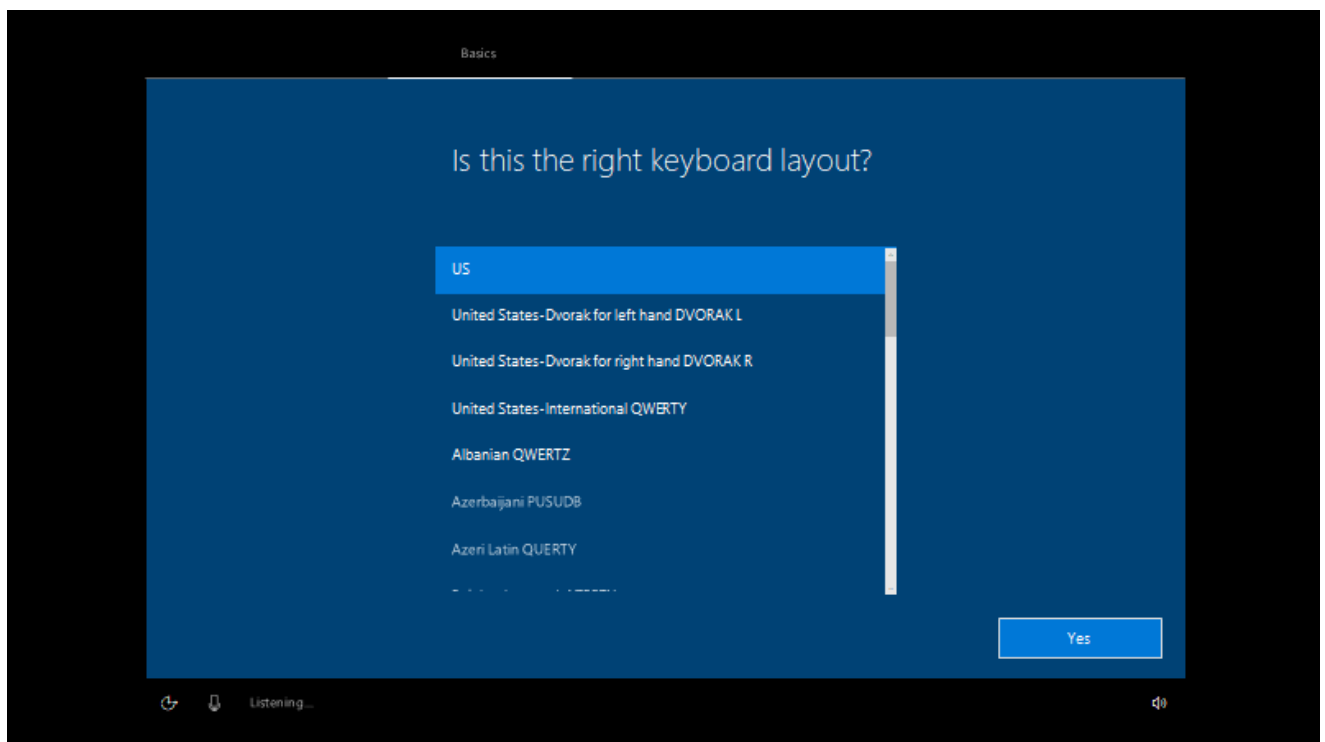
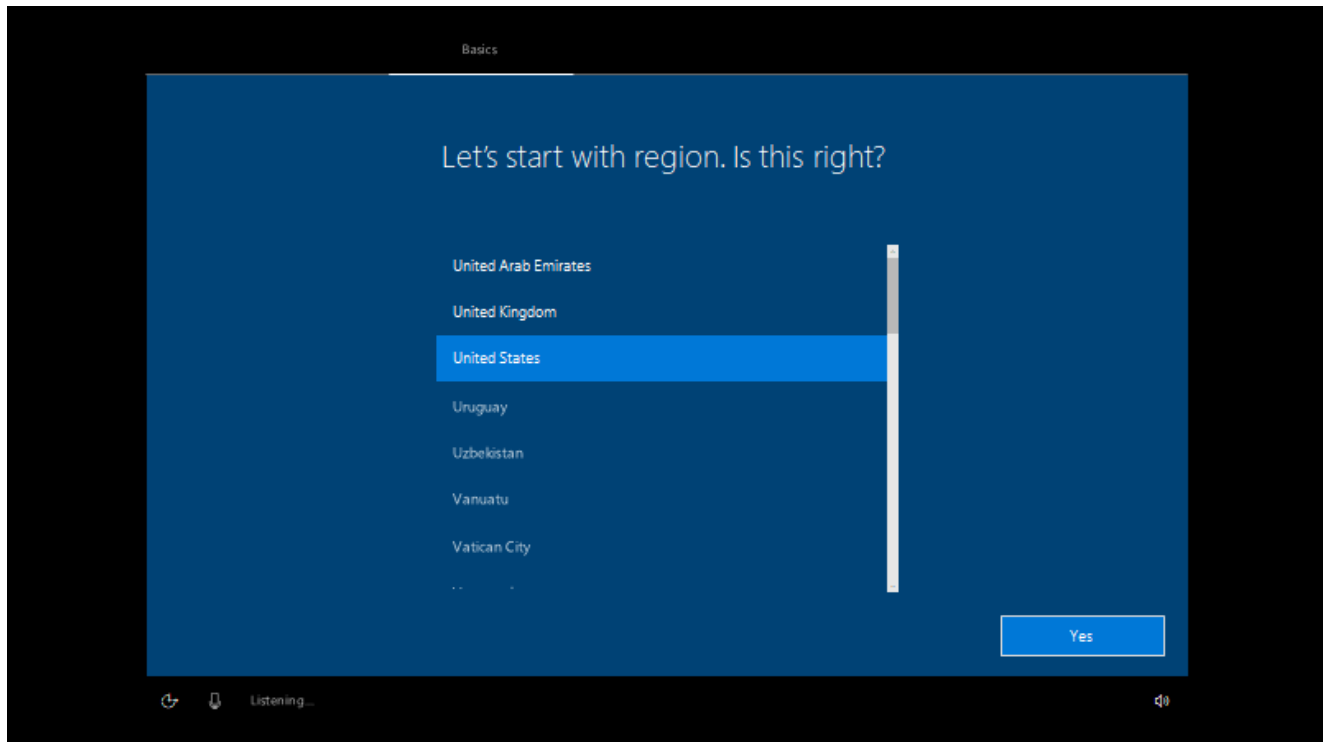
<ol style="list-style-type: none"> 1. Go to Endpoint.microsoft.com 2. Select Devices -> Windows Devices -> Windows Enrollment 3. Select Windows Hello For Business 	
<ol style="list-style-type: none"> 1. Select settings 2. At Configure Windows for Business select Enabled. 3. You can leave the default settings 4. And select Save 	

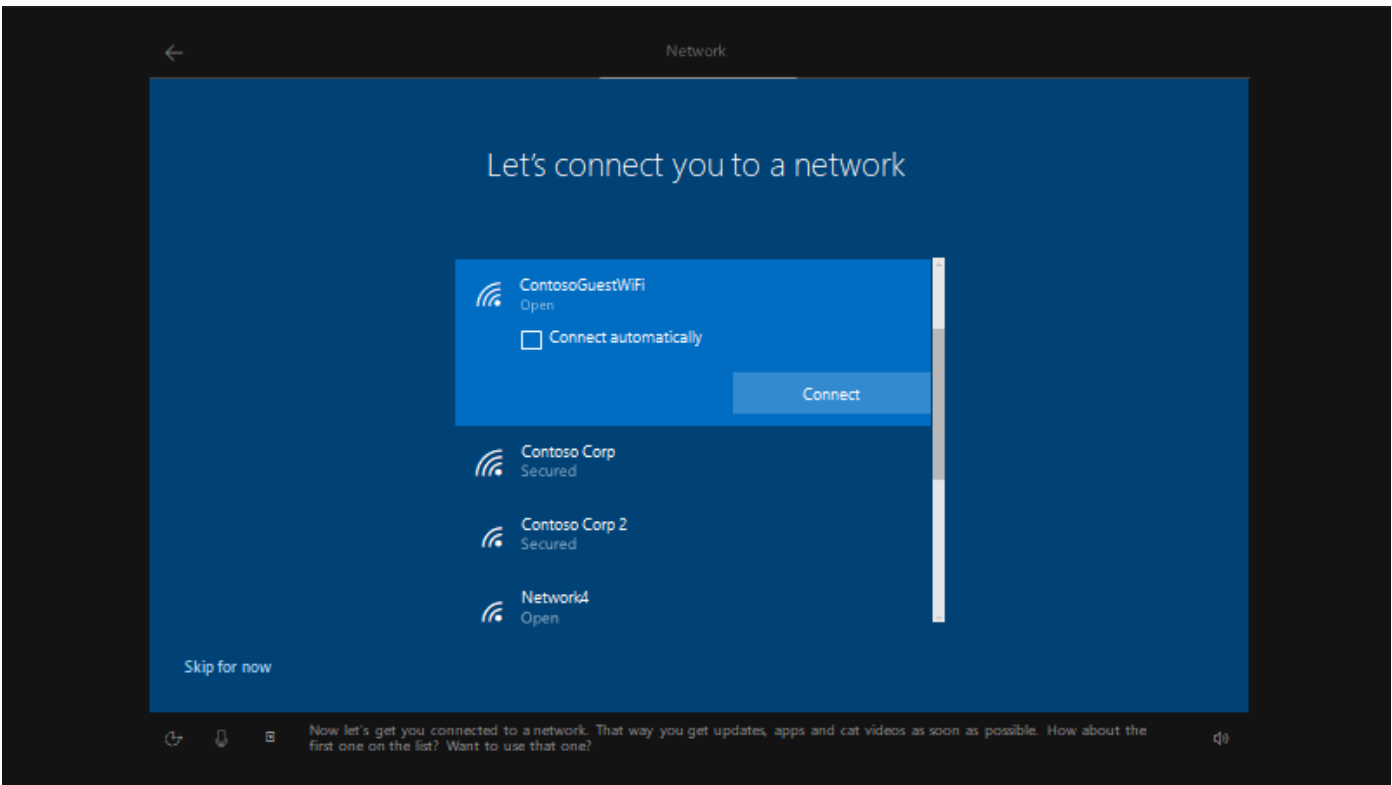
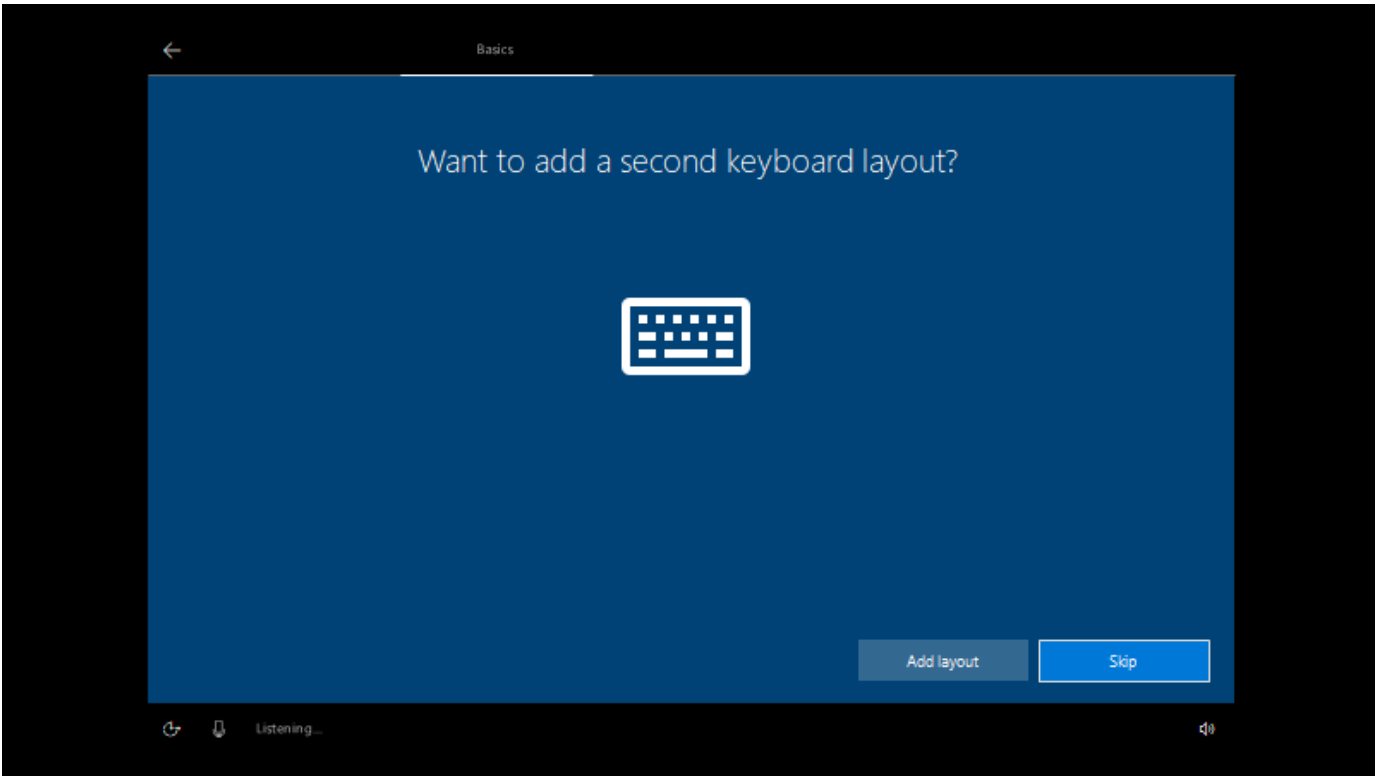
Activity 3: Add Windows to MDM

