2tCloud

Modern Workplace
Hands-on lab

AAD Premium, Intune, Office ProPlus

Microsoft 365 Enterprise

Lab Guide

Thursday, October 18, 2018

Version 2.0

Prepared by

Gino van Essen
Gido Veekens
Stephan van de Kruis

Technical Cloud Consultants – Copaco Nederland

Document Revision

Change Record

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

Name	Version Approved	Position	Date

Table of Contents

Introduction

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

Estimated time to complete this lab

150 minutes

Objectives

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

Prerequisites

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

Student Materials

All student materials are available for download here:

https://github.com/Copaco/handsonlab/tree/master/modernworkplace

Activity 1: Getting Started

Objectives

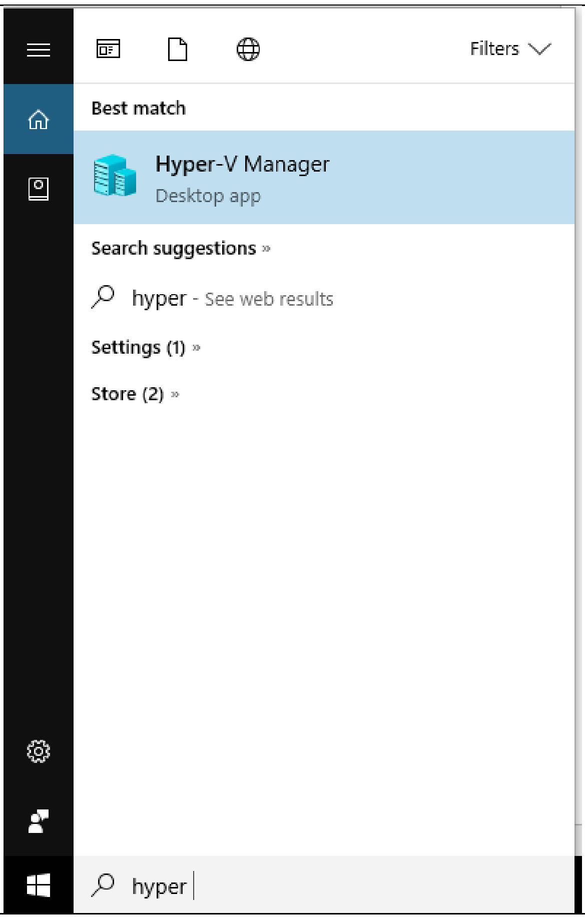
In this activity, you will configure the components necessary to perform this lab:

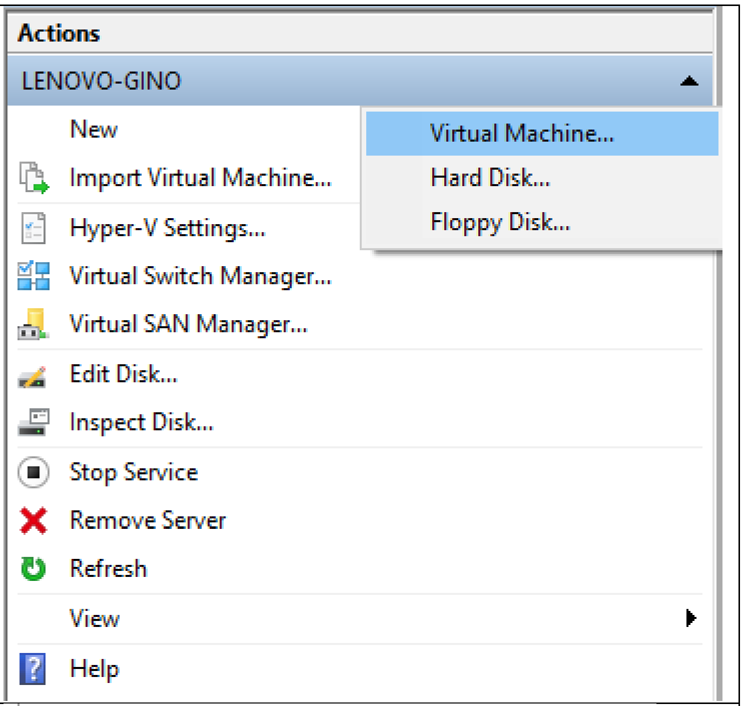
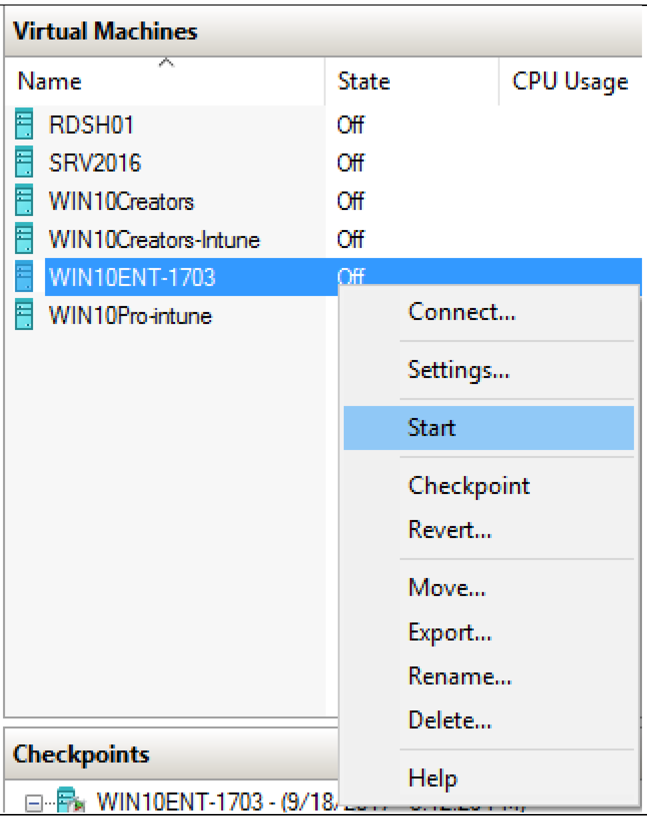
- Windows 10 Pro N, version 1803 - Azure VM

When Azure tenant \ subscription is not available

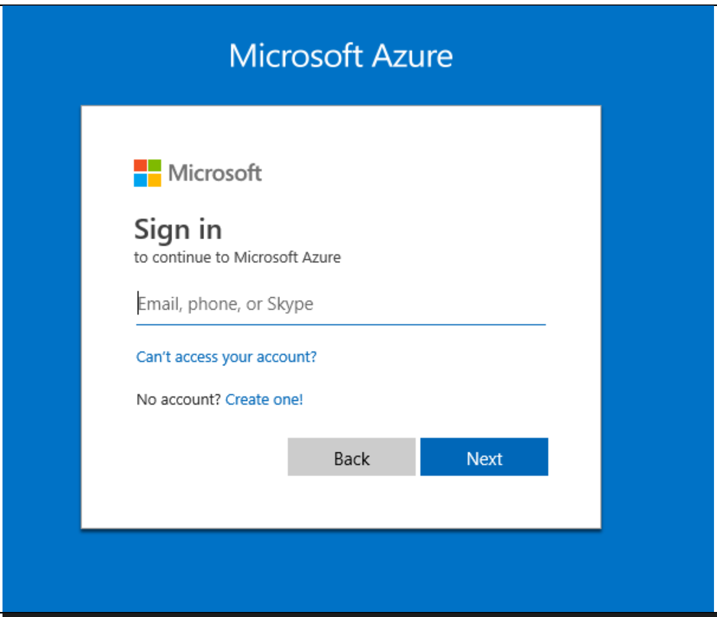
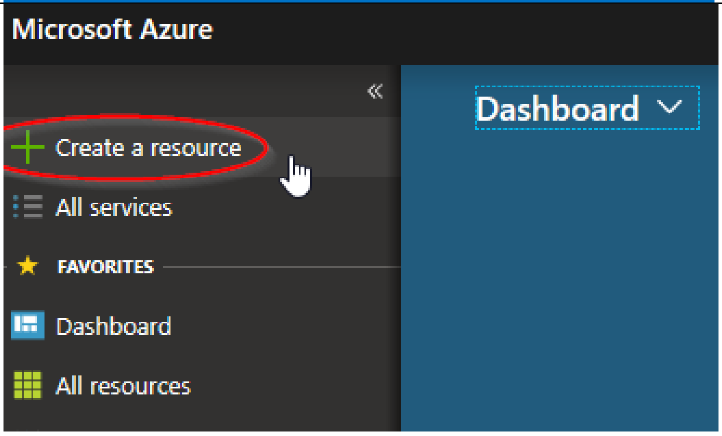
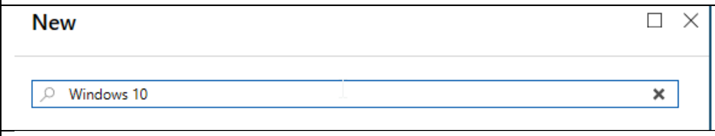
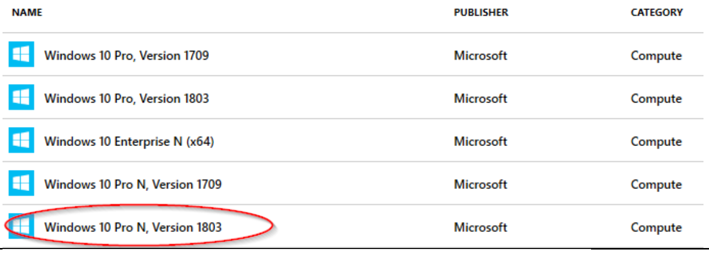
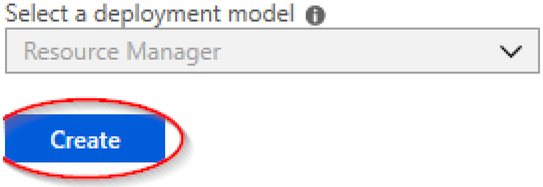
- ISO of Windows 10 Enterprise 1803 handed out by Copaco
- Hyper V Manager VM configuration

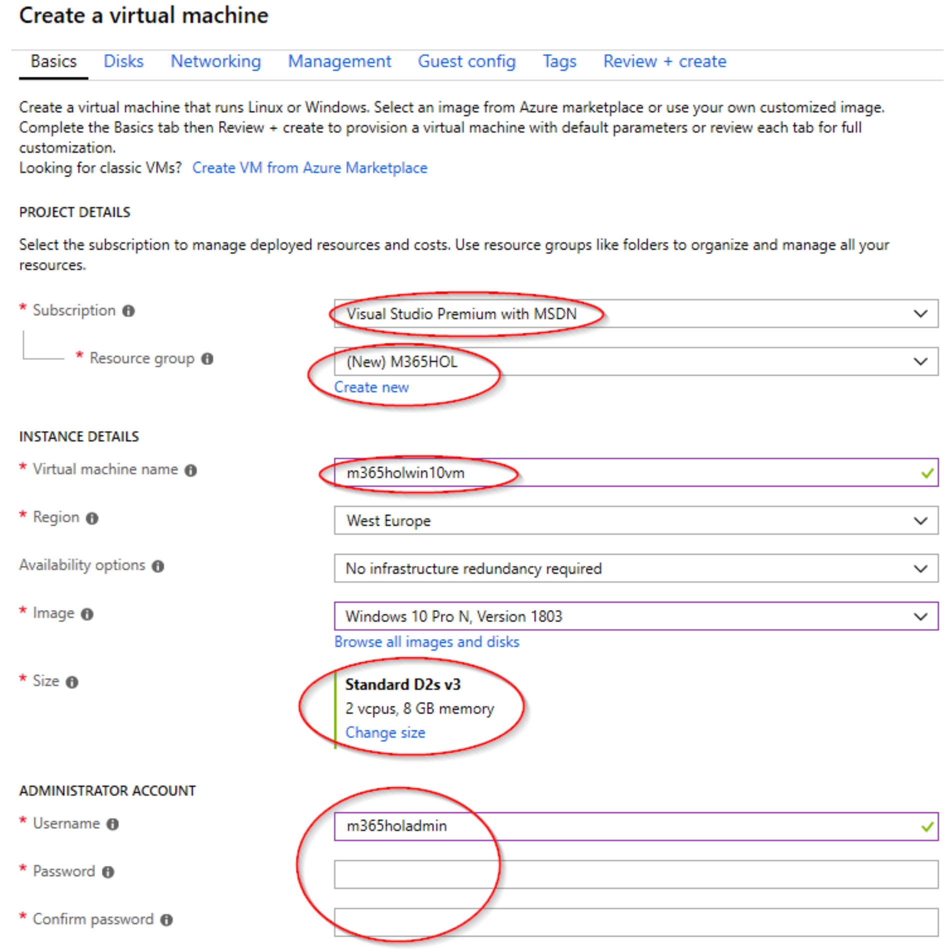
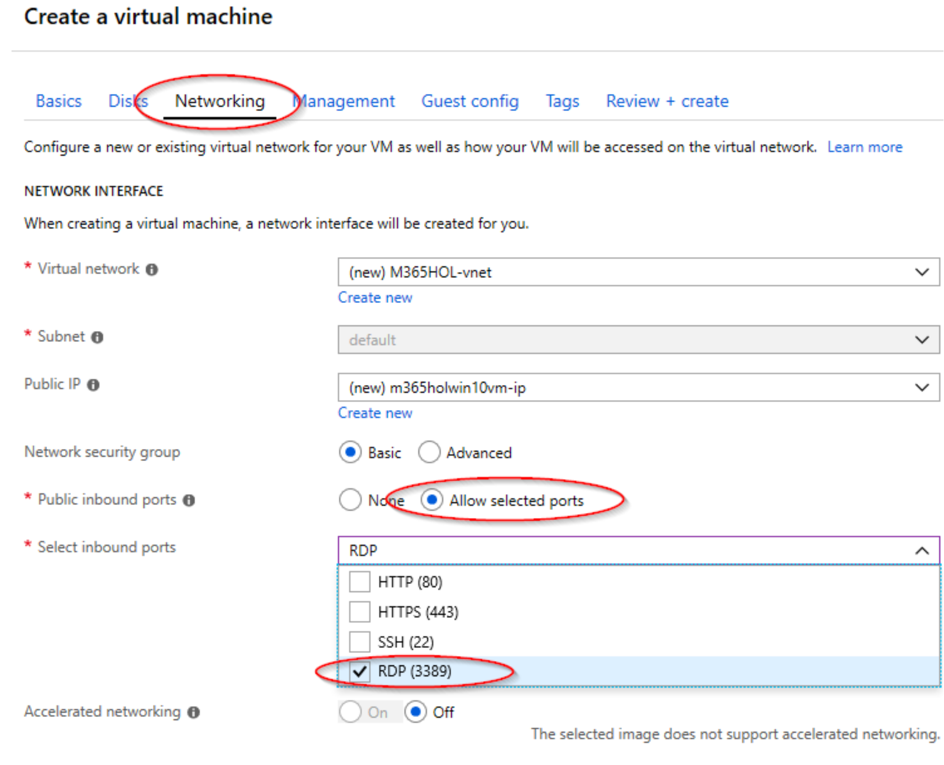
Exercise 1a: Create Windows 10 Enterprise VM

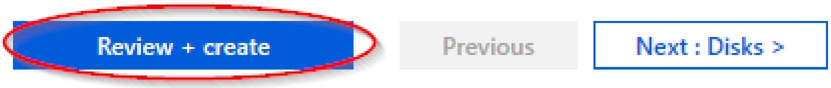
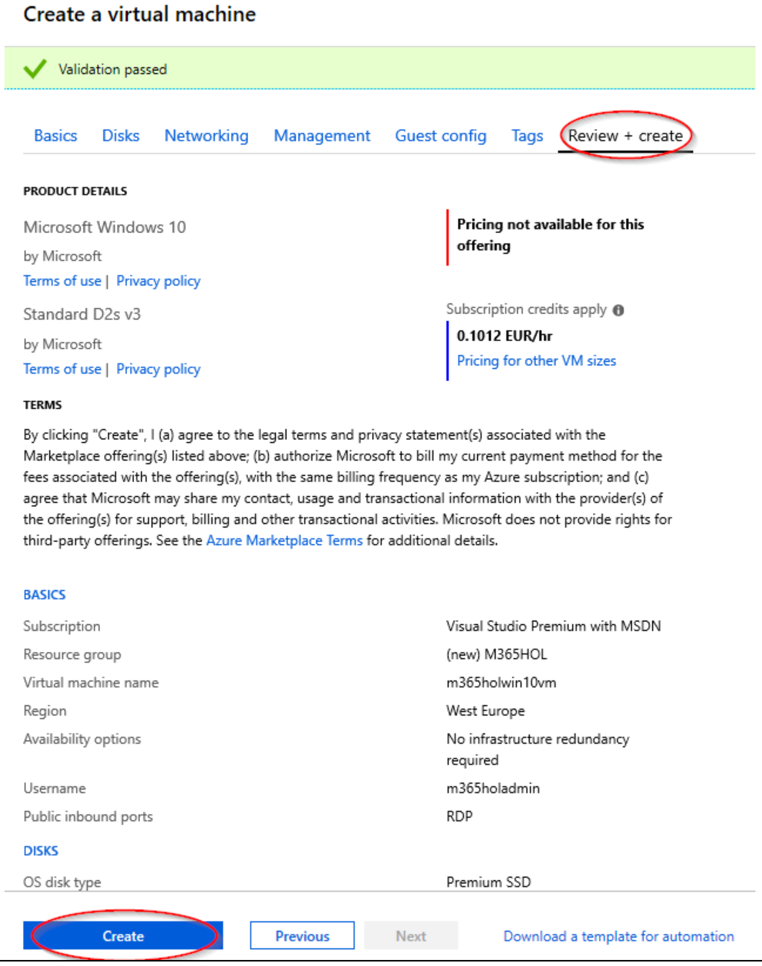
1. Open **Hyper-v Manager**	 Filters Best match Hyper-V Manager Desktop app Search suggestions » hyper - See web results Settings (1) » Store (2) » hyper