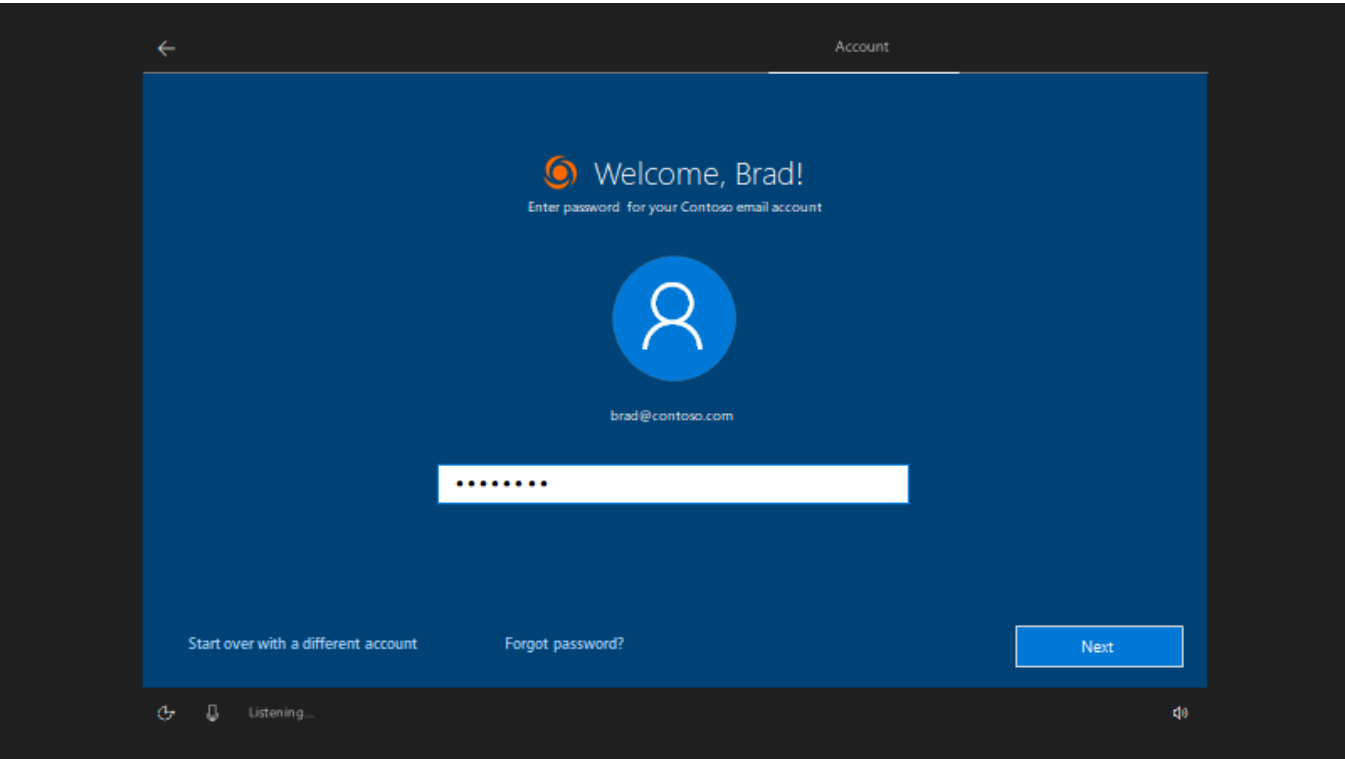
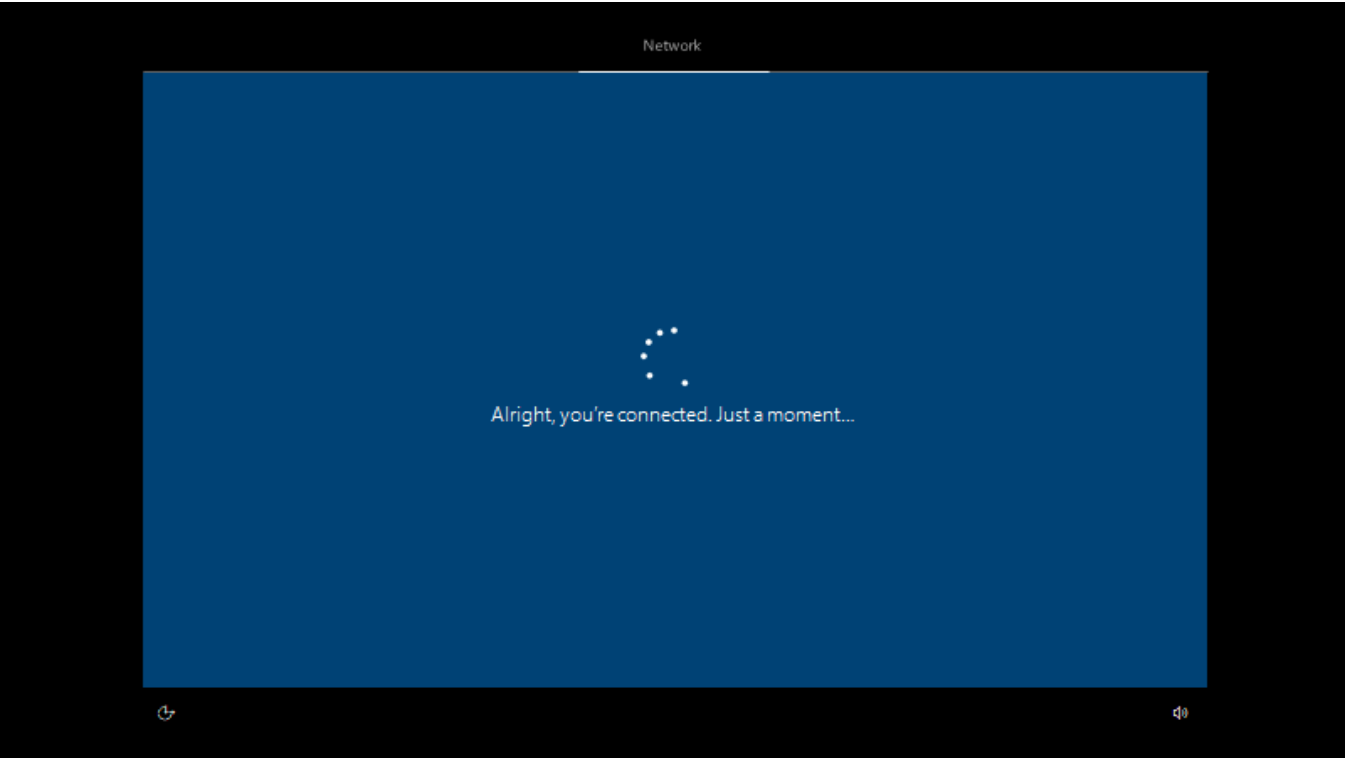
Exercise– Hyper V Win10 VM

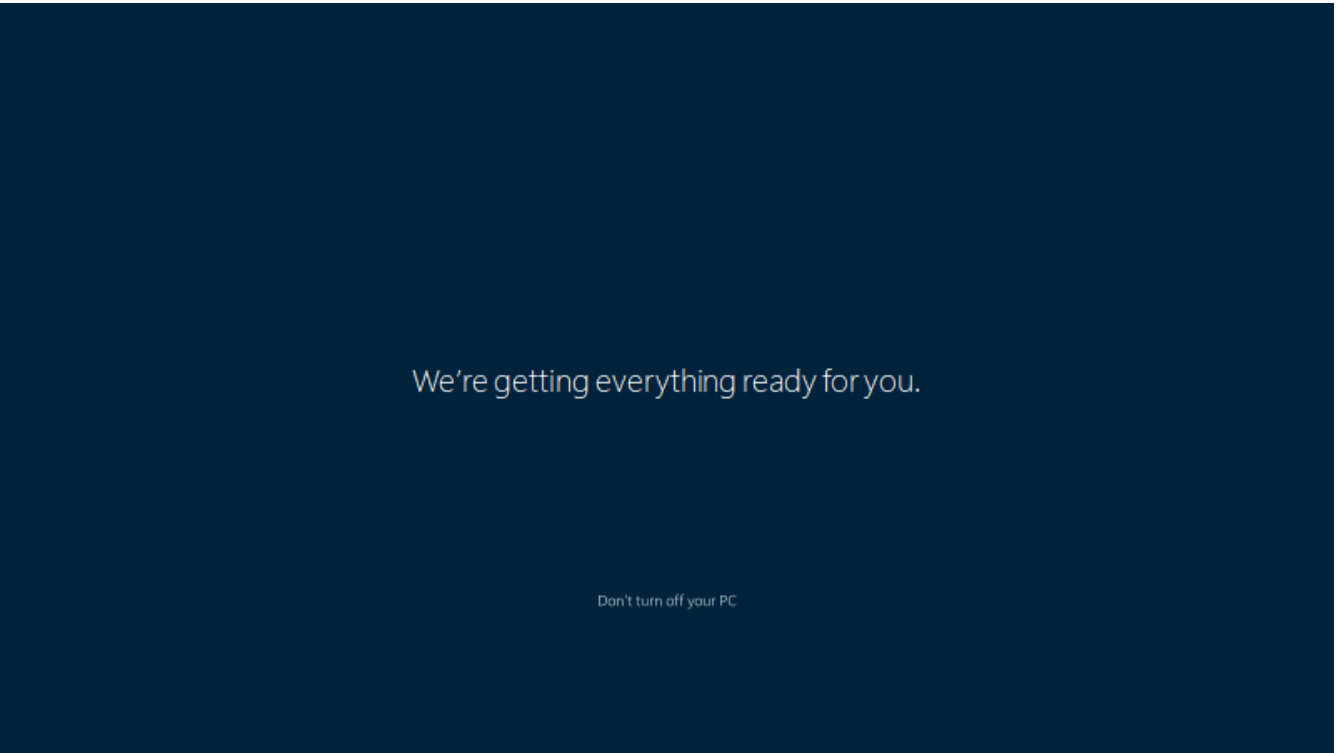
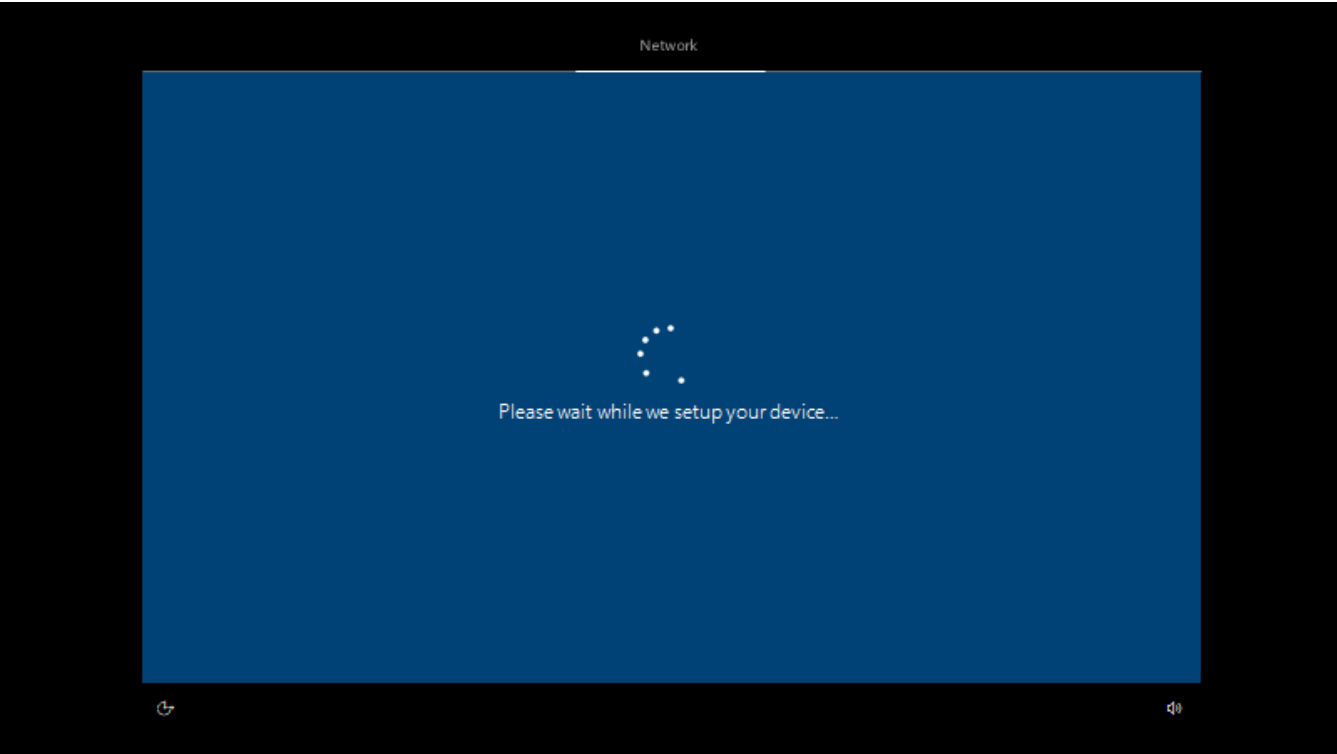
Start the setup of the Windows 10 Enterprise OS, and sign in with your test account









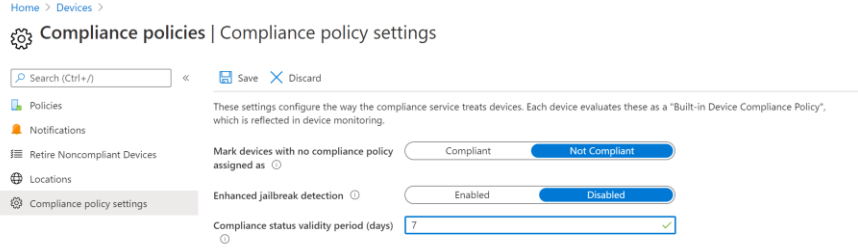
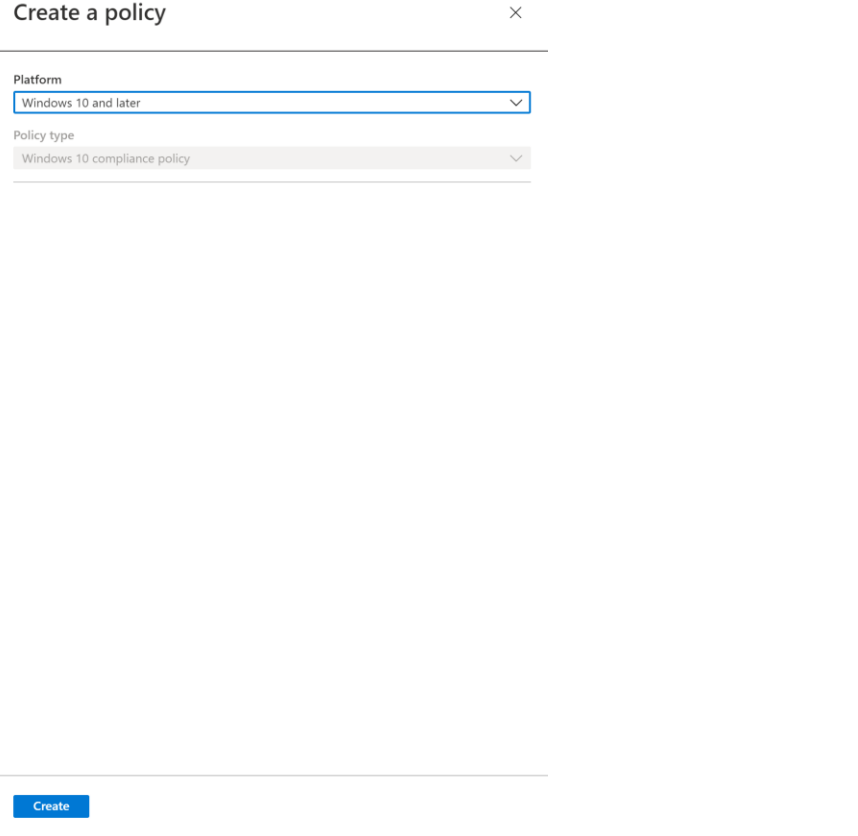
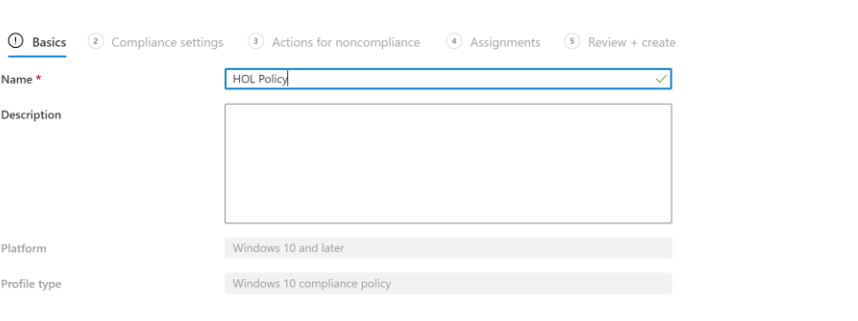


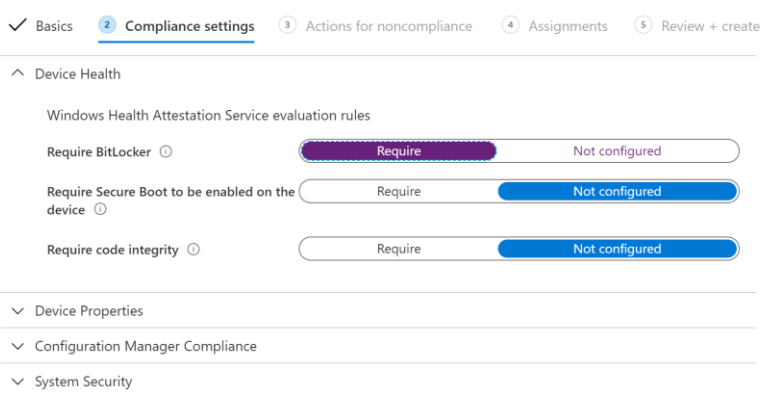
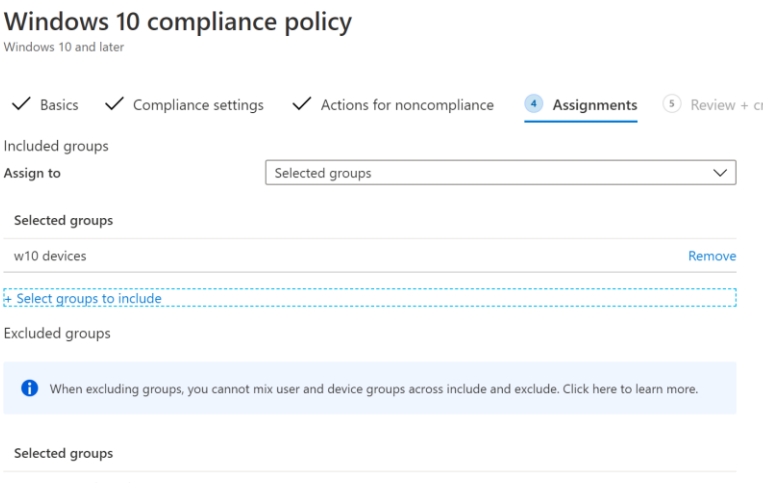
We're getting everything ready for you.