<table>
<tr>
<td>2. Create <b>New &gt; virtual machine</b>
3. Name <b>WIN10ENT-1803</b>
4. Generation <b>Generation 2</b>
5. Assign Memory <b>4096 MB</b>
6. Configure Networking <b>Connection External</b>
7. Create VHD <b>Standard settings</b>
8. Installation Options <b>install an OS from a bootable CD/DVD</b>
9. Image file: “Win10.iso”
10. Finish / complete the configuration</td>
<td> </td>
</tr>
<tr>
<td>11. Start VM <b>WIN10ENT-1803</b></td>
<td> </td>
</tr>
<tr>
<td>12. Start Windows installation with <b>default</b> settings (<b>Custom installation)</b></td>
<td></td>
</tr>
</table>

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

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

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

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

Create a virtual machine

✓ Validation passed

Basics Disks Networking Management Guest config Tags Review + create

PRODUCT DETAILS

Microsoft Windows 10 by Microsoft Terms of use | Privacy policy	Pricing not available for this offering
Standard D2s v3 by Microsoft Terms of use | Privacy policy	Subscription credits apply 0.1012 EUR/hr Pricing for other VM sizes

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the Azure Marketplace Terms for additional details.

BASICS

Subscription	Visual Studio Premium with MSDN
Resource group	(new) M365HOL
Virtual machine name	m365holwin10vm
Region	West Europe
Availability options	No infrastructure redundancy required
Username	m365holadmin
Public inbound ports	RDP

DISKS

OS disk type	Premium SSD

Create Previous Next Download a template for automation

Activity 2: Prepare Modern workplace with Intune

The most important components in this exercise are:

Azure Active Directory.

Users and Groups.

Intune.

Exersize 2: Create an AAD Group

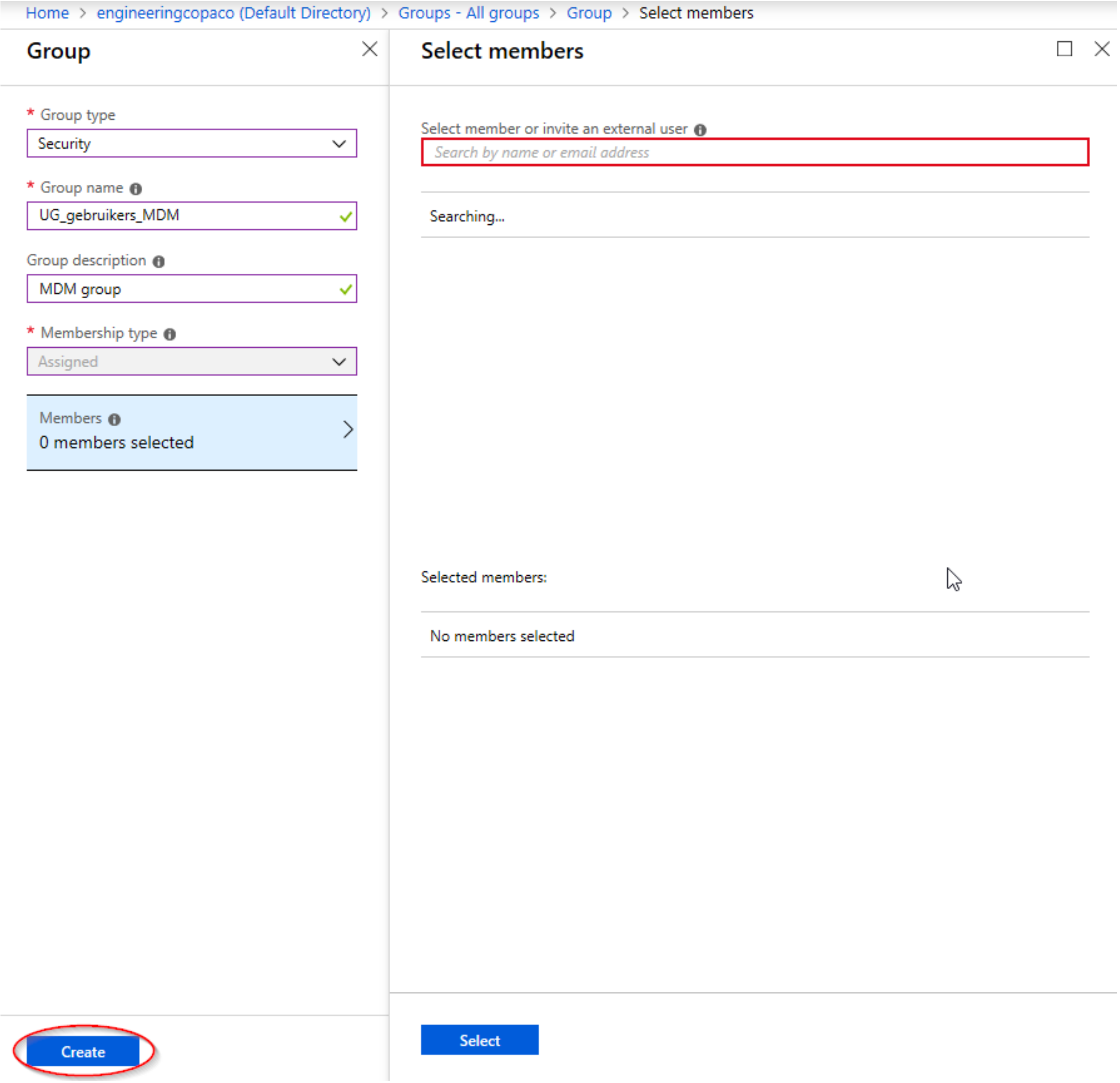
1. Go to : http://portal.azure.com
2. Go to: **Azure Active Directory->Manage->Groups**
3. Click **New Group** and create a group with the following settings

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

4. Add Admin account to group “**UG_Gebruikers_MDM”**
5. Click Create (bottom of screen)

Exercise 2a: Configure group-based Licensing

1. Go to: **Azure Active Directory → Licenses → All products**
2. Select **Enterprise Mobility + Security 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
8. Repeat this step for the Office 365 Enterprise E3 Licenses



Home > engineeringcopaco (Default Directory) > Groups - All groups > Group > Select members

Group

* Group type: Security

* Group name: UG_gebruikers_MDM

Group description: MDM group

* Membership type: Assigned

Members: 0 members selected

Select members

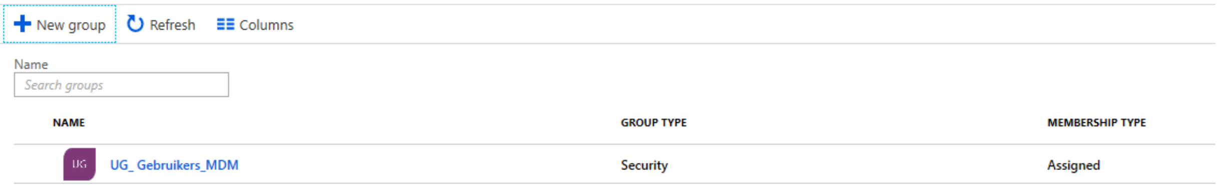
Select member or invite an external user

Searching...

Selected members:

No members selected

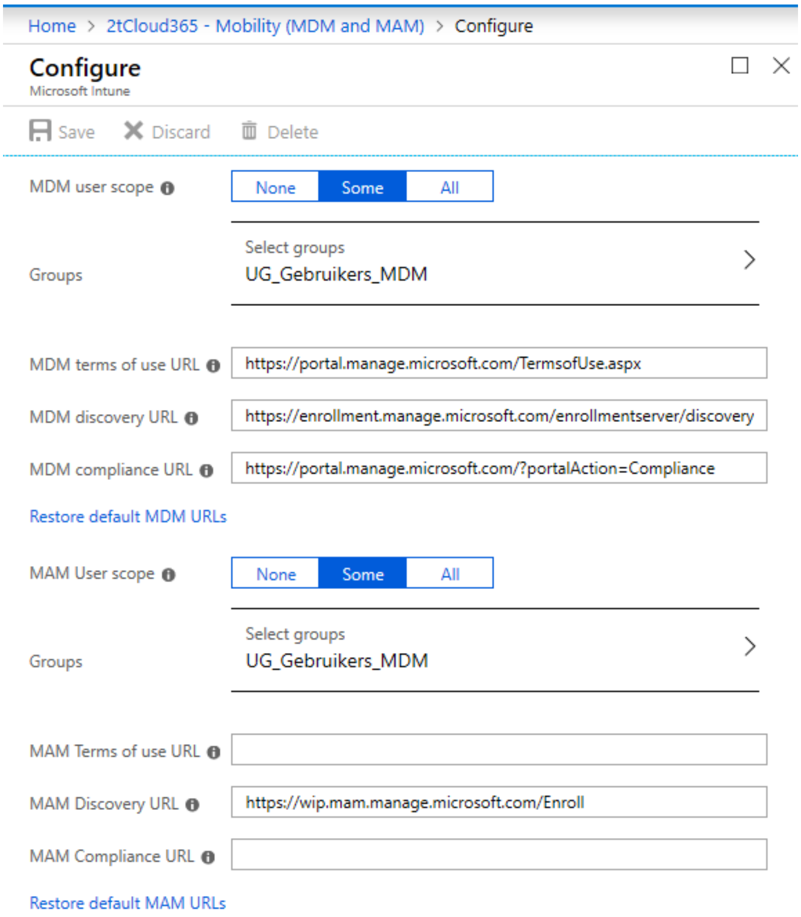
6. AAD Group “**UG_Gebruikers_MDM”** is created



NAME	GROUP TYPE	MEMBERSHIP TYPE
UG UG_ Gebruikers_MDM	Security	Assigned

Exercise 3: Configure MDM and MAM Intune settings

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



MDM user scope: Some

Groups: UG_Gebruikers_MDM

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

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

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

MAM User scope: Some

Groups: UG_Gebruikers_MDM

MAM Terms of use URL:

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

MAM Compliance URL:

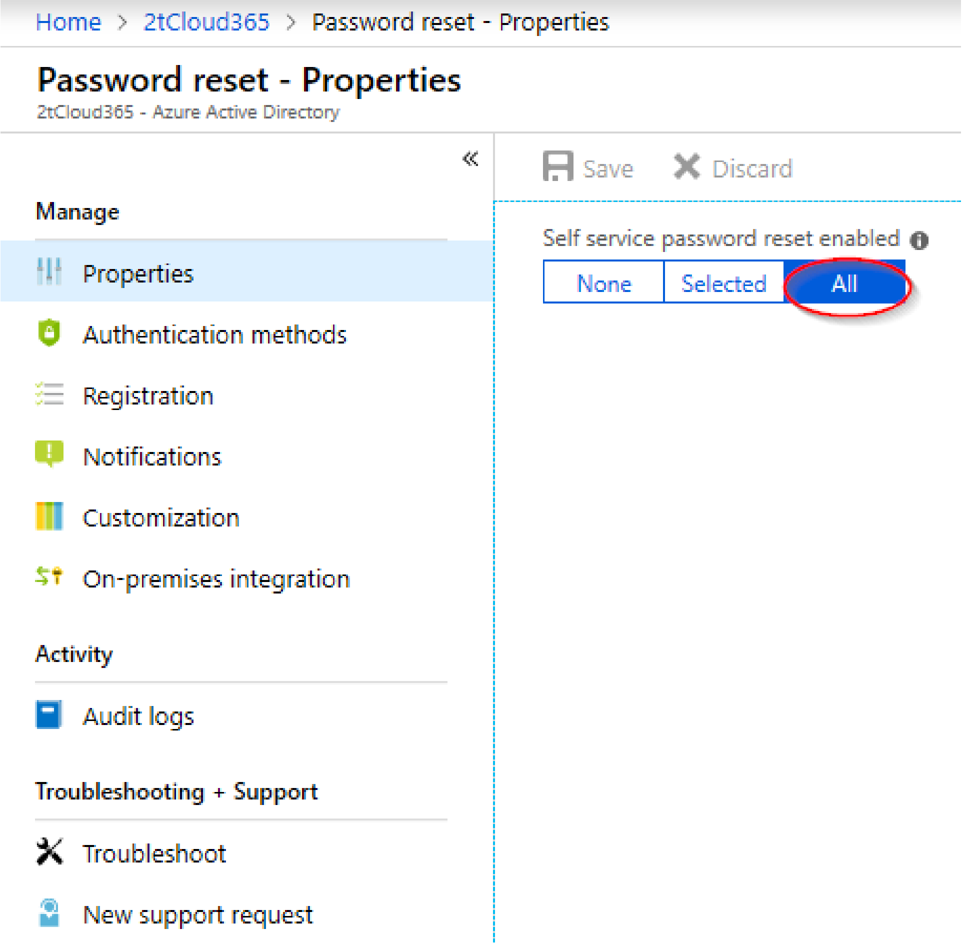
2. Configure the settings ->

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

3. Click on **Save**

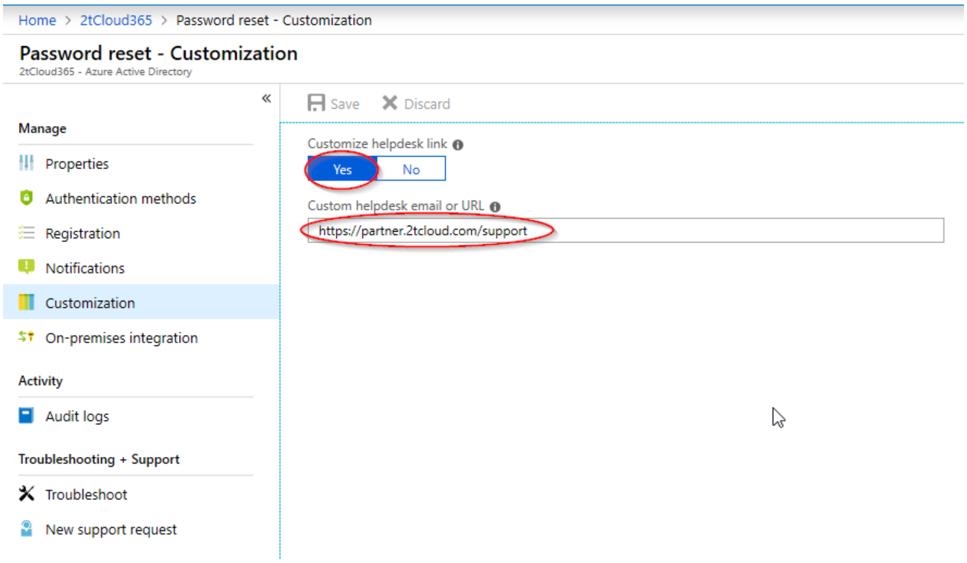
Exercise 4: Activate Self Service Password Reset