Don't turn off your PC

Activity 4: Configuration Intune

Exercise 10: Device Compliance

<p>1. Go to Endpoint Manager->Devices -> Compliance policies -> Compliance policy settings</p>			
<p>2. Configure the settings > Click Save</p>	<p>Mark devices with no compliance</p>	<p>Not Compliant</p>	
	<p>Enhanced Jailbreak detection</p>	<p>Enabled</p>	
	<p>Compliance status validity period</p>	<p>7</p>	
<p>3. Go to Endpoint Manager->Devices -> Compliance policies 4. Create Policy 5. Select platform Windows 10 and later and select Create</p>			
<p>6. Give the policy a Name and select next</p>			

<p>7. Select Device Health and require Bitlocker</p> <p>8. Select Next</p> <p>9. Select Next</p>	
<p>10. For assignments select the group UG_Gebruikers_MDM</p>	

Exercise 11a: Device Configuration - Windows Device Restrictions

<ol style="list-style-type: none"> Go to Devices -> Configuration Profiles -> Create Profile Select Platform Windows 10 and Later Select Profile Device Restrictions Select Create 	<div> <div>Create a profile</div> <div> <div>Platform</div> <div>Windows 10 and later</div> </div> <div> <div>Profile</div> <div>Device restrictions</div> </div> <div>Device restrictions</div> </div>
<ol style="list-style-type: none"> Give the policy a Name and select NExt 	
<ol style="list-style-type: none"> Configure settings as showed on the screenshot (Password) 	<div> <div> <div>^ Password</div> <div> <div> <div>Password</div> <div>Require</div> <div>Not configured</div> </div> <div> <div>Required password type</div> <div>Alphanumeric</div> </div> <div> <div>Password complexity *</div> <div>Numbers and lowercase letters required</div> </div> <div> <div>Minimum password length</div> <div>8</div> <div>✓</div> </div> <div> <div>Number of sign-in failures before wiping device</div> <div>5</div> <div>✓</div> </div> <div> <div>Maximum minutes of inactivity until screen locks</div> <div>1 Minute</div> </div> <div> <div>Password expiration (days)</div> <div>41</div> </div> <div> <div>Prevent reuse of previous passwords</div> <div>Enter a number (1-24)</div> </div> <div> <div>Require password when device returns from idle state (Mobile and Holographic)</div> <div>Require</div> <div>Not configured</div> </div> <div> <div>Simple passwords</div> <div>Block</div> <div>Not configured</div> </div> <div> <div>Automatic encryption during AADJ</div> <div>Block</div> <div>Not configured</div> </div> <div> <div>Federal Information Processing Standard (FIPS) policy</div> <div>Allow</div> <div>Not configured</div> </div> <div> <div>Windows Hello device authentication</div> <div>Allow</div> <div>Not configured</div> </div> <div> <div>Preferred Azure AD tenant domain</div> <div>contoso.com</div> </div> </div> </div> </div>
<ol style="list-style-type: none"> Configure settings as showed on the screenshot (Personalization) 	<div> <div> <div>^ Personalization</div> <div> <div>Desktop background picture URL (Desktop only)</div> <div>https://fabrikam.com/image.png</div> </div> </div> </div>

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

^ Locked Screen Experience

Action center notifications (mobile only) ☐ Block ☒ Not configured

Locked screen picture URL (Desktop only) ✓

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)

Voice activate apps from locked screen ☐ Not configured ✓

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

^ Microsoft Edge Browser

Use Microsoft Edge kiosk mode ☐ No ✓

^ Start experience

Start Microsoft Edge with ☐ Start pages in local app settings ✓

Allow user to change Start pages ☐ Yes ☒ No

Allow web content on new Tab page ☒ Yes ☐ No

New Tab URL

Home button ☐ Start pages ✓

Allow Users to change Home button ☐ Yes ☒ No

Show First Run Experience page (Mobile only) ☒ Yes ☐ No

First Run Experience URL list location ✓

Allow pop-ups ☒ Yes ☐ No

Send intranet traffic to Internet Explorer ☐ Yes ☒ No

Enterprise mode site list location (Desktop only)

Message when opening sites in Internet Explorer ☐ Don't show message ✓

Allow Microsoft compatibility list ☒ Yes ☐ No

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

Control Panel and Settings

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

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

Device restrictions
Windows 10 and later

✓ Basics ✓ Configuration settings **3 Assignments** 4 Applicability Rules 5 Review + create

Included groups

Assign to

Selected groups

No groups selected

[+ Select groups to include](#)

Excluded groups

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

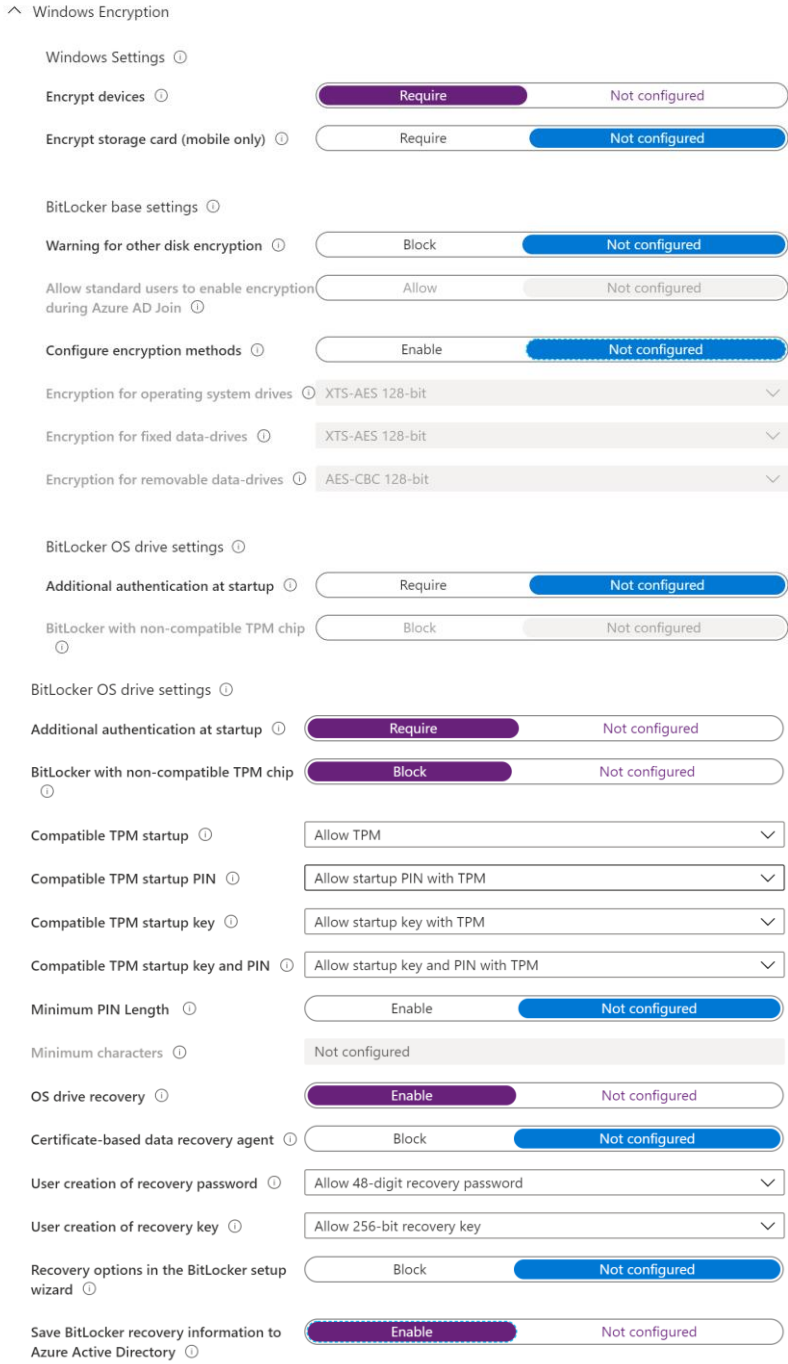
Selected groups

No groups selected

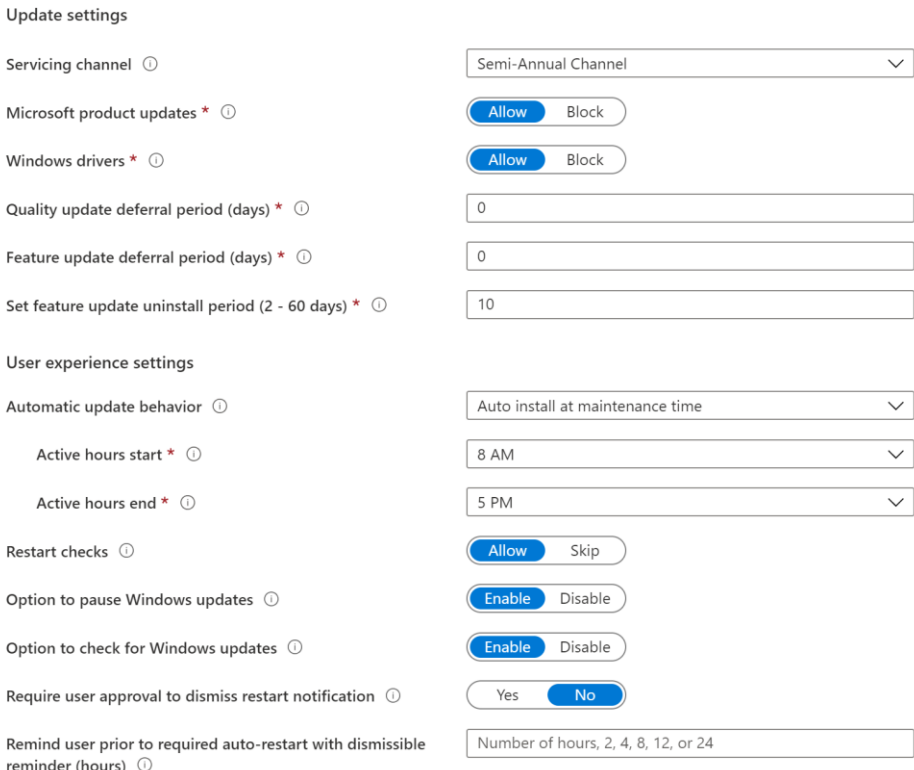
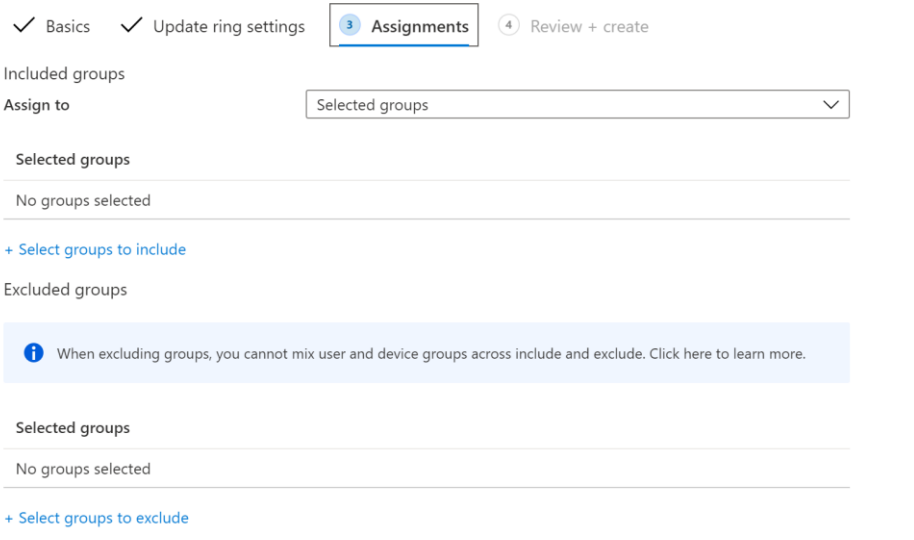
[+ Select groups to exclude](#)

Exercise 12b: Device Configuration - Windows Device Configuration

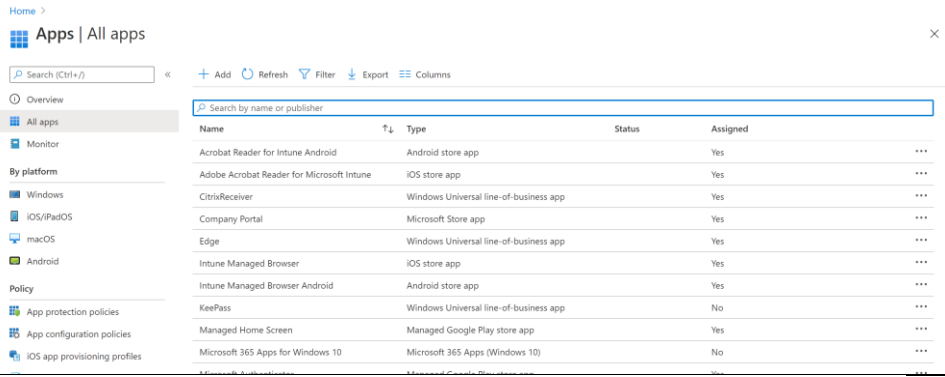
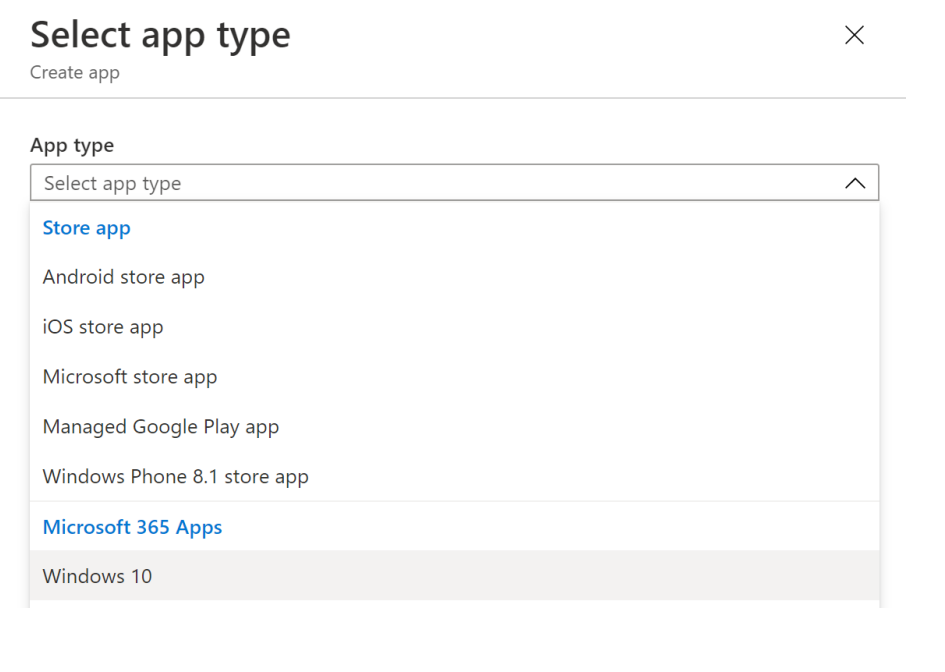
We are going to configure Bitlocker.

<ol style="list-style-type: none"> 1. Go to Enpoint Manager -> Devices -> Configuration Profiles-> Create Profile 2. Select Windows 10 and Later and Enpoint Protection 3. Give the Policy a Name en select Next 4. Configure the Windows Encryption section as shown in the screenshot 	
<ol style="list-style-type: none"> 5. Save the Configuration and assign the Configuration to the UG_gebruikers_MDM group 	

Exercise 12: Windows 10 Update Rings

<ol style="list-style-type: none"> Go to Endpoint Manager -> Devices -> Windows 10 update rings Click "Create Profile" Give the update ring a name and select Next Configure settings as showed on the screenshot 	
<ol style="list-style-type: none"> Assign the Windows 10 Update Ring to Group "UG_Gebruikers_MDM" 	

Exercise 13: Office ProPlus Deployment via Intune

<ol style="list-style-type: none"> 1. Go to Endpoint Manager -> Apps -> All Apps 	
<ol style="list-style-type: none"> 2. Add a App with App type "Microsoft 365 apps -> Windows 10" 3. On the App suite information page leave the defaults and select Next 	

4. On the Configure app suite configure the settings as shown in the screen shot.
5. Assign the app to MDM users group

Add Microsoft 365 Apps

Microsoft 365 Apps (Windows 10)

✓ App suite information 2 **Configure app suite** 3 Assignments 4 Review + create

Configuration settings format * Configuration designer

Configure app suite

Select Office apps 10 selected

Select other Office apps (license required) 0 selected

App suite information

These settings apply to all apps you have selected in the suite. [Learn more](#)

Architecture 32-bit 64-bit

Update channel * Current Channel

Remove other versions Yes No

Version to install Latest Specific

Specific version Latest version

Properties

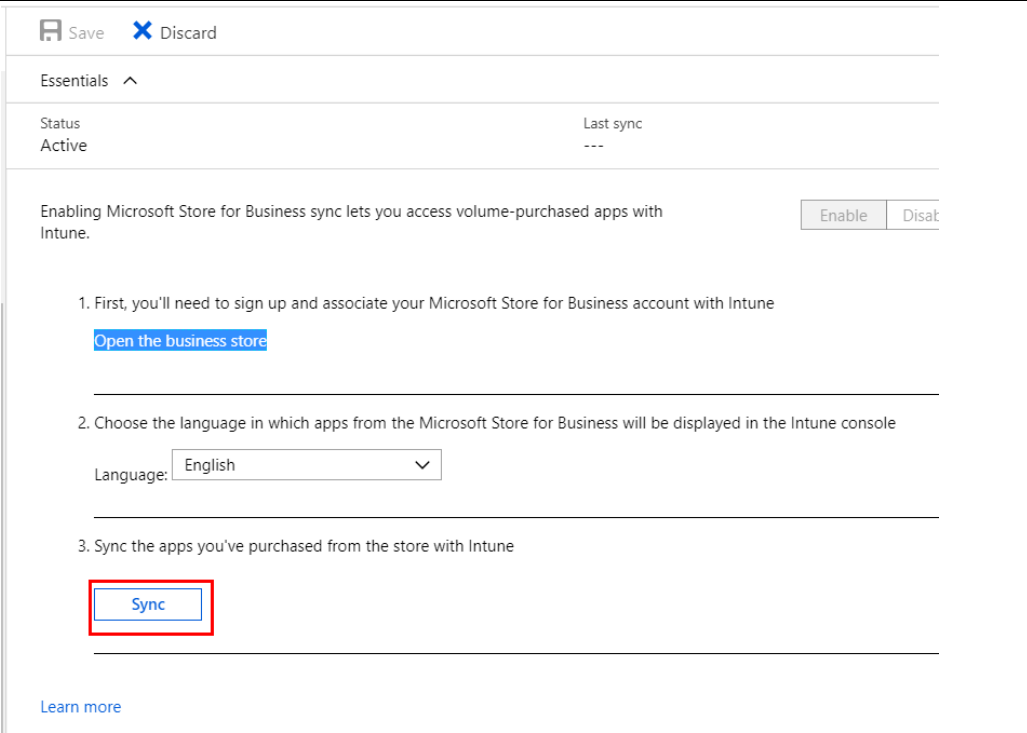
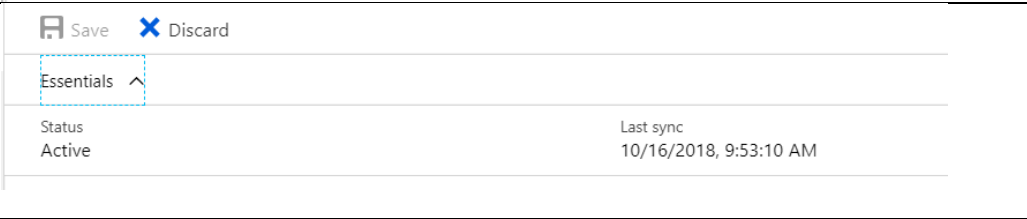
Use shared computer activation Yes No