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



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

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



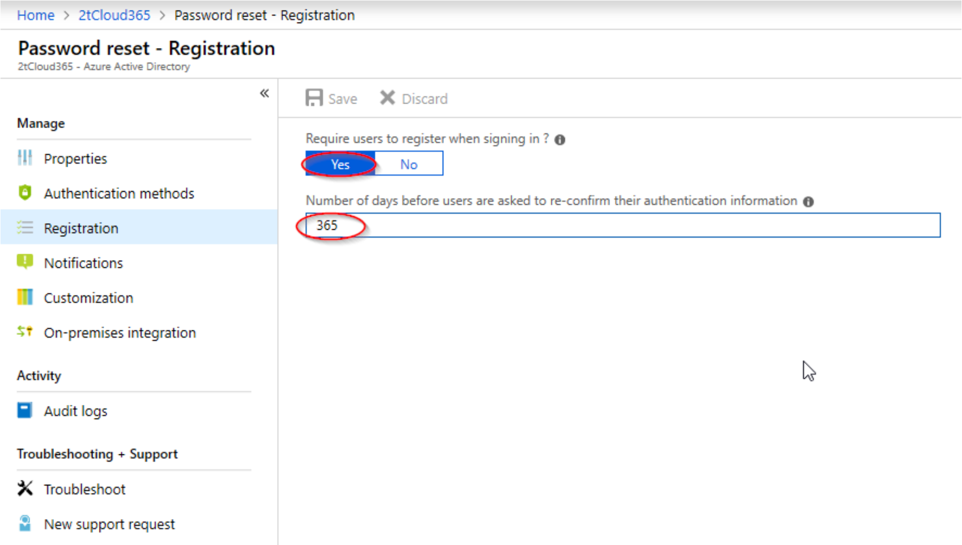
Customize helpdesk link: Yes No

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

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

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

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



Require users to register when signing in ? Yes No

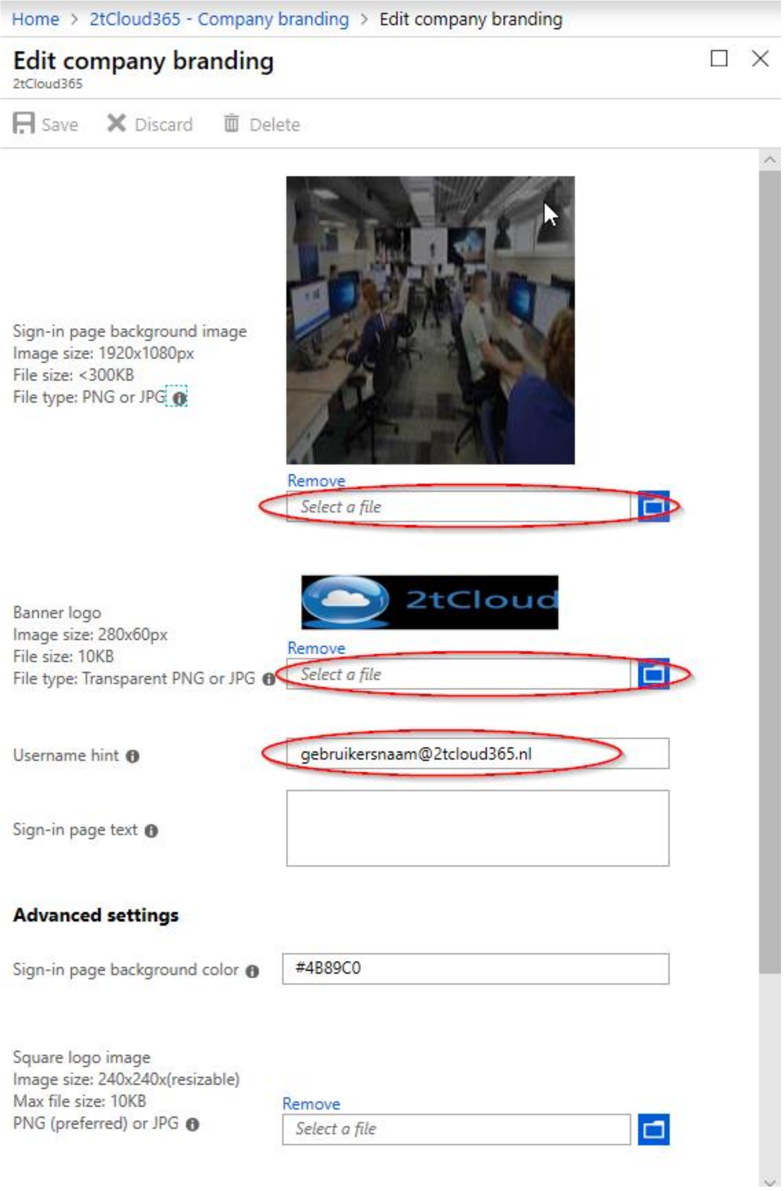
Number of days before users are asked to re-confirm their authentication information: 365

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

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

Exercise 5: Company branding

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



Home > 2tCloud365 - Company branding > Edit company branding

Edit company branding

2tCloud365

Save Discard Delete

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

Remove

Select a file

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

Remove

Select a file

Username hint: gebruikersnaam@2tcloud365.nl

Sign-in page text

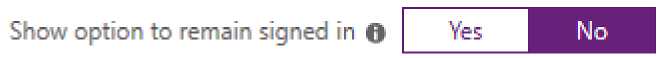
Advanced settings

Sign-in page background color: #4B89C0

Square logo image
Image size: 240x240x(resizable)
Max file size: 10KB
PNG (preferred) or JPG

Remove

Select a file

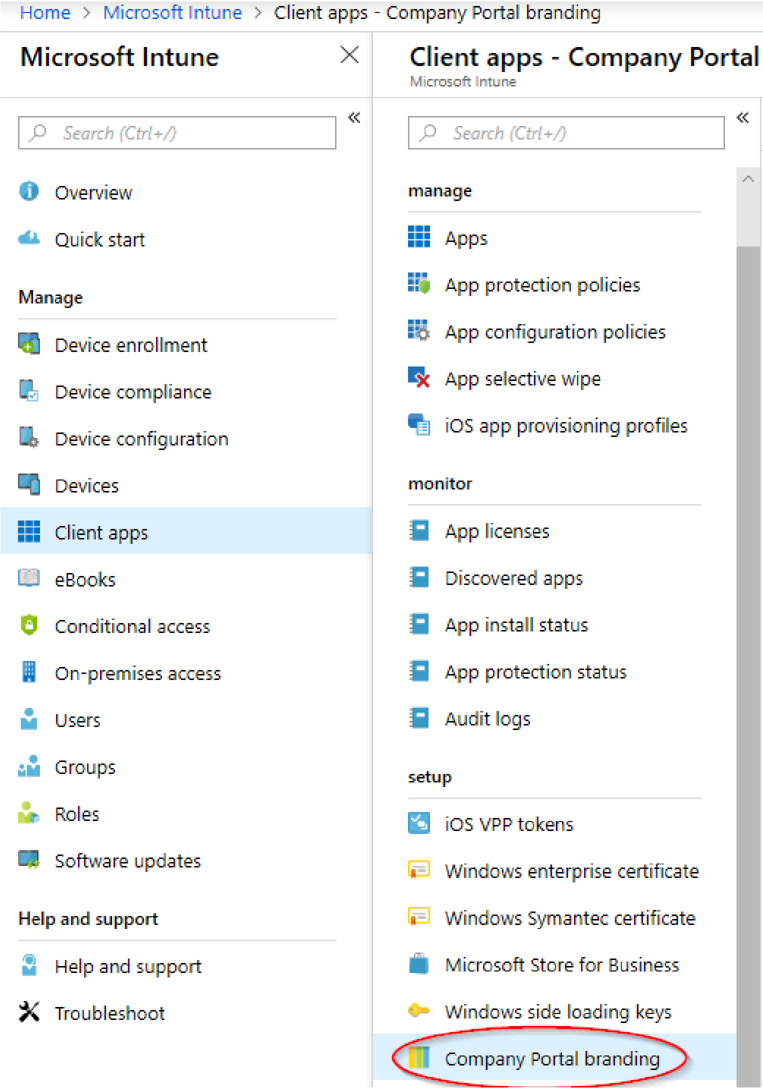


Show option to remain signed in: Yes [✓ No]

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

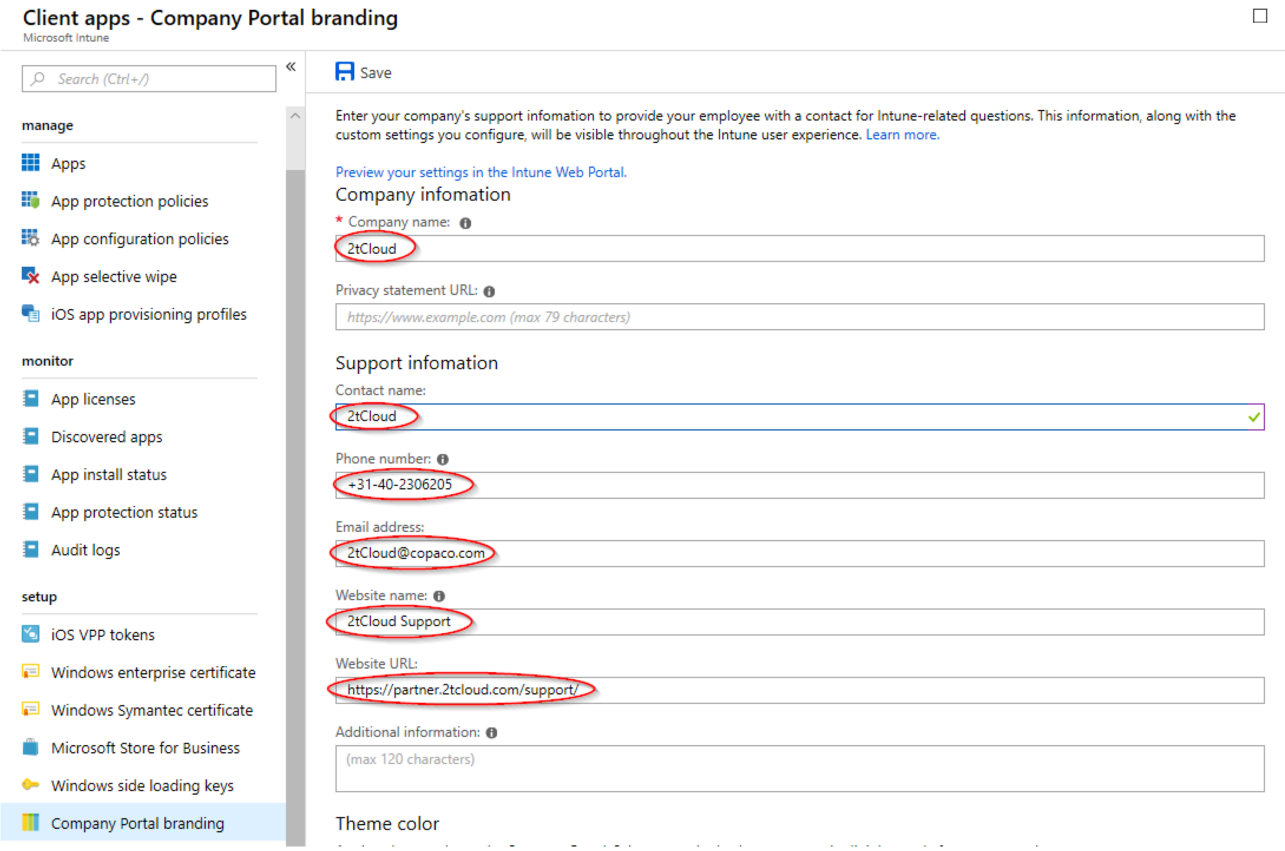
Sign-in page image	Add image
Banner image	Add image
User name hint	gebruikersnaam@2tcloud365.nl
Show option to remain signed in	No

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



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

Company Name	2tCloud or your own company
Contact name	2tCloud or your own company
Phone number	Add picture
E-mail adress	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



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

Preview your settings in the Intune Web Portal.

Company infomation

* Company name: 2tCloud

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

Support infomation

Contact name: 2tCloud

Phone number: +31-40-2306205

Email address: 2tCloud@copaco.com

Website name: 2tCloud Support

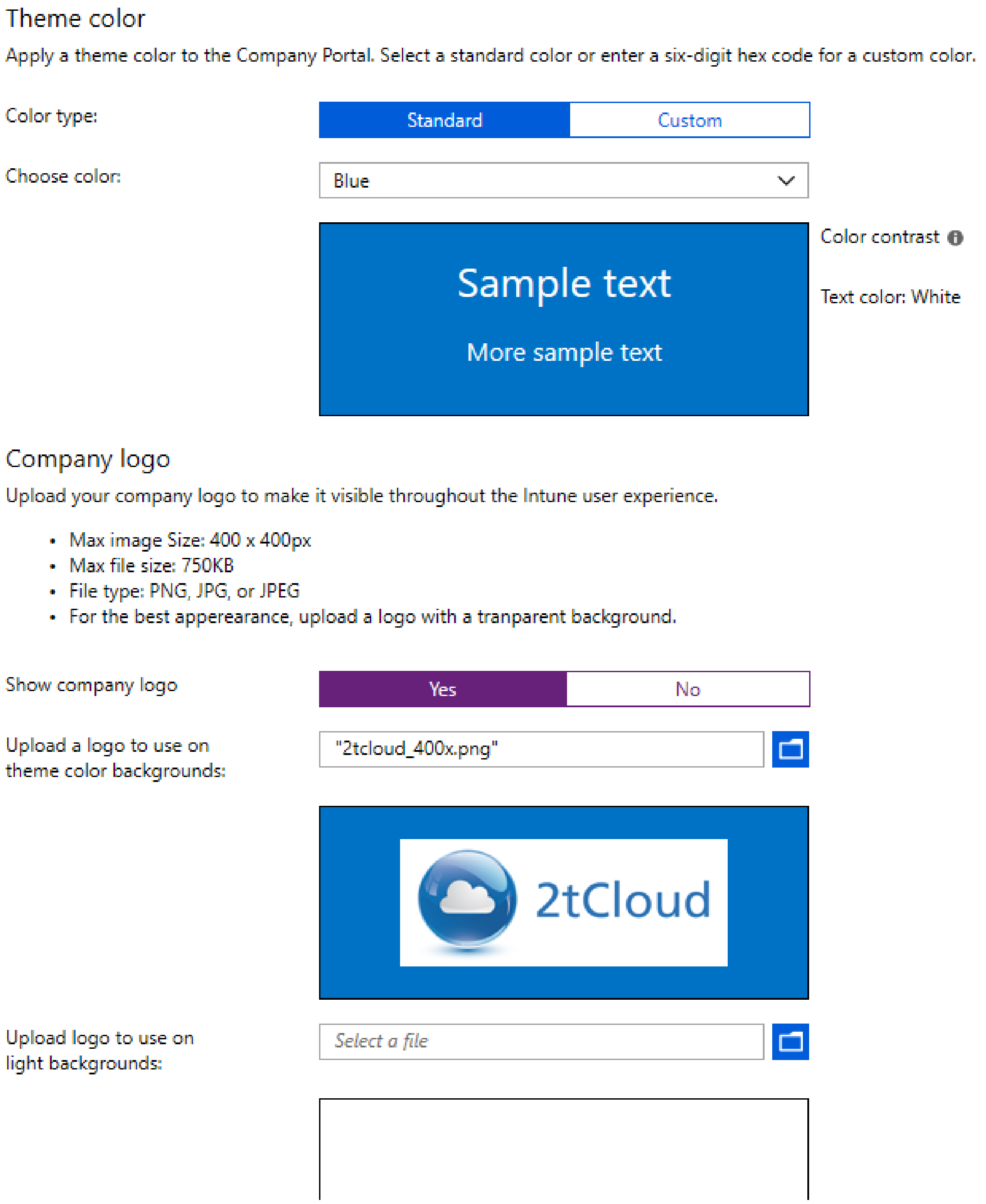
Website URL: https://partner.2tcloud.com/support/

Additional information: (max 120 characters)

Theme color

For more settings -> Next page

Show company logo	Yes
Company logo	Add logo



Theme color

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

Color type: Standard | Custom

Choose color: Blue

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 apperearance, upload a logo with a tranparent background.