Accept the Microsoft Software License Terms on behalf of users Yes No

Install background service for Microsoft Search in Bing Yes No

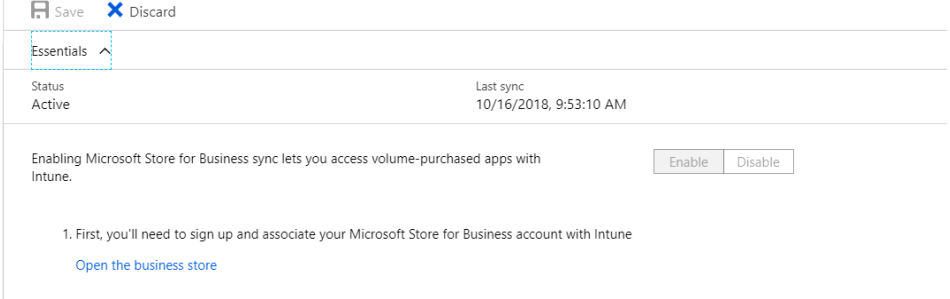
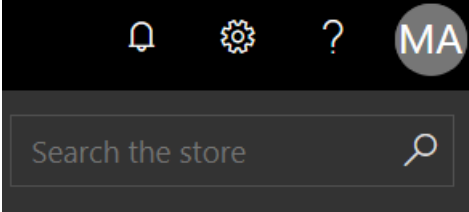
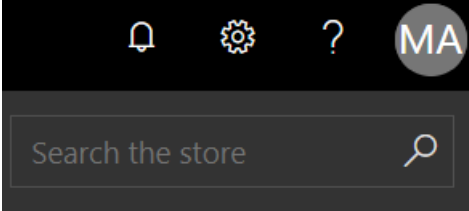
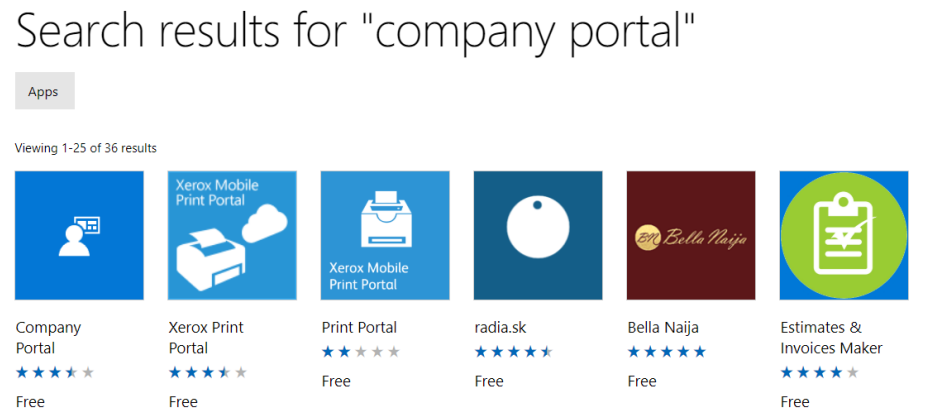
Exercise 14: Windows Store for Business

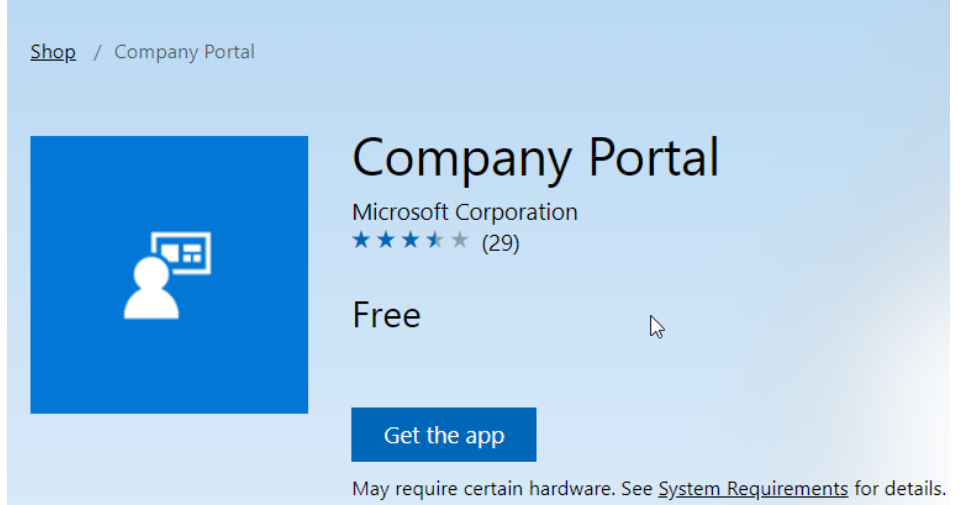

<p>Go to Endpoint manager -</p> <p>> Tenant administration -></p> <p>Connectors and tokens →</p> <p>Microsoft store for Business</p> <p>1. There you select Enable and press Save</p>	<div><div><div>Save</div><div>Discard</div></div><div><div>Status</div><div>Last sync</div></div><div><div>Not set up</div><div>--</div></div><div>Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. <div>Enable</div> <div>Disable</div></div><div><div>1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune</div><div>Open the business store</div></div><div><div>2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console</div><div>Language: <div>English</div></div></div><div><div>3. Sync the apps you've purchased from the store with Intune</div><div>Sync</div></div></div>									
<p>2. After that you can select the link open</p> <p>Open the business store</p> <p>3. Sign in with your AAD account</p>	<div><div>https://businessstore.microsoft.com/en-us/store</div><div>Microsoft Store for Business</div><div>Shop for my group Find a solution provider Search the store</div><div>Sign in</div></div>									
<p>4. Once your signed in select manage</p> <p>5. Accept any terms and license agreements</p>	<div><div>Microsoft Store for Business</div><div>Shop for my group Private store Manage Find a solution provider</div></div>									
<p>Go to settings → Distribute</p> <p>6. Activate Microsoft Intune and Microsoft Intune Enrollment</p>	<div><div><div>Microsoft Store for Business</div><div>Shop for my group Private store Manage Find a solution provider</div><div><div>Home</div><div>Quotes</div><div>Products & services</div><div>My organization</div><div>Devices</div><div>Billing</div><div>Order history</div><div>Partners</div><div>Permissions</div><div>Settings</div><div>Support</div></div><div><div>Shop</div><div>Distribute</div><div>Devices</div><div>Notifications</div><div>Private store</div><div>These settings control the private store, which allows you to curate online apps for distribution to people in your organization</div><div>Your private store name: Contoso Change</div><div>Management tools</div><div>These settings allow you to configure a mobile device management (MDM) tool to synchronize your Microsoft Store for Business inventory</div><div>Pick a tool from the list to activate. Is your tool not on the list? Make sure it's in your Azure Active Directory. Still not there? Select Add management tool below. Get more info</div><div>+ Add management tool</div><div><table><tr><th>Tool</th><th>Status</th><th>Action</th></tr><tr><td>Microsoft Intune</td><td>Inactive</td><td>Activate</td></tr><tr><td>Microsoft Intune Enrollment</td><td>Inactive</td><td>Activate</td></tr></table></div></div></div></div>	Tool	Status	Action	Microsoft Intune	Inactive	Activate	Microsoft Intune Enrollment	Inactive	Activate
Tool	Status	Action								
Microsoft Intune	Inactive	Activate								
Microsoft Intune Enrollment	Inactive	Activate								



<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, the 'Status' is 'Active' and '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. Sign up and associate your Microsoft Store for Business account with Intune, with 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, with a dropdown menu set to 'English'. 3. Sync the apps you've purchased from the store with Intune, with a 'Sync' button highlighted by a red rectangle. 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>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, indicating the process is complete.</p>
<p>9. At this point you can deploy apps from the Windows Store for Business</p>	

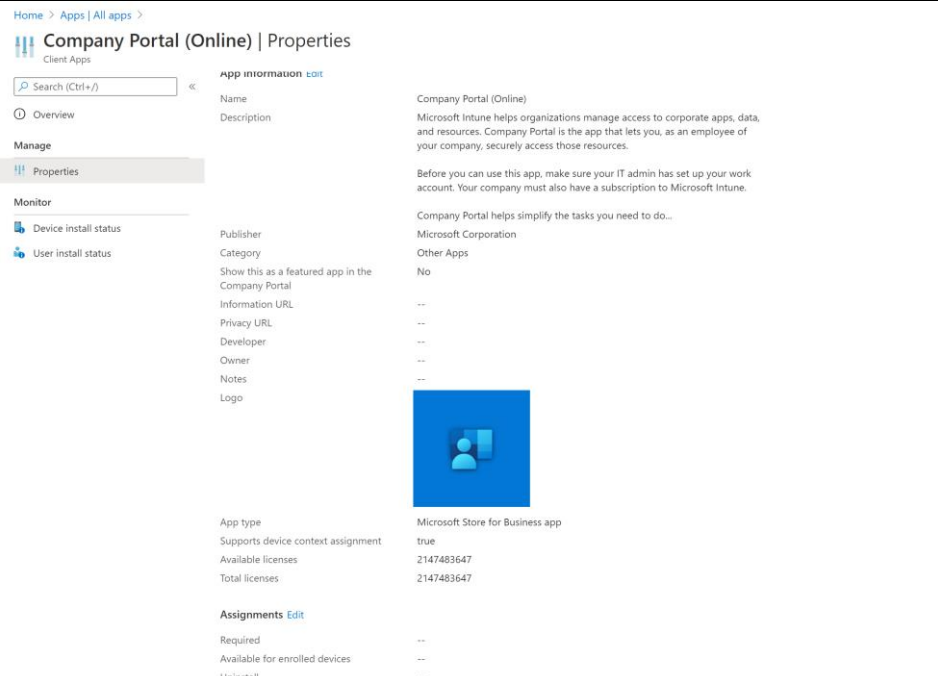
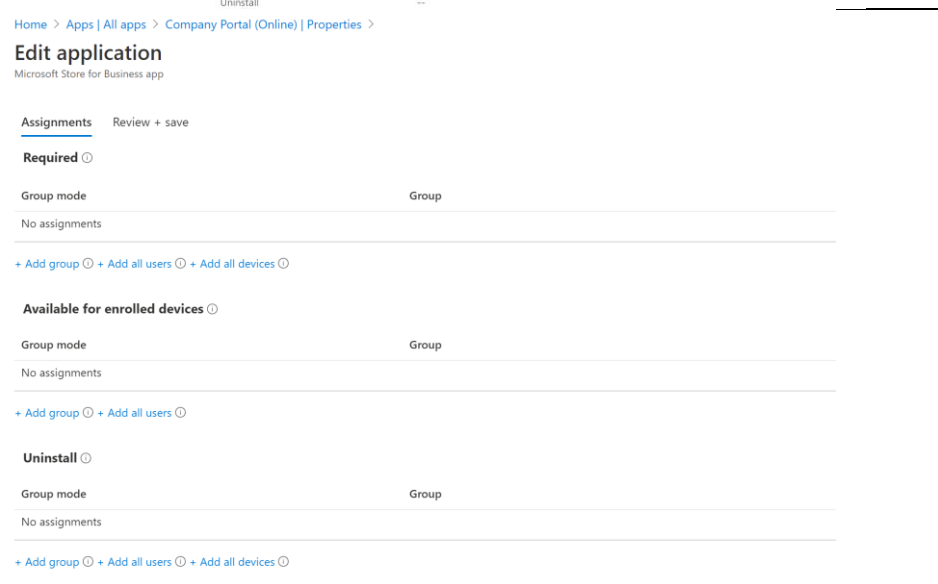
Exercise 15: Company portal