Show company logo: Yes | No

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

Upload logo to use on light backgrounds: Select a file

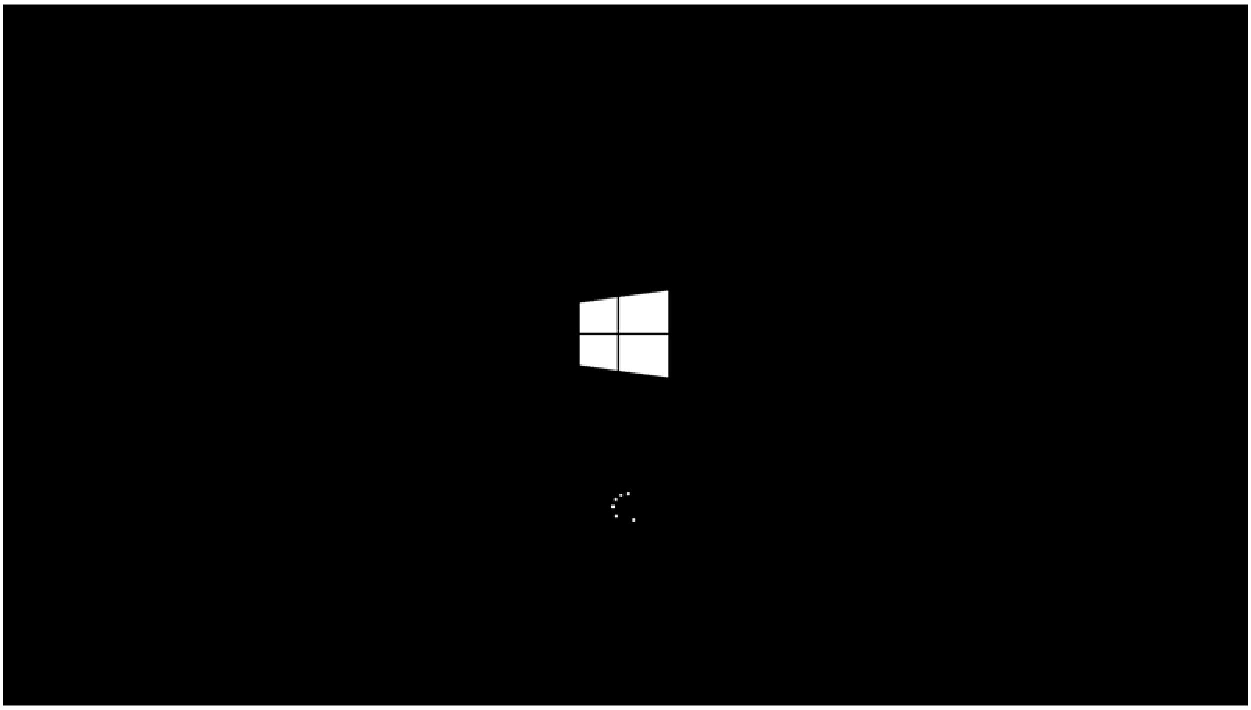
Activity 3: Add Windows to MDM

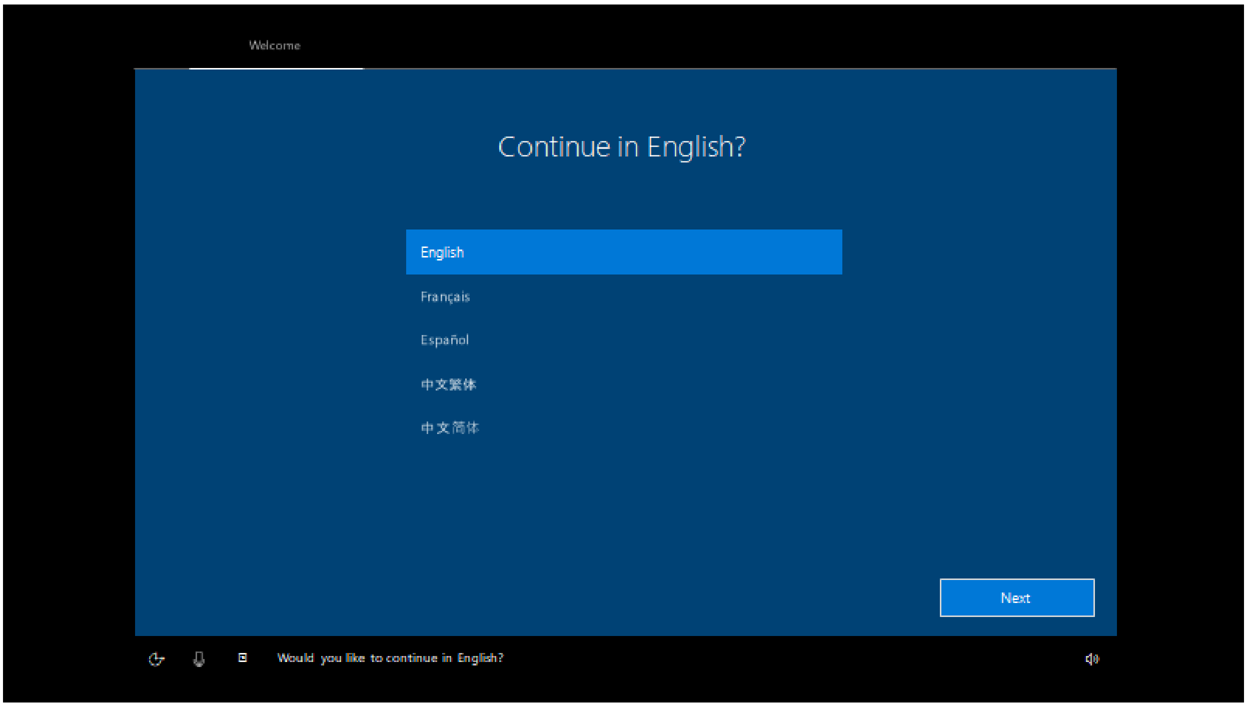
Exercise 6: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)

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

Exersize 6b – Hyper V Win10 VM

Start the setup of the Windows 10 Enterprise OS





Welcome

Continue in English?

English

Français

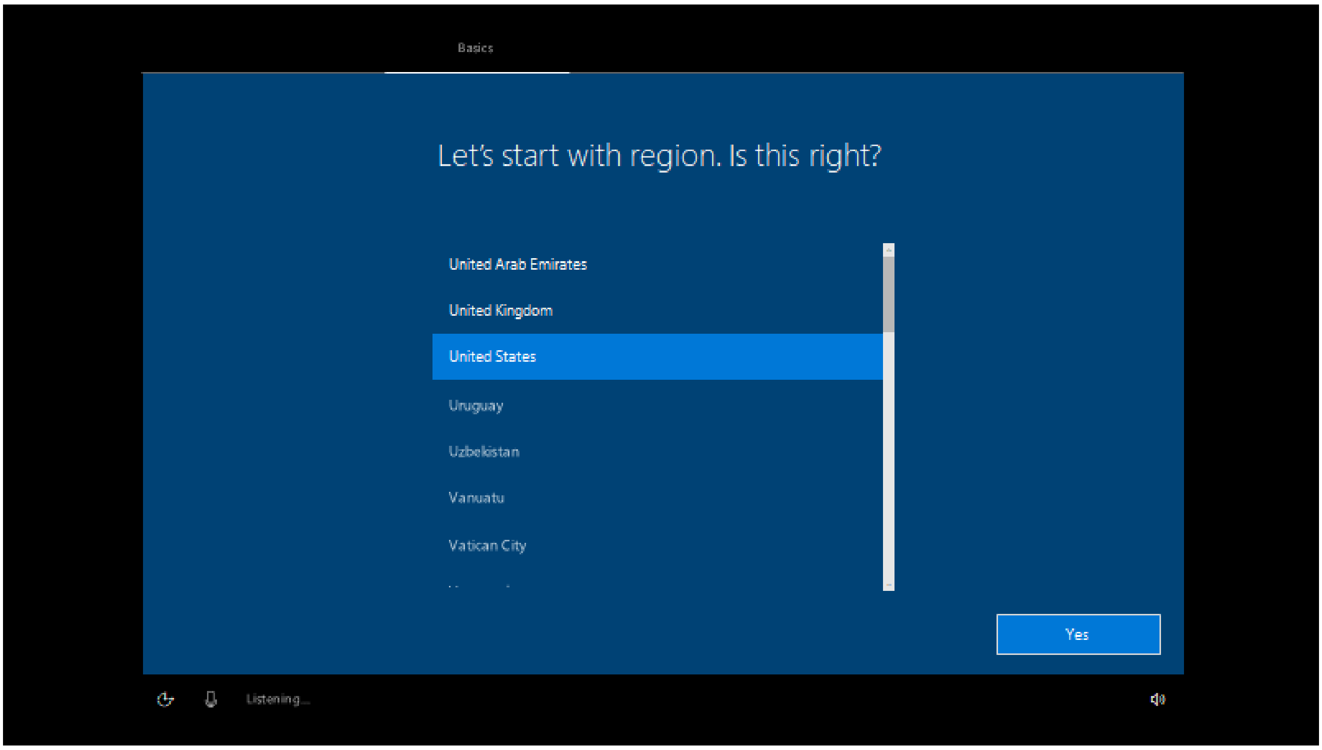
Español

中文繁体

中文简体

Next

Would you like to continue in English?



Basics

Let's start with region. Is this right?

United Arab Emirates

United Kingdom

United States

Uruguay

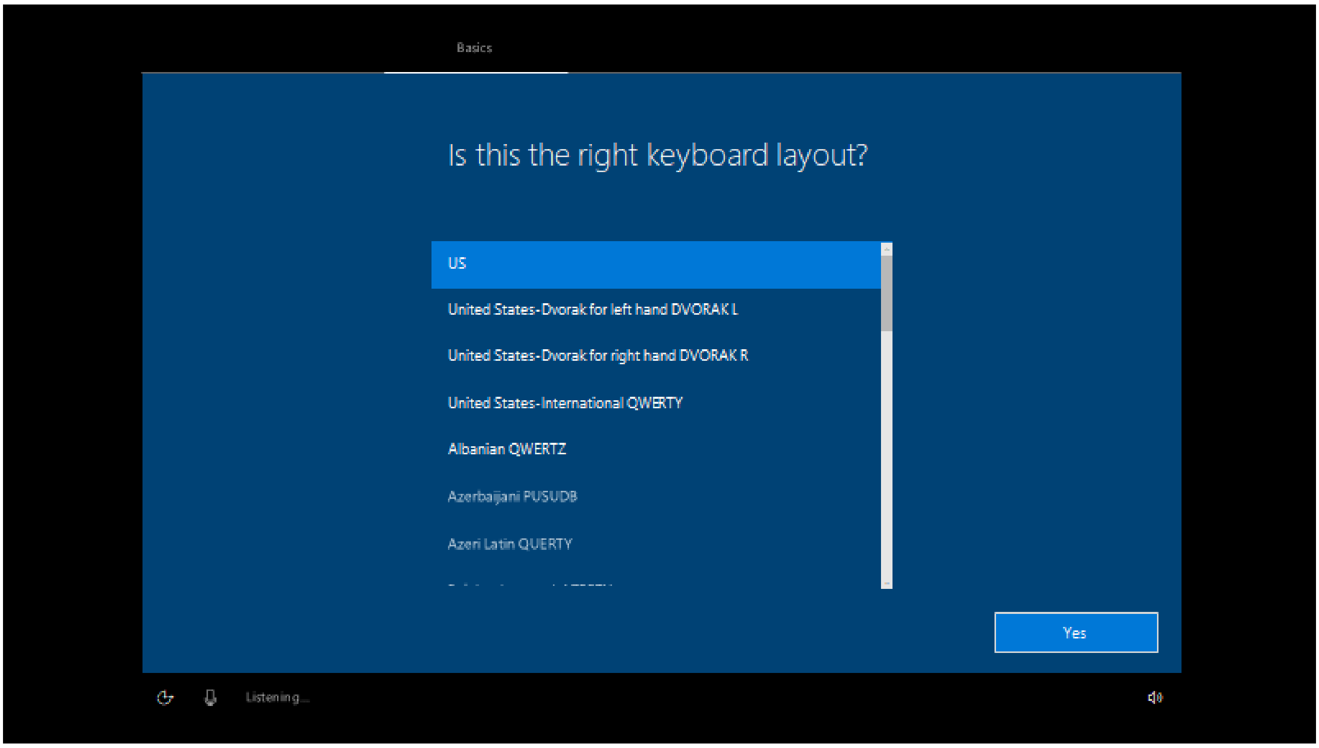
Uzbekistan

Vanuatu

Vatican City

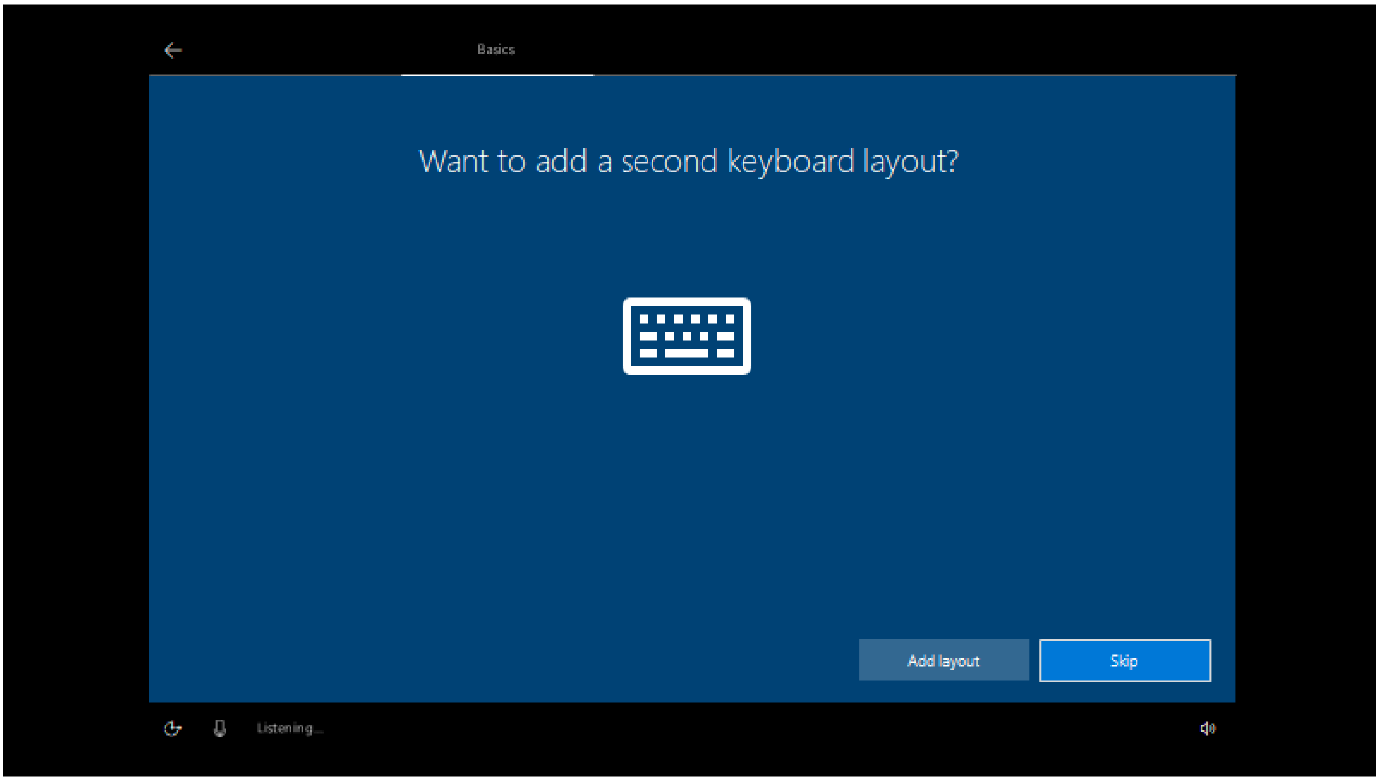
Yes

Listening...

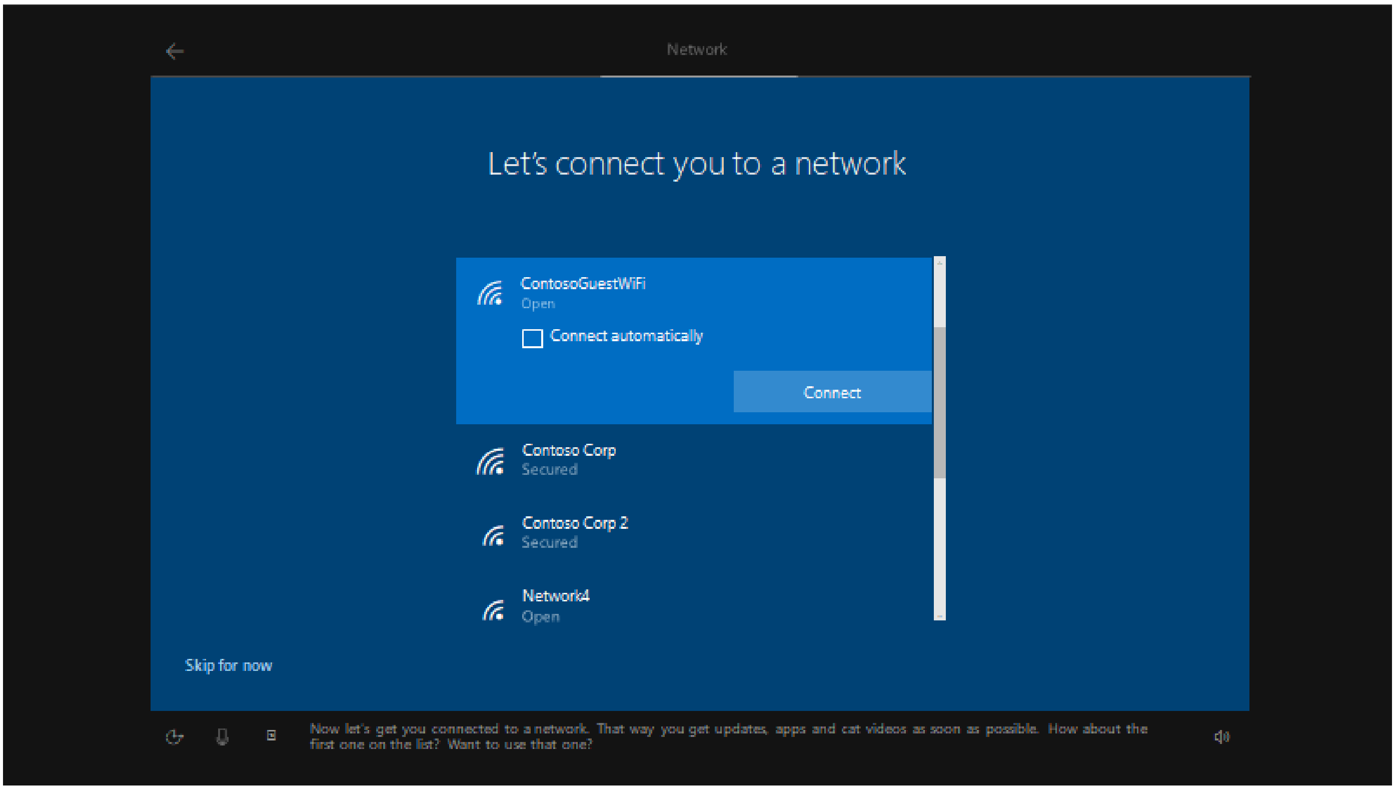


Is this the right keyboard layout?

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



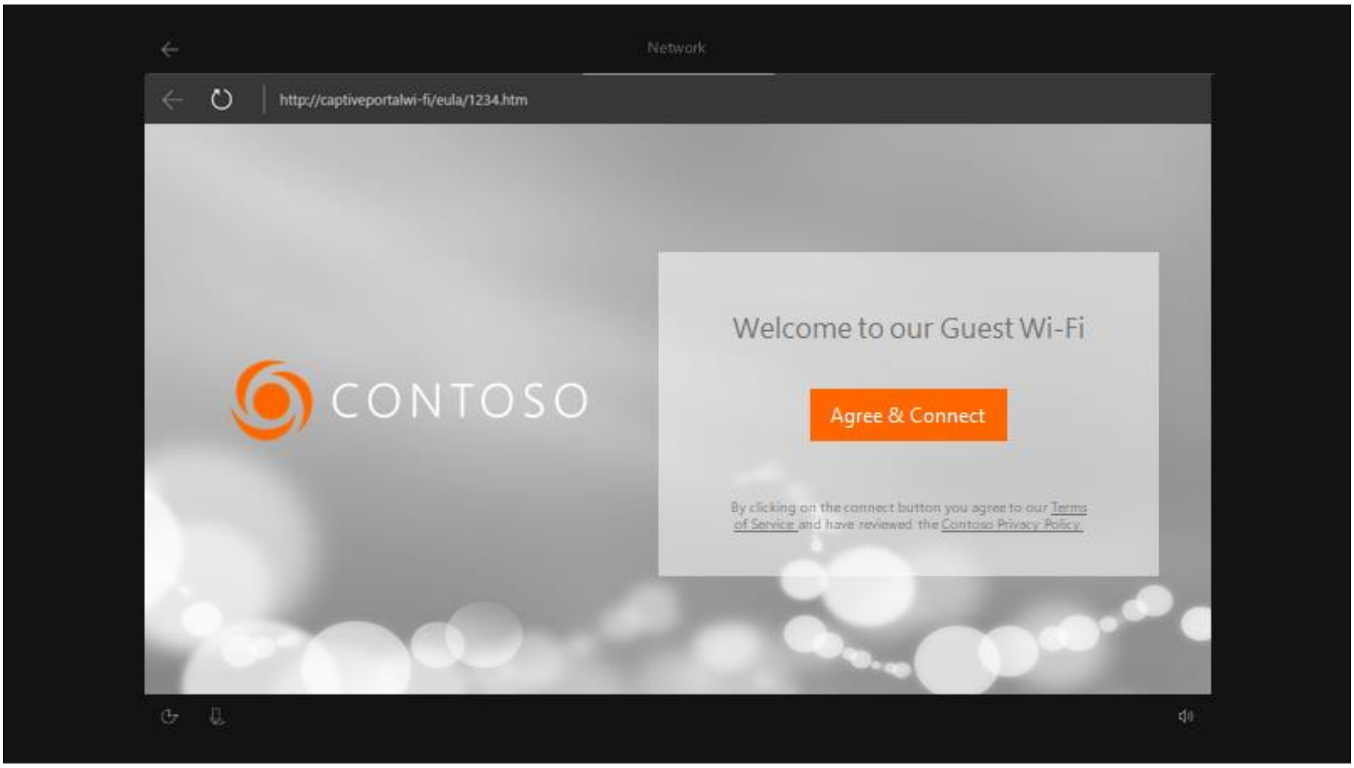
Want to add a second keyboard layout?



Let's connect you to a network

□ Connect automatically

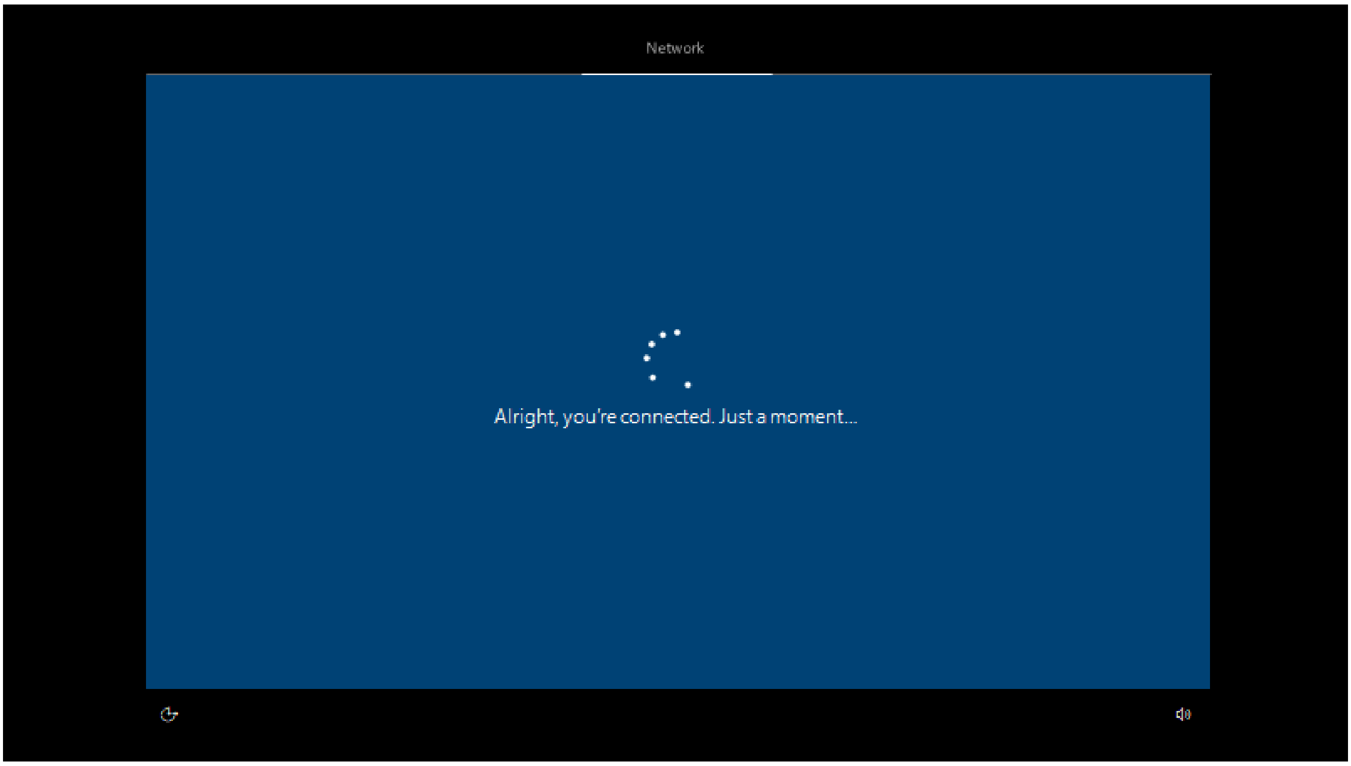
Now let's get you connected to a network. That way you get updates, apps and cat videos as soon as possible. How about the first one on the list? Want to use that one?



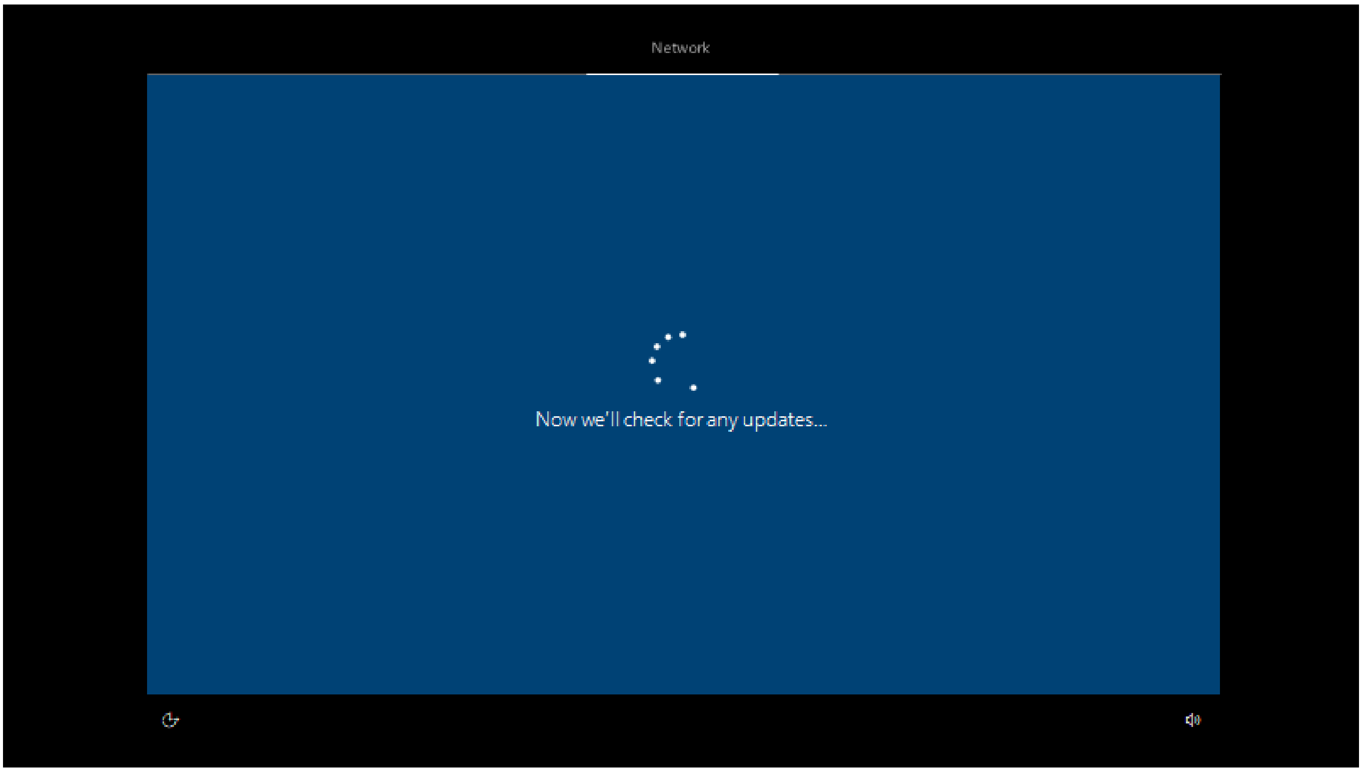
http://captiveportalwi-fi/eula/1234.htm

Welcome to our Guest Wi-Fi

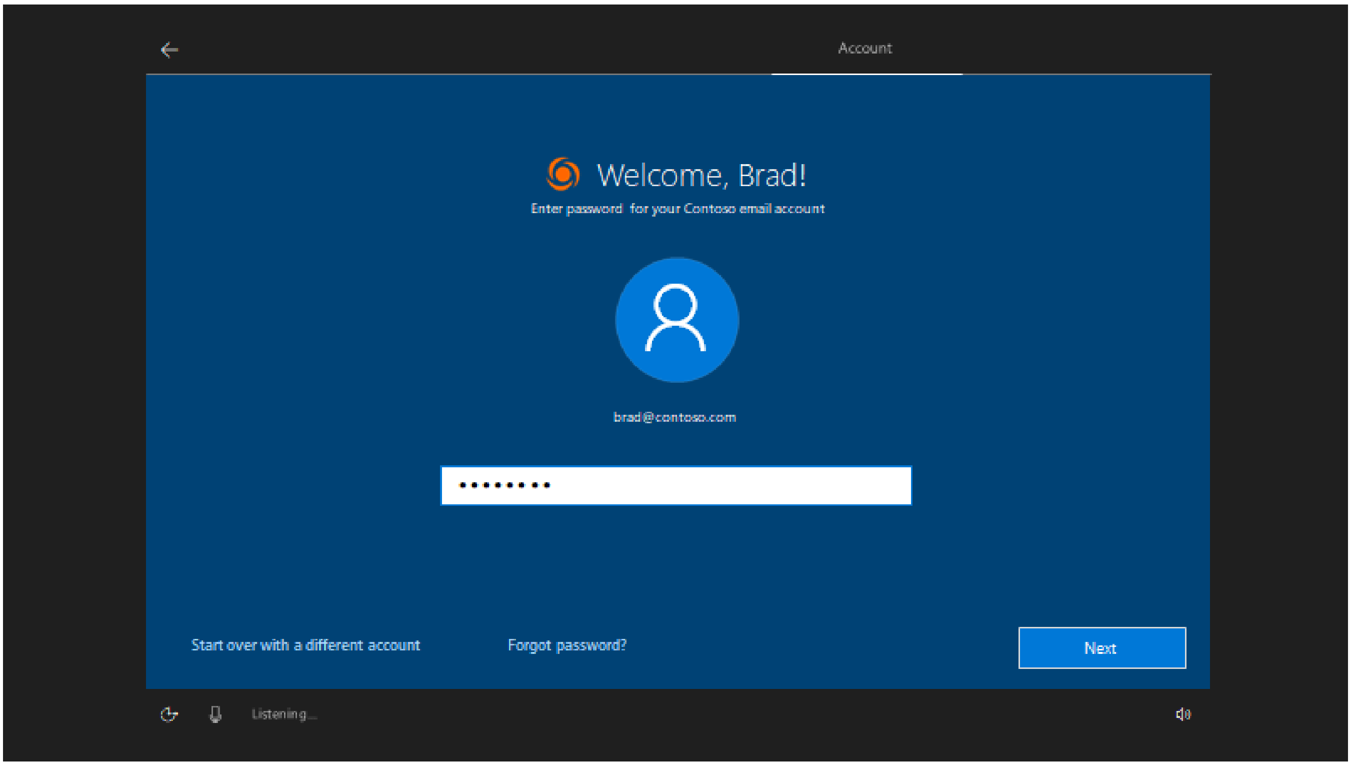
By clicking on the connect button you agree to our Terms of Service and have reviewed the Contoso Privacy Policy.



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



Now we'll check for any updates...