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

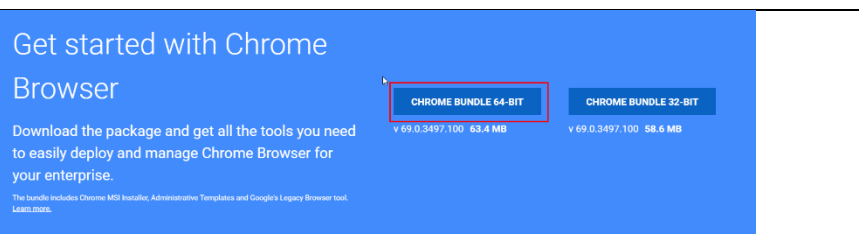
<p>Go to Endpoint manager -> Tenant administration -> Connectors and tokens → Microsoft store for Business</p> <p>1. Select open the business store</p>	
<p>2. Check if you are signed in. If not sign in with your account</p>	
<p>3. Use the search bar to search for company portal (bedrijfsportaal)</p>	
<p>4. Select Company Portal</p>	

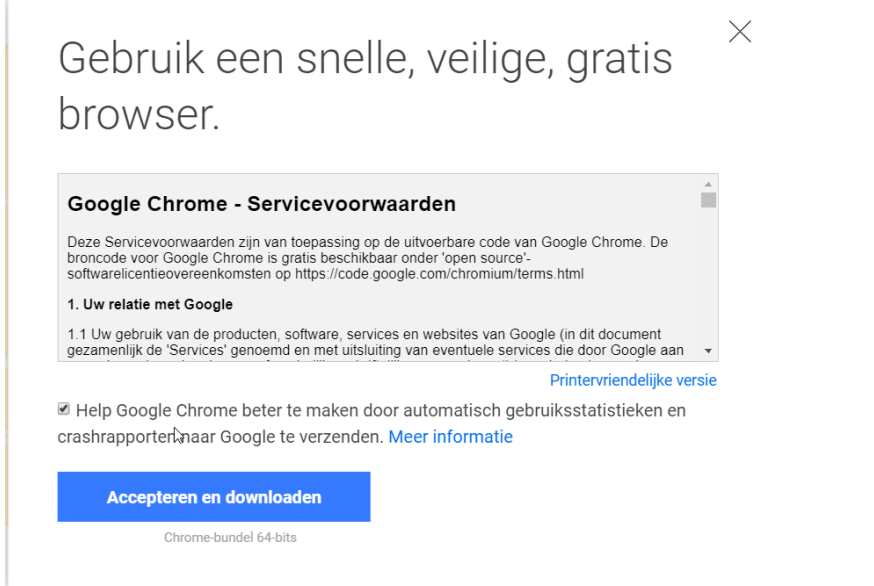
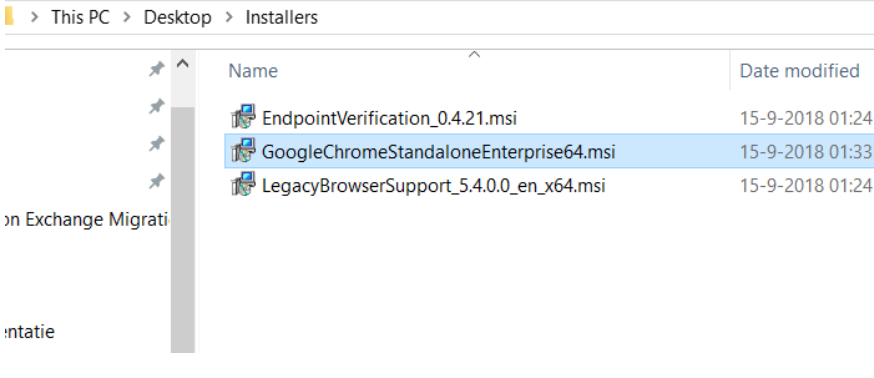
<p>5. Select Get the app</p>	
<p>6. Accept the agreement</p>	<p>Review and accept the services agreement to sign up for the Microsoft Store for Bu</p> 

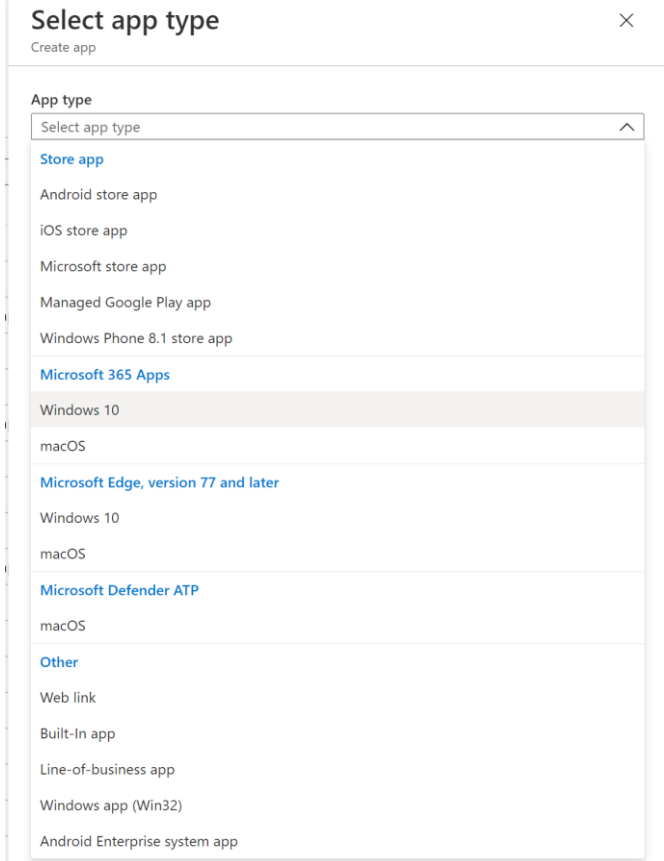
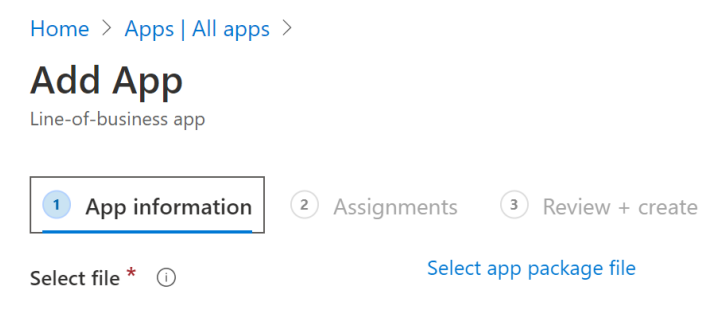
<p>7. After that the app is added</p>	<div data-bbox="612 367 890 405"><p>Thanks for your order</p></div> <div data-bbox="668 488 742 562"></div> <div data-bbox="754 495 1150 555"><p>Company Portal has been purchased and added to your inventory.</p></div> <div data-bbox="911 712 938 741"></div> <div data-bbox="1038 981 1086 1010"><p>Close</p></div>
---------------------------------------	--

<p>After the sync is completed go to Microsoft Endpoint Manager → apps → All Apps</p> <p>There you should find The company portal. Note that the Type is Microsoft Store for Business app</p> <ol style="list-style-type: none"> 1. Select Company Portal and click on Properties 	
<ol style="list-style-type: none"> 2. Select Edit Assignemnts 3. On Assignment Type choose required 4. Then select group and select the MDM group that you have created. 5. Select Review + Save 	

Exercise 16: MSI app deployment

<p>Go to https://enterprise.google.com/chrome/e/chrome-browser/</p> <ol style="list-style-type: none"> 1. Search the page for Chrome Bundle 64-bit 	
--	--

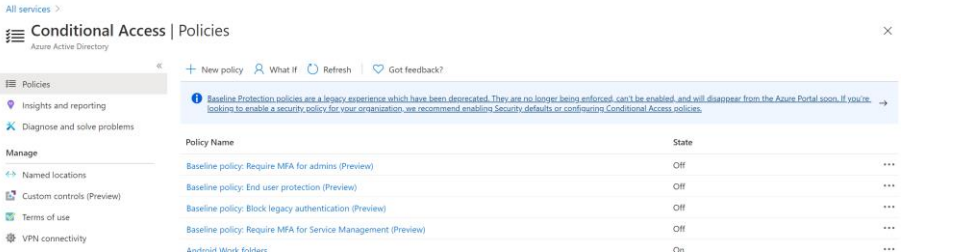
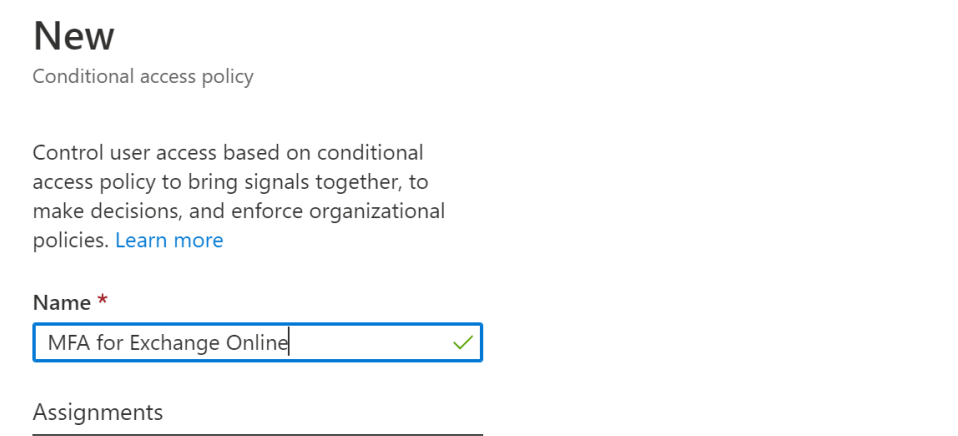
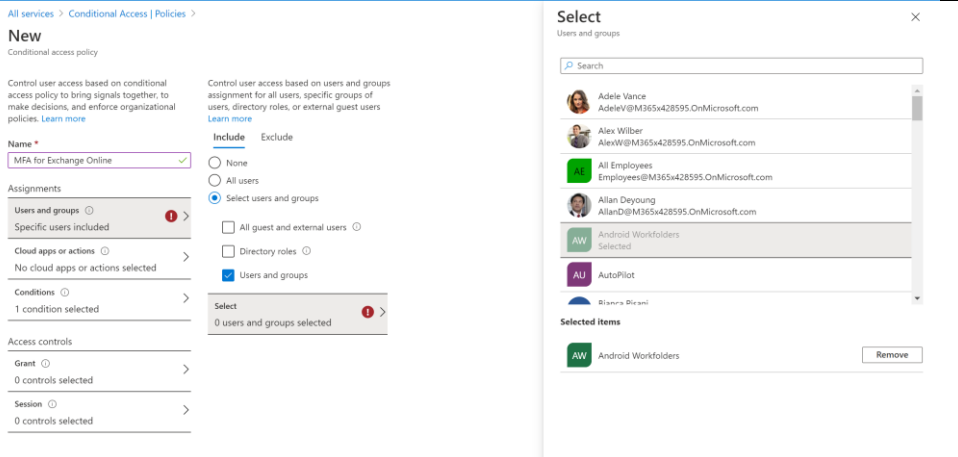
<p>2. Accept and download the MSI</p>	
<p>3. This will download a zip file</p> <p>4. Extract the files to your desktop</p> <p>5. There you can find the GoogleChromeStandAloneEnterprise64.msi</p> <p>Desktop\Installers\GoogleChromeStandAloneEnterprise64.msi</p>	