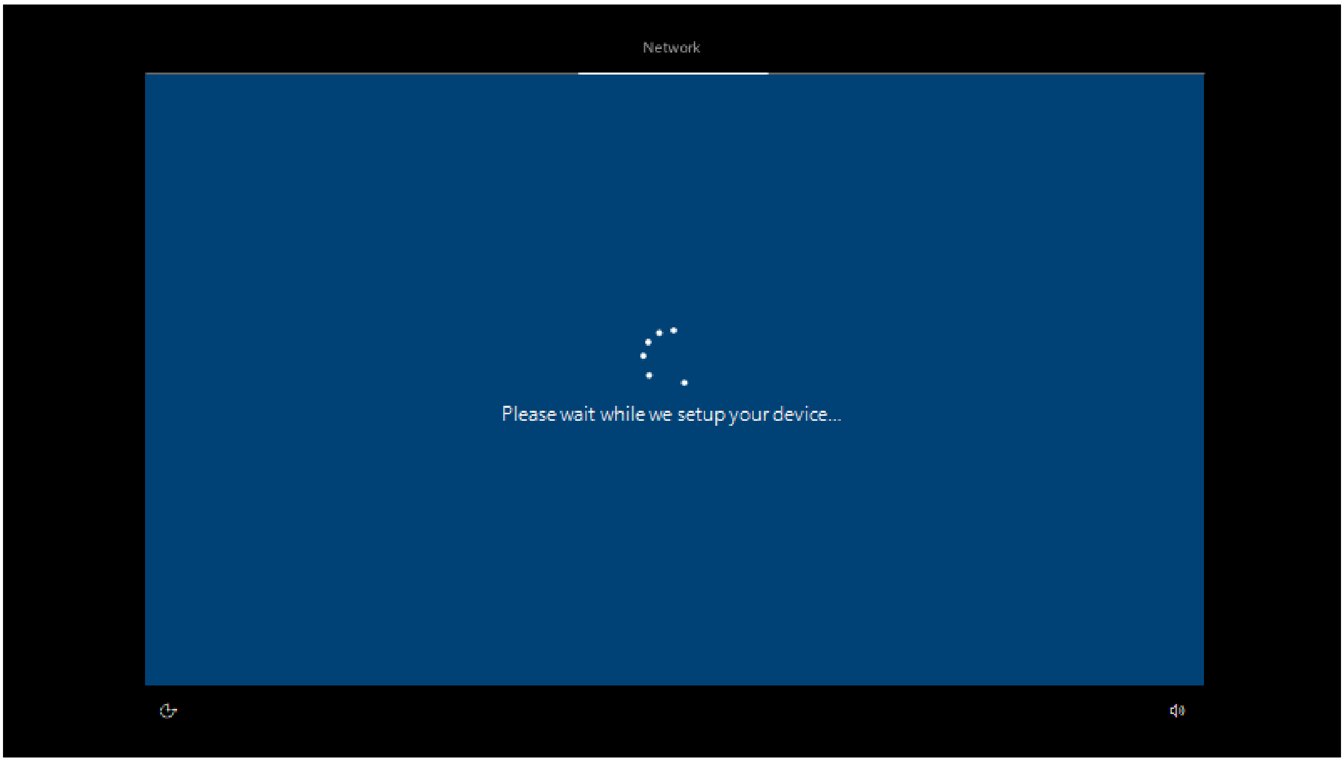


Account

Welcome, Brad!

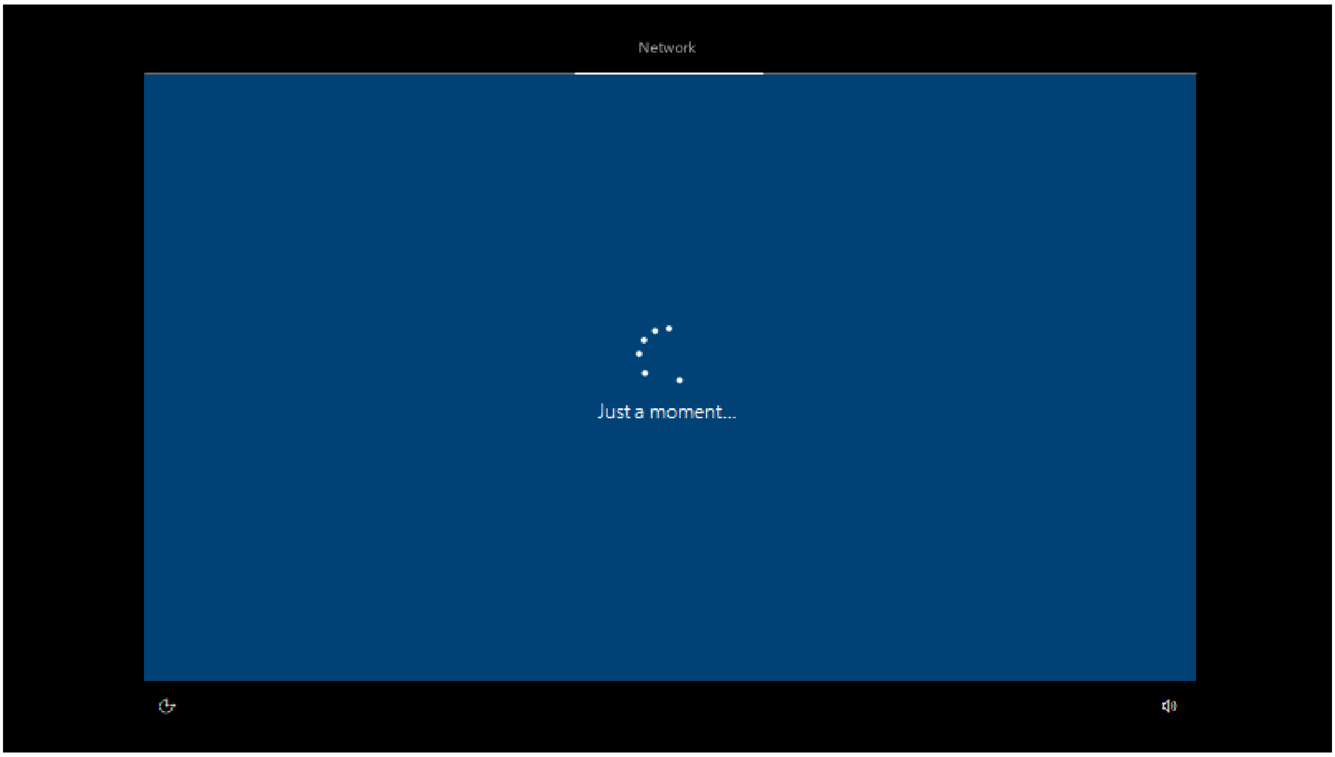
Enter password for your Contoso email account

brad@contoso.com

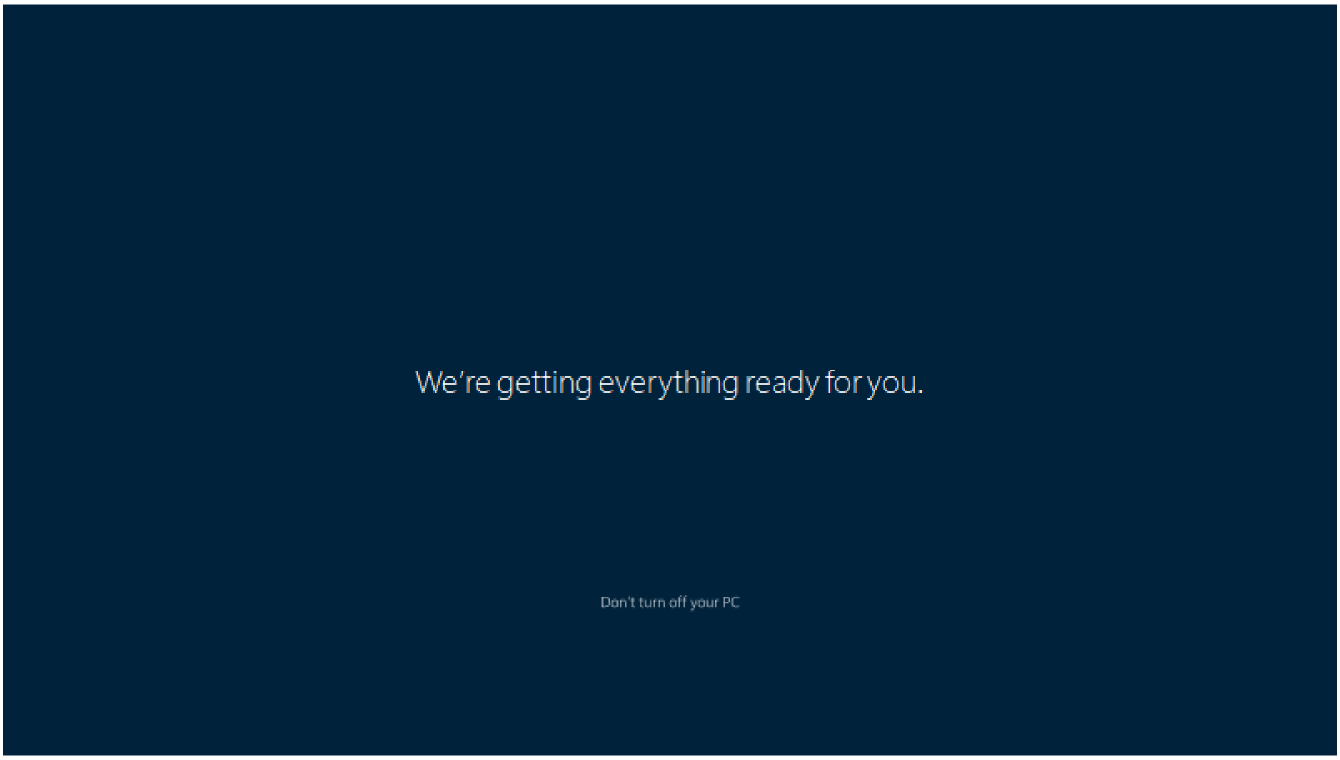


Network

Please wait while we setup your device...

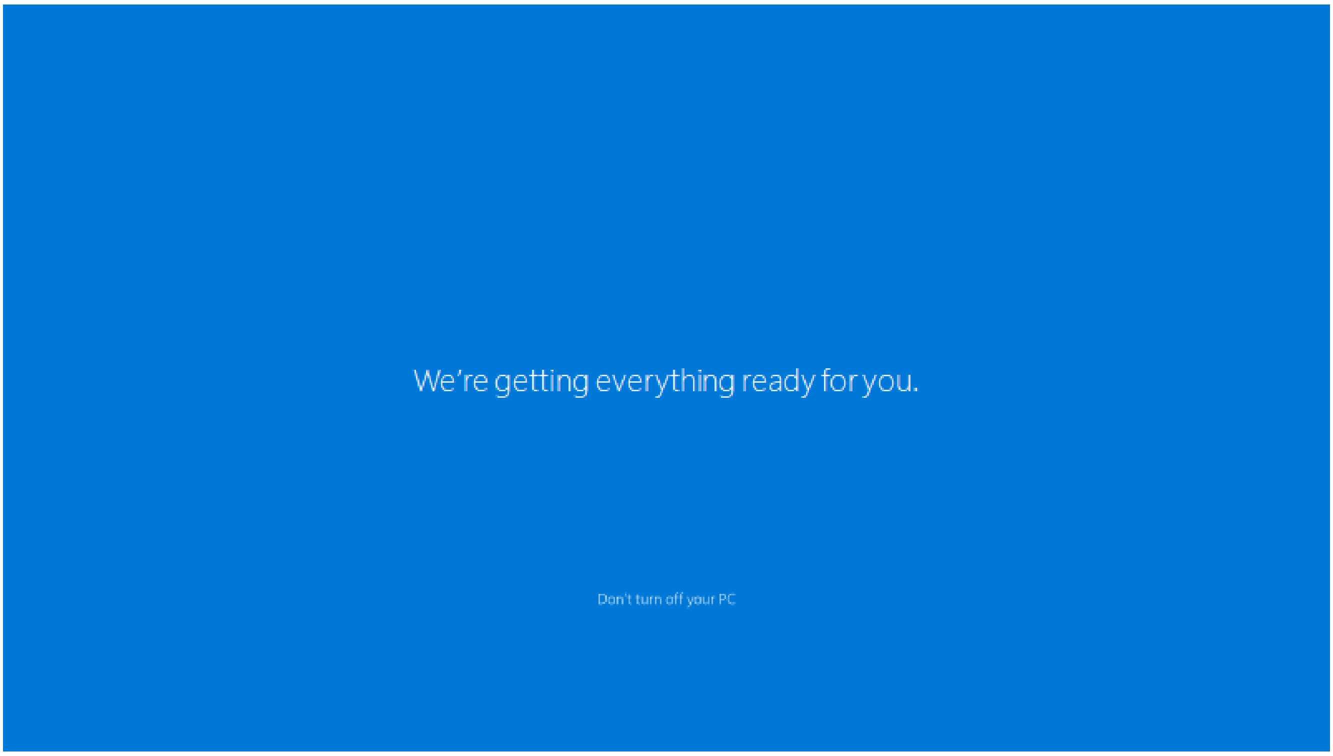


Just a moment...



We're getting everything ready for you.

Don't turn off your PC

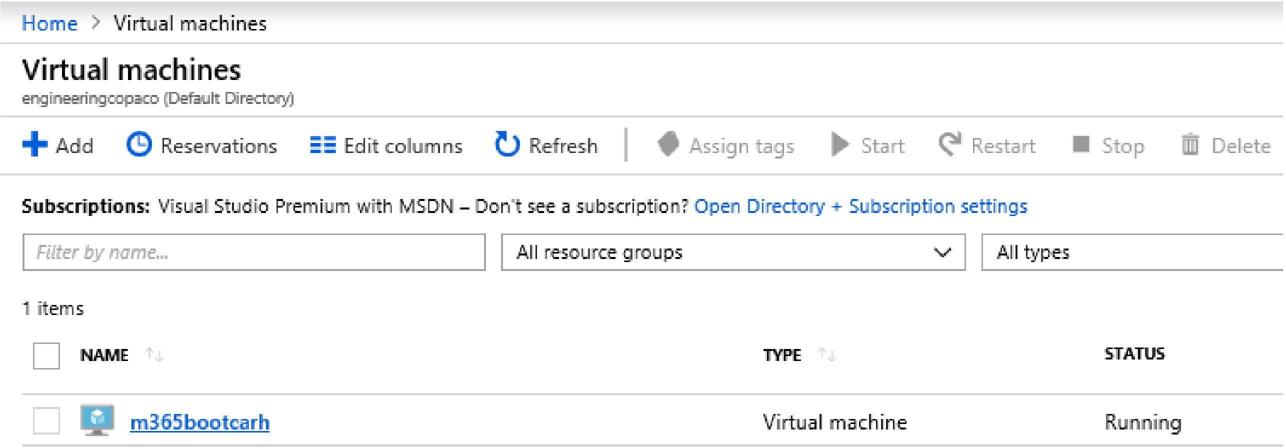


We’re getting everything ready for you.

Don’t turn off your PC

Exersize 6c Azure steps OPTIONAL

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



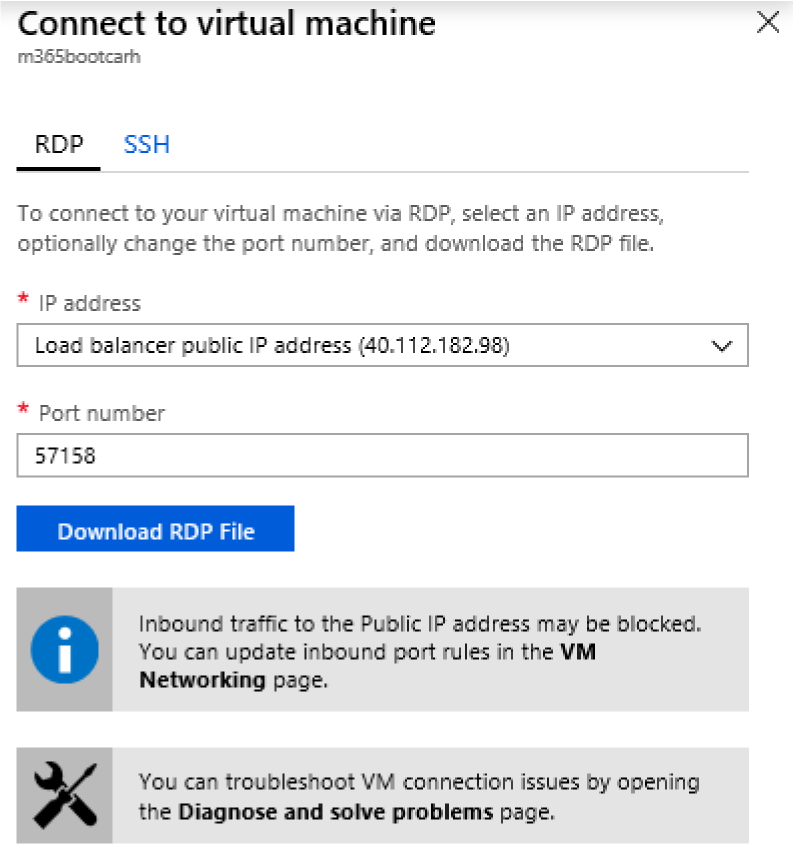
Virtual machines
engineeringcopaco (Default Directory)

Subscriptions: Visual Studio Premium with MSDN – Don't see a subscription? Open Directory + Subscription settings

All resource groups | All types

1 items

NAME	TYPE	STATUS
m365bootcarh	Virtual machine	Running



Connect to virtual machine
m365bootcarh

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

* IP address: Load balancer public IP address (40.112.182.98)

* Port number: 57158

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

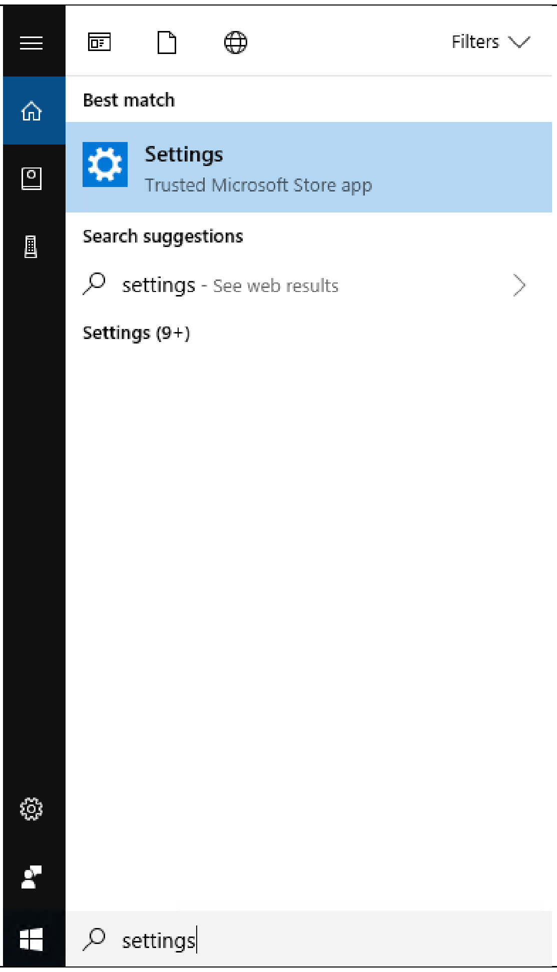
You can troubleshoot VM connection issues by opening the **Diagnose and solve problems** page.

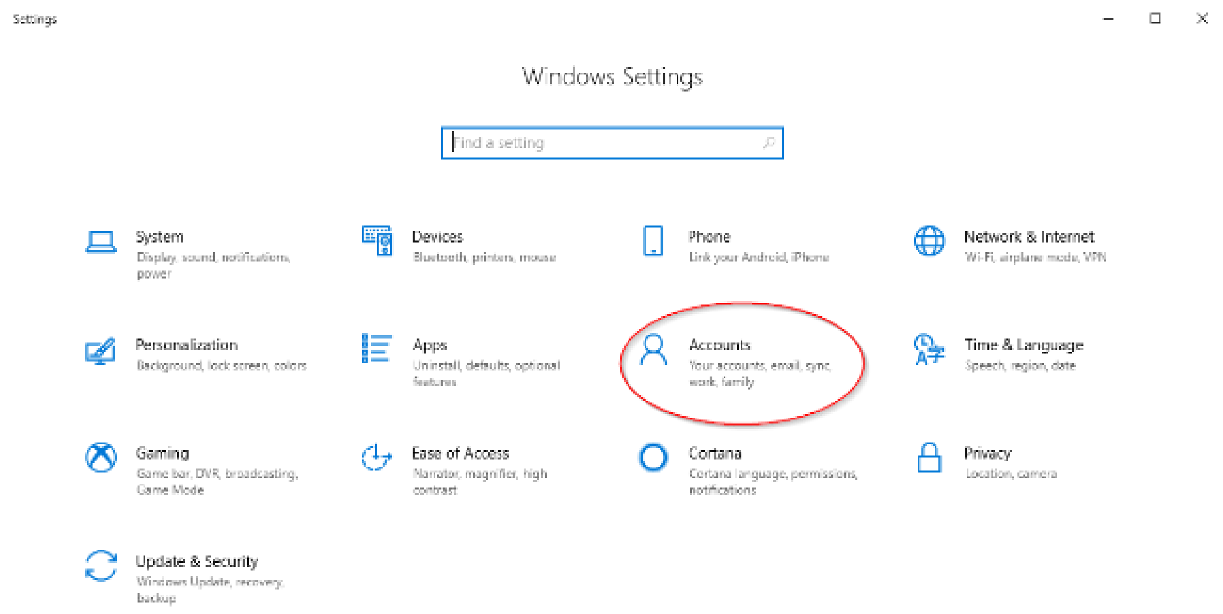
This section outlines how to enroll a Windows 10 device into Microsoft Intune for MDM.

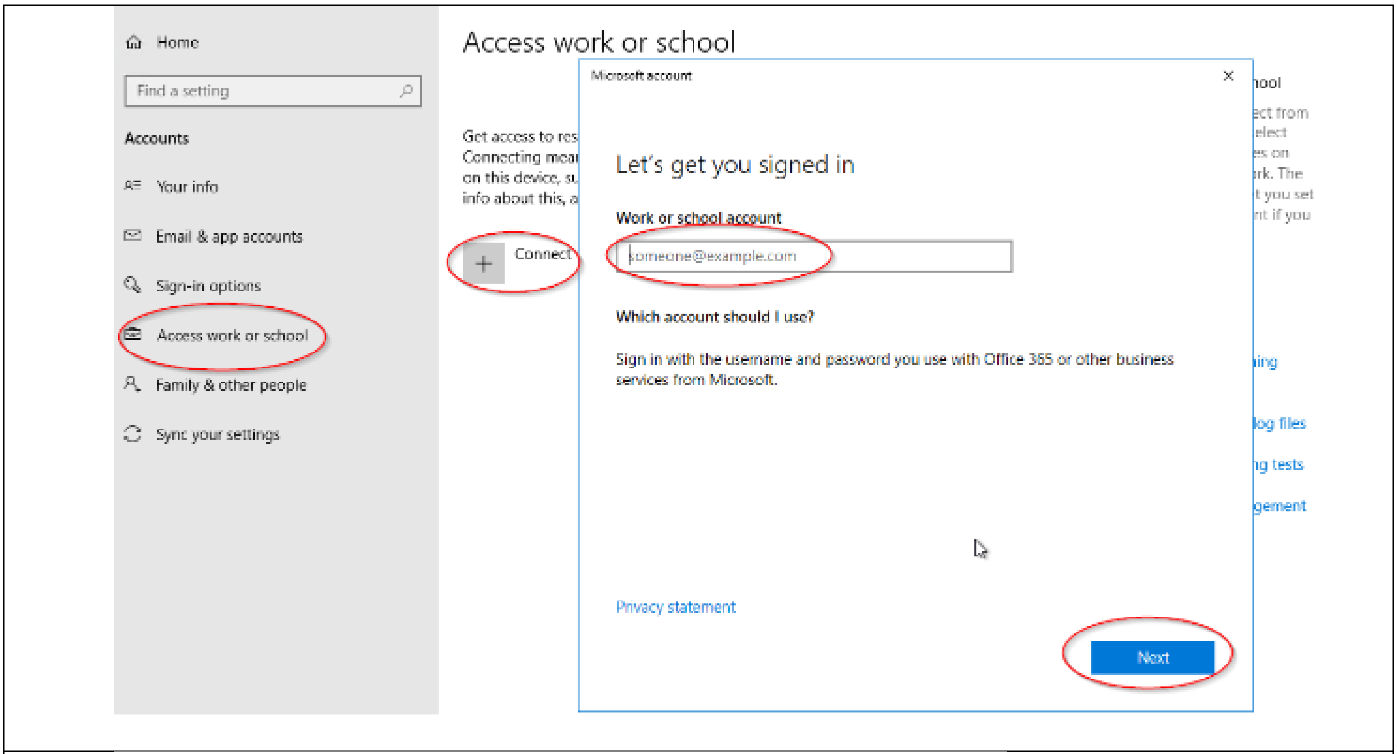
Complete these steps on the M365holwin10vm virtual machine.

Enroll a Windows 10 Device in Intune

1. Login to the virtual machine and go to **Start > Settings**.
2. In the **Settings** app, browse to **Accounts > Access work or school**.
3. Click **Enroll only in device management**.
4. The **Setup a work or school account** dialog box will show, asking for your account to enroll the device.
5. Provide the **Azure AD** account and click **Next**.
6. In the **Microsoft Intune Enrollment** page, enter the **password** then click **Sign in**. Click **Got it**.
7. In the **Settings** app, you should see that the device is now connected to the corporate MDM.
8. Click **Sync** and confirm that the sync was **successful**.




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



Access work or school

Get access to res
Connecting mea
on this device, su
info about this, a

Microsoft account

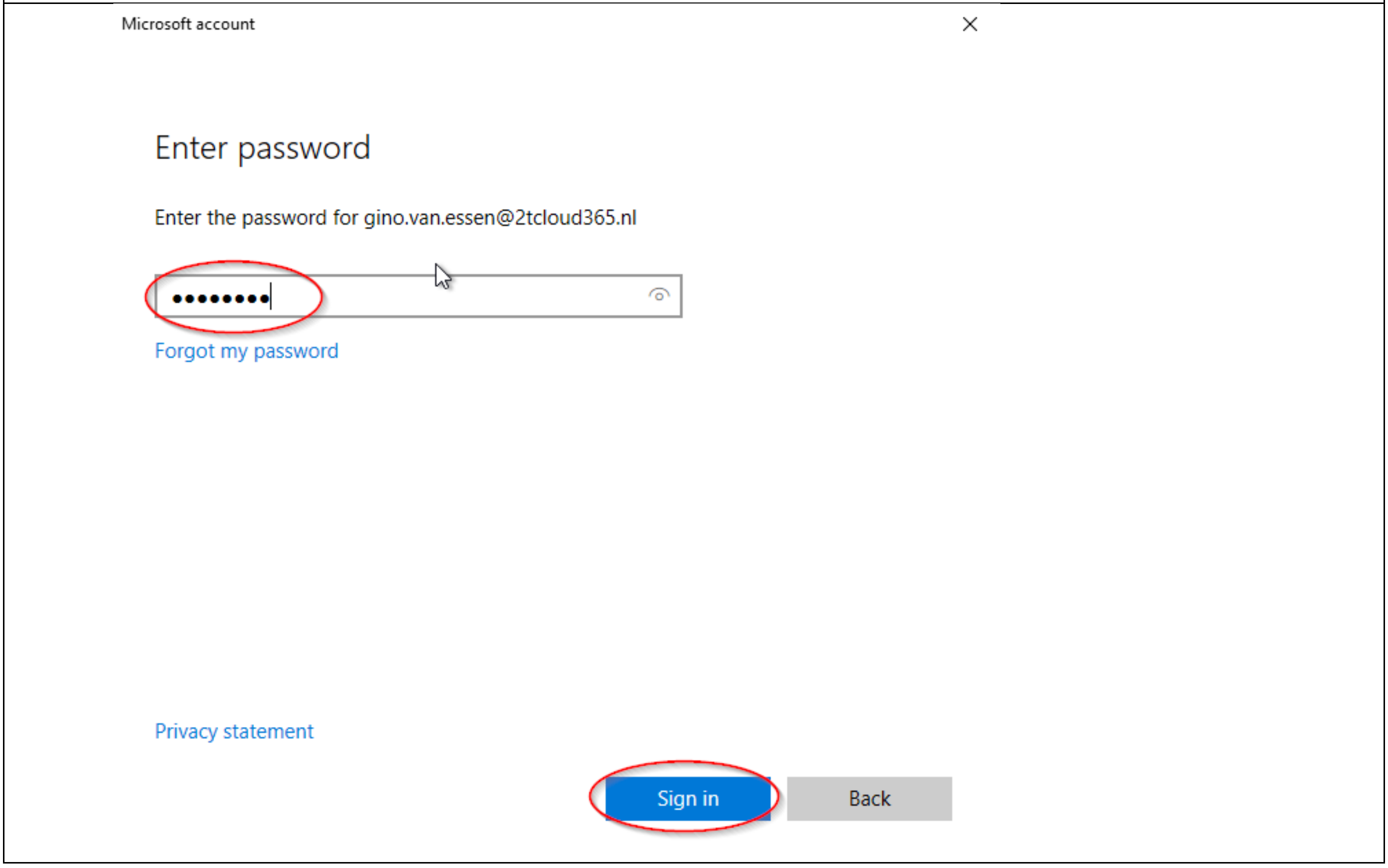
Let's get you signed in

Work or school account

someone@example.com

Which account should I use?

Sign in with the username and password you use with Office 365 or other business services from Microsoft.