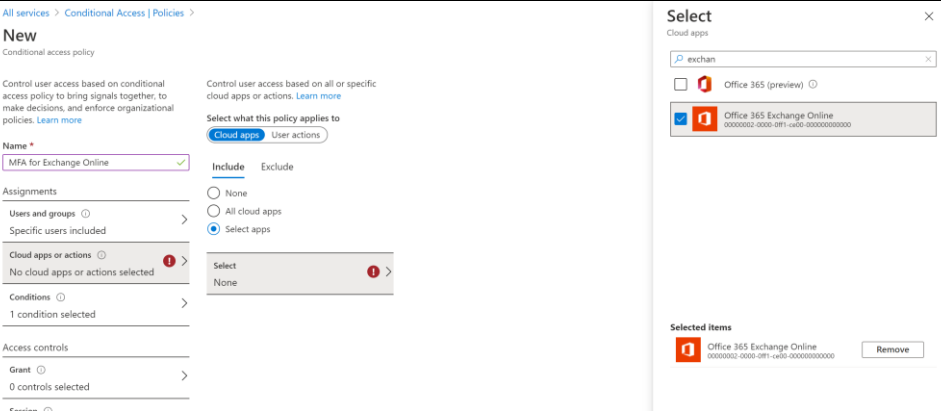
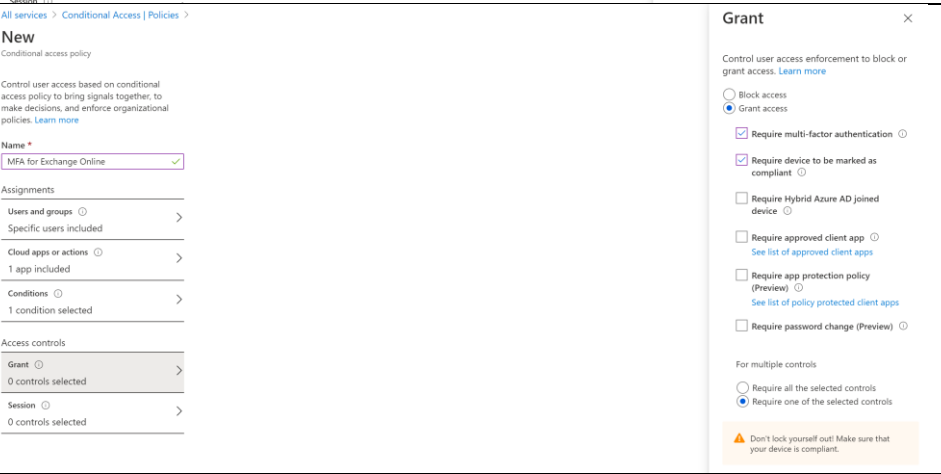
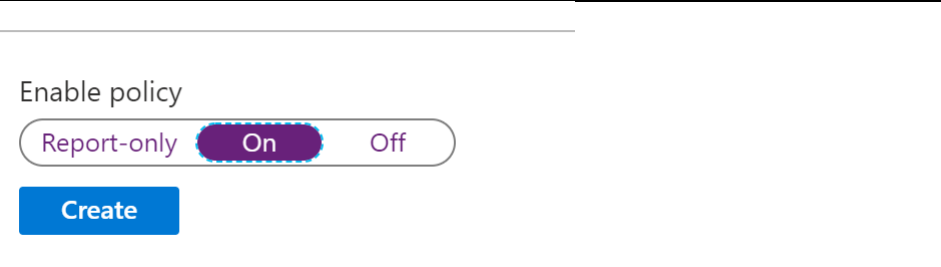
<p>Go to Endpoint Manager -> Apps -> All Apps -> Add</p> <p>1. For App type choose Line-of-business app</p>	 <p>Select app type ×</p> <p>Create app</p> <p>App type</p> <p>Select app type ^</p> <p>Store app</p> <p>Android store app</p> <p>iOS store app</p> <p>Microsoft store app</p> <p>Managed Google Play app</p> <p>Windows Phone 8.1 store app</p> <p>Microsoft 365 Apps</p> <p>Windows 10</p> <p>macOS</p> <p>Microsoft Edge, version 77 and later</p> <p>Windows 10</p> <p>macOS</p> <p>Microsoft Defender ATP</p> <p>macOS</p> <p>Other</p> <p>Web link</p> <p>Built-in app</p> <p>Line-of-business app</p> <p>Windows app (Win32)</p> <p>Android Enterprise system app</p>
<p>2. At App package file select GoogleChromeStandaloneEnterprise64.msi from your desktop and click OK</p>	 <p>Home > Apps All apps ></p> <h2>Add App</h2> <p>Line-of-business app</p> <p>1 App information 2 Assignments 3 Review + create</p> <p>Select file * ⓘ Select app package file</p>

<ol style="list-style-type: none"> 3. Select App information 4. Enter a Description 5. Enter a Publisher 6. Select OK 7. Select next 	<div> 1 App information 2 Assignments 3 Review + create </div> <div> <p>Select file * ⓘ GoogleChromeStandaloneEnterprise64.msi</p> <p>Name * ⓘ <input type="text" value="Google Chrome"/></p> <p>Description * ⓘ <input type="text" value="Google Chrome"/></p> <p>Publisher * ⓘ <input type="text" value="Enter a publisher name"/></p> <p>App install context ⓘ User Device</p> <p>Ignore app version ⓘ Yes No</p> <p>Command-line arguments <input type="text"/></p> <p>Category ⓘ 0 selected ▼</p> <p>Show this as a featured app in the Company Portal ⓘ Yes No</p> <p>Information URL ⓘ <input type="text" value="Enter a valid url"/></p> <p>Privacy URL ⓘ <input type="text" value="Enter a valid url"/></p> <p>Developer ⓘ <input type="text"/></p> <p>Owner ⓘ <input type="text"/></p> <p>Notes ⓘ <input type="text"/></p> </div>																		
<ol style="list-style-type: none"> 8. Assign the application to the MDM user group 	<div> ✓ App information 2 Assignments 3 Review + create </div> <div> <p>Required ⓘ</p> <table border="1"> <thead> <tr> <th>Group mode</th> <th>Group</th> <th>Install Context</th> </tr> </thead> <tbody> <tr> <td>No assignments</td> <td></td> <td></td> </tr> </tbody> </table> <p>+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ</p> <p>Available for enrolled devices ⓘ</p> <table border="1"> <thead> <tr> <th>Group mode</th> <th>Group</th> <th>Install Context</th> </tr> </thead> <tbody> <tr> <td>No assignments</td> <td></td> <td></td> </tr> </tbody> </table> <p>+ Add group ⓘ + Add all users ⓘ</p> <p>Uninstall ⓘ</p> <table border="1"> <thead> <tr> <th>Group mode</th> <th>Group</th> <th>Install Context</th> </tr> </thead> <tbody> <tr> <td>No assignments</td> <td></td> <td></td> </tr> </tbody> </table> <p>+ Add group ⓘ + Add all users ⓘ + Add all devices ⓘ</p> </div>	Group mode	Group	Install Context	No assignments			Group mode	Group	Install Context	No assignments			Group mode	Group	Install Context	No assignments		
Group mode	Group	Install Context																	
No assignments																			
Group mode	Group	Install Context																	
No assignments																			
Group mode	Group	Install Context																	
No assignments																			

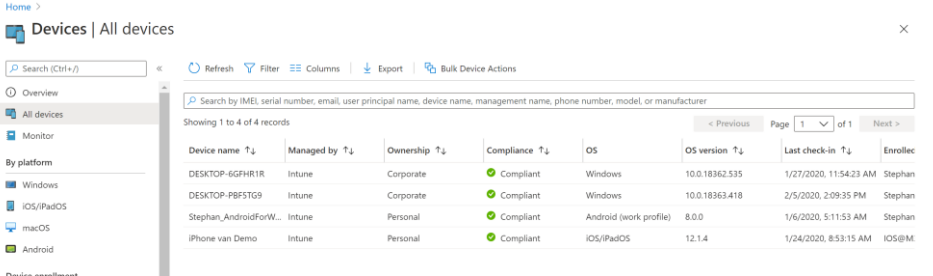
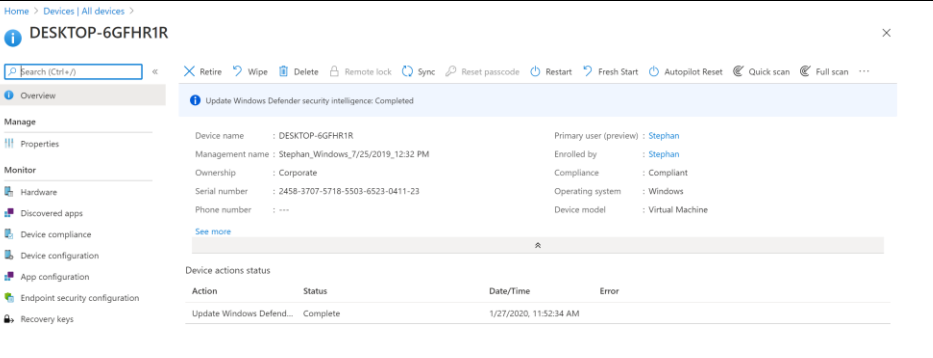
Exercise 17: Conditional Access

Conditional Access is a great way to secure your environment. You can use Intune to make sure that your device is 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 aad.portal.azure.com → select all services and select Azure AD Conditional Access 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>8. Select Cloud apps or actions</p> <p>9. Check Selects apps</p> <p>10. From the select menu find and check Office 365 Exchange Online</p>	
<p>11. Under Access controls select Grant</p> <p>12. Here you select Grant access and you Require multi-factor authentication and Require device to be marked as compliant</p> <p>13. Select Require one of the selected controls</p>	
<p>1. Enable the policy and click on Create</p>	

Activity 5: Selective Wipe

<p>Go to Endpoint Manager → 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>