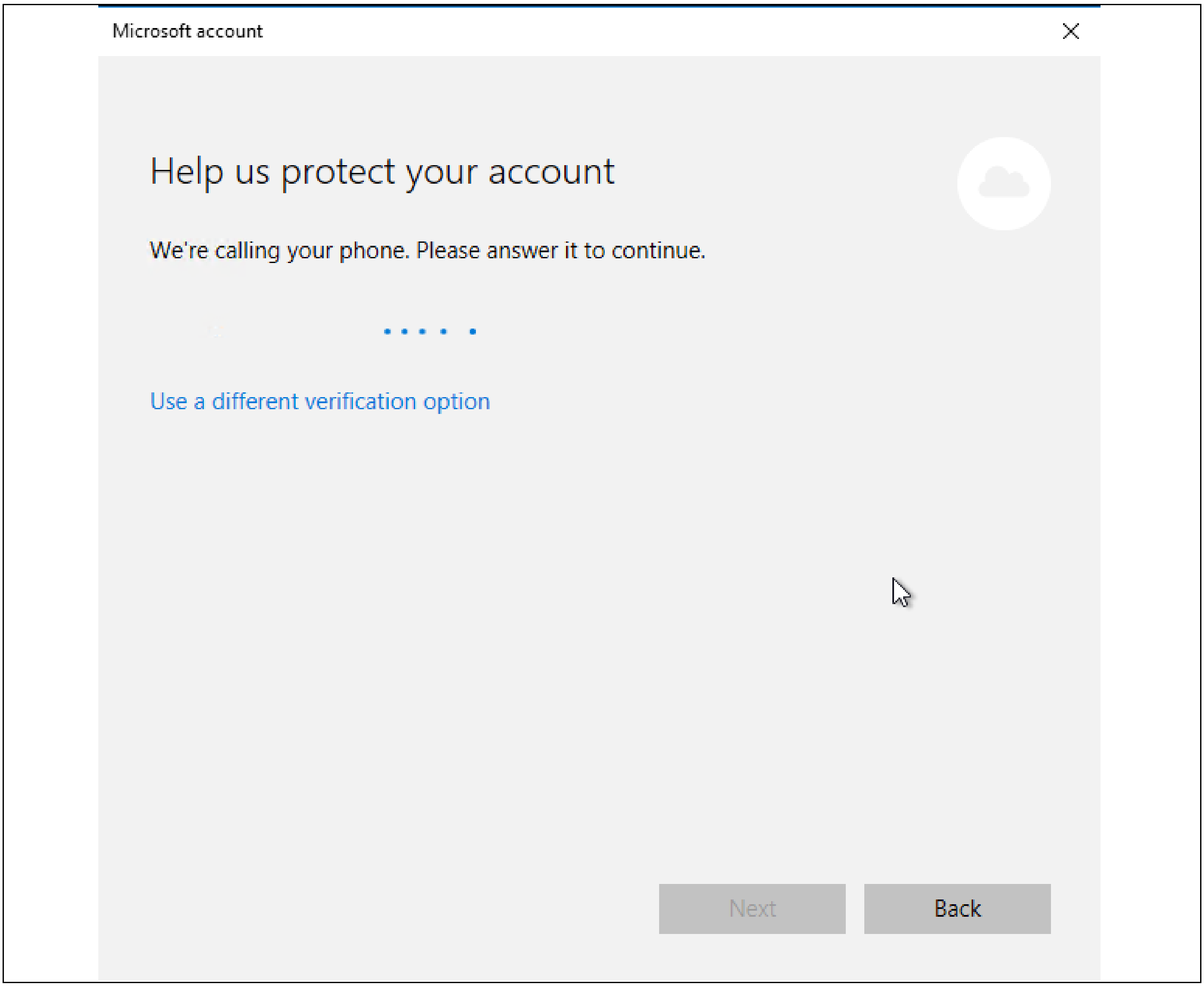


Microsoft account

Enter password

Enter the password for gino.van.essen@2tcloud365.nl

••••••••

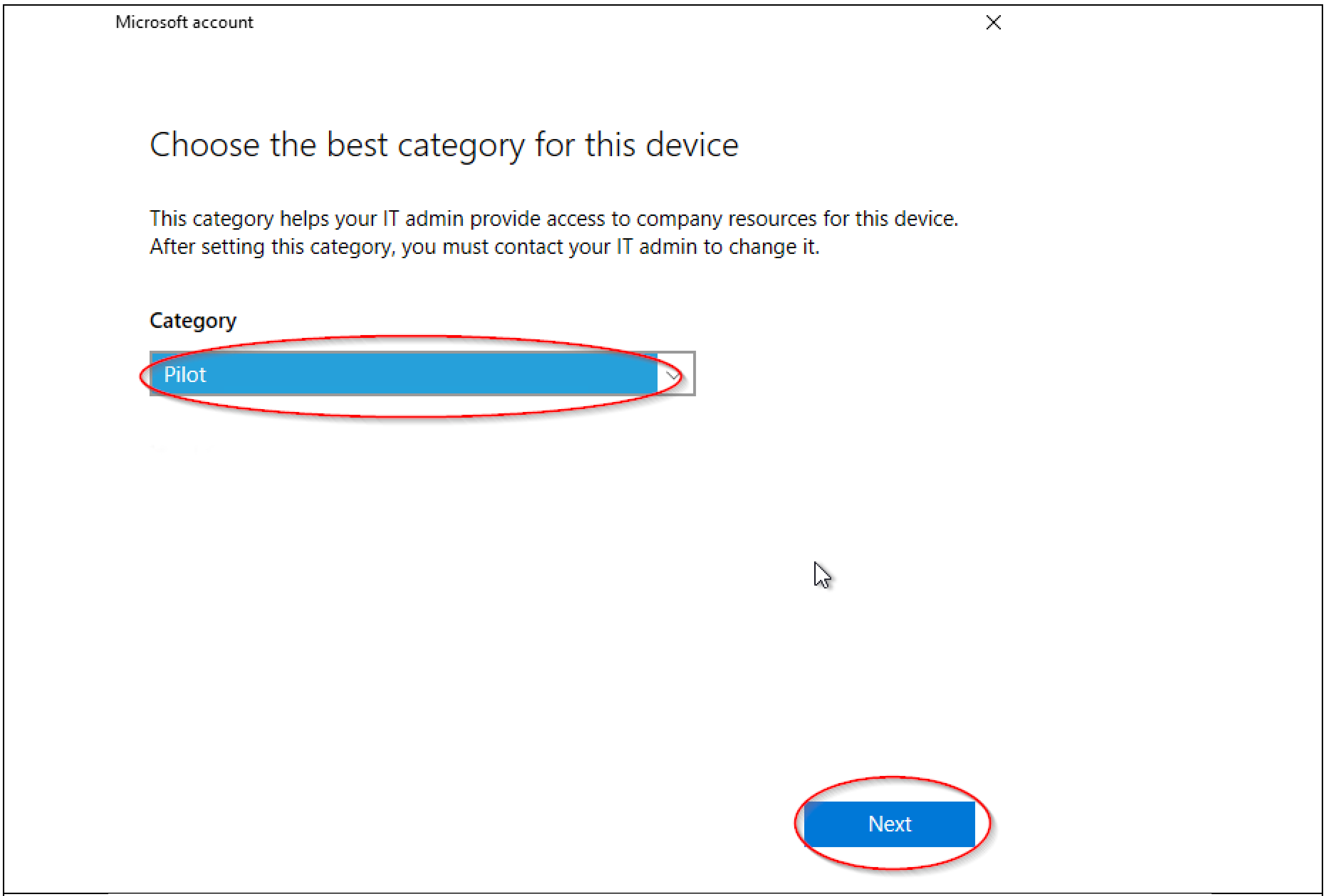


Microsoft account

Help us protect your account

We're calling your phone. Please answer it to continue.

Use a different verification option



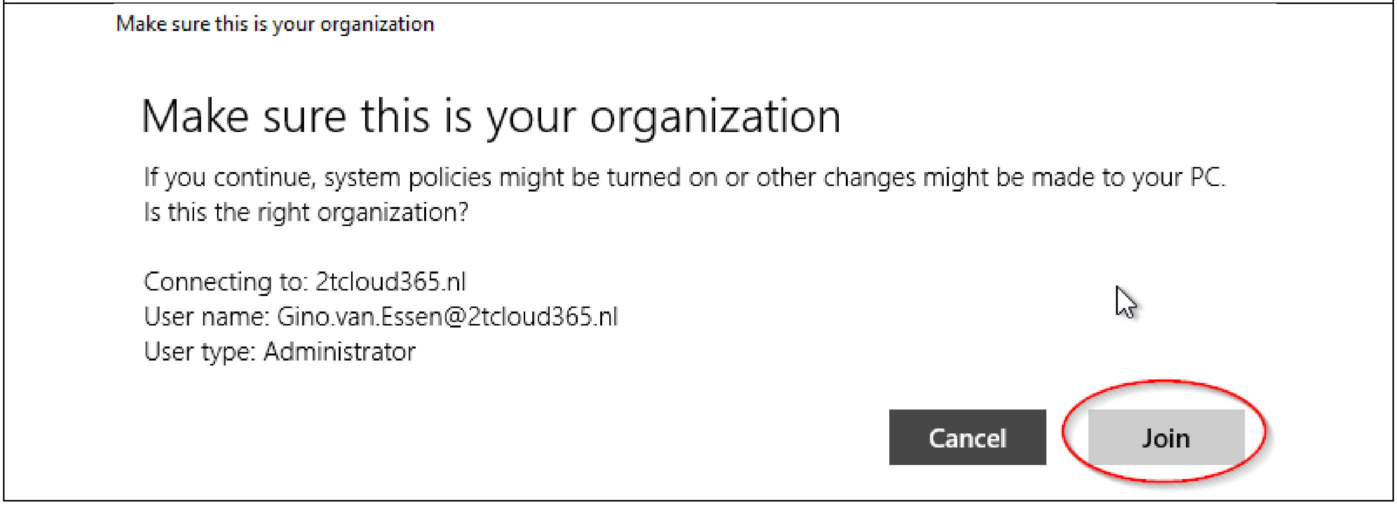
Microsoft account

Choose the best category for this device

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

Category

Pilot

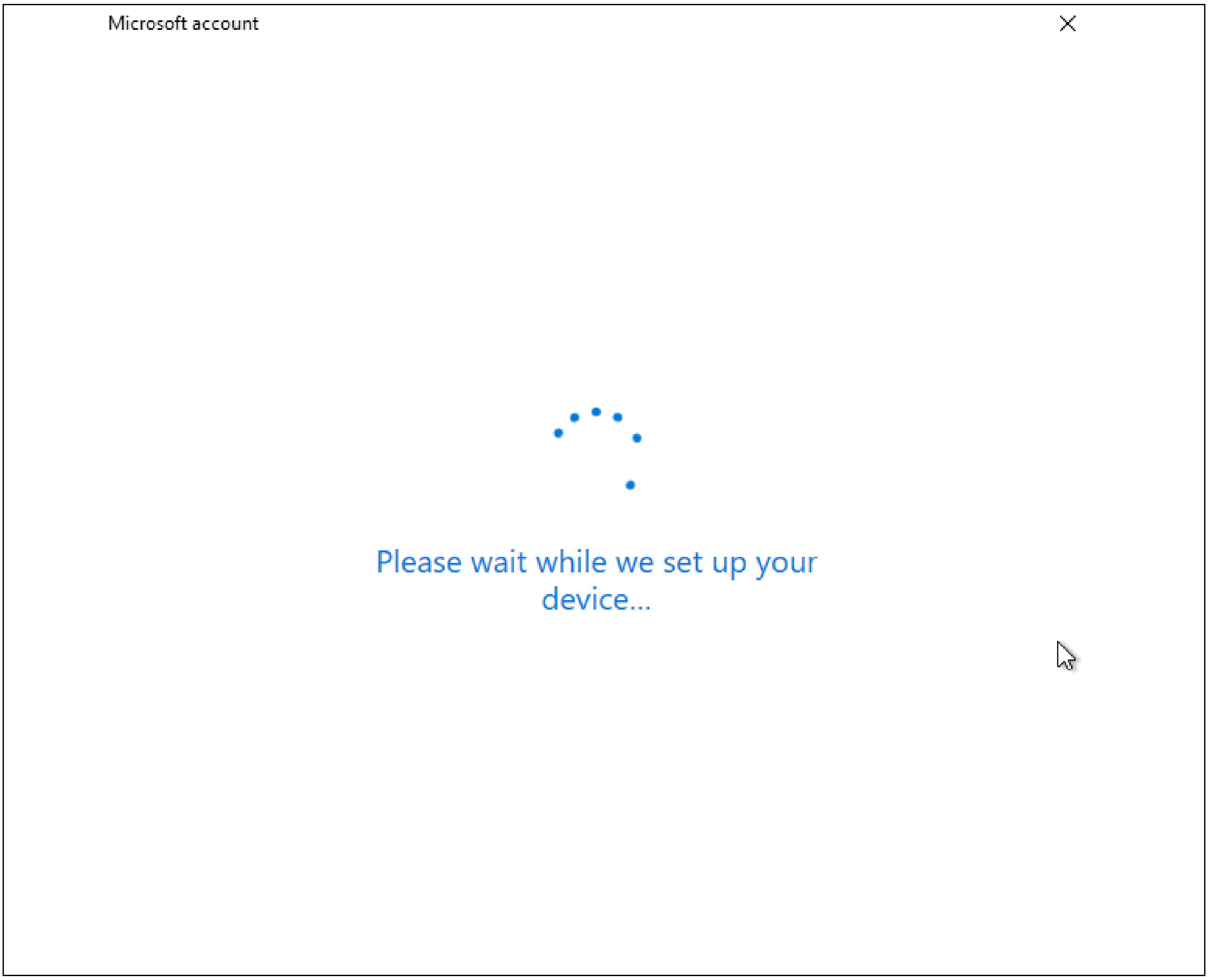


Make sure this is your organization

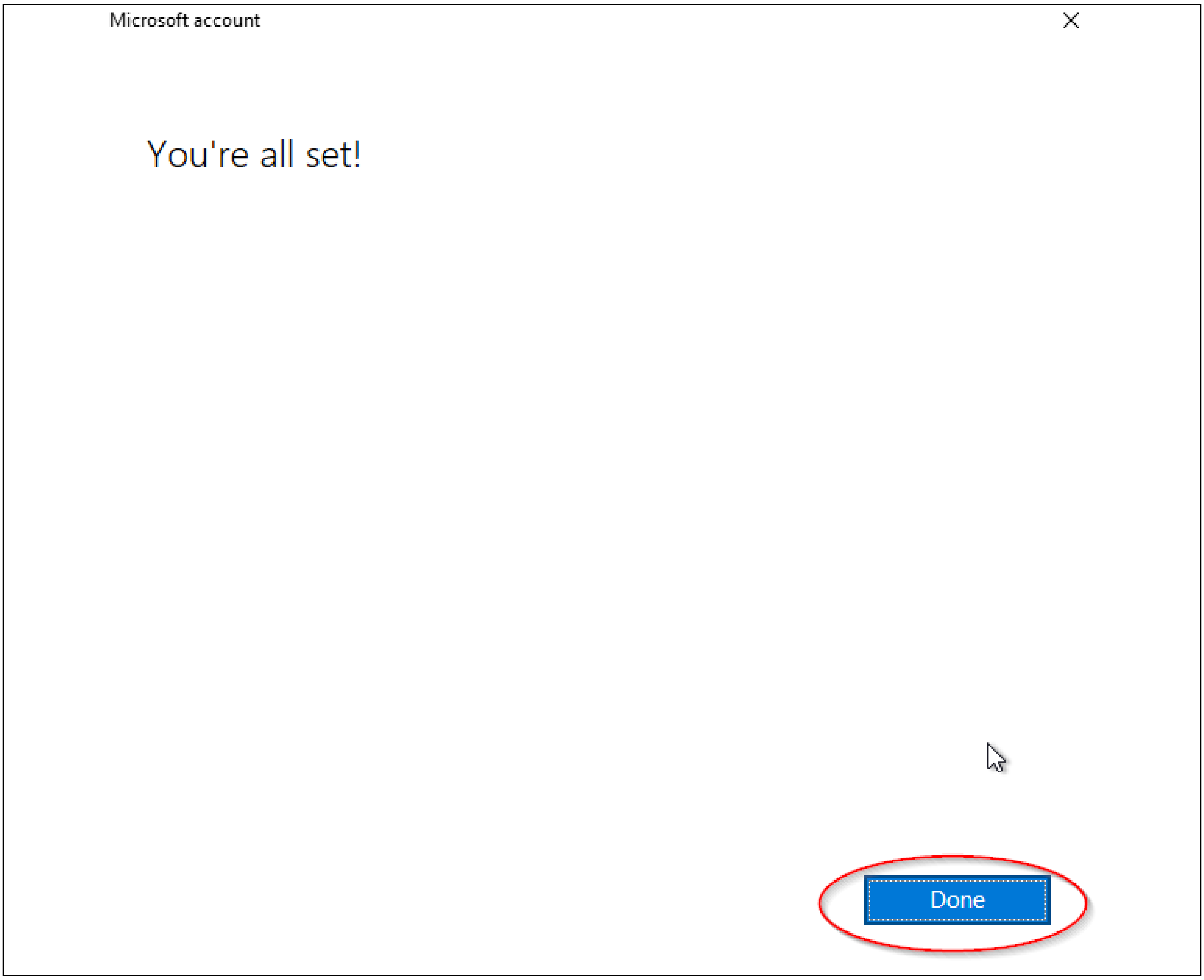
Make sure this is your organization

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

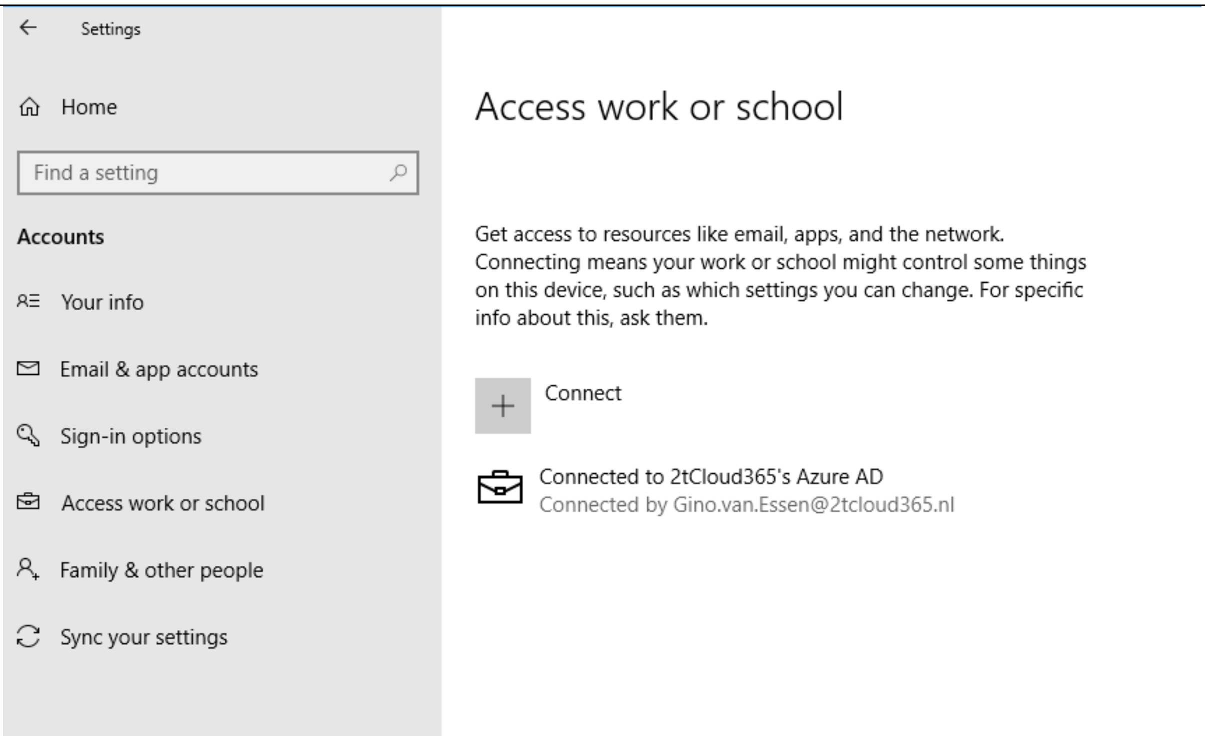
Connecting to: 2tcloud365.nl
User name: Gino.van.Essen@2tcloud365.nl
User type: Administrator



Please wait while we set up your device...



You're all set!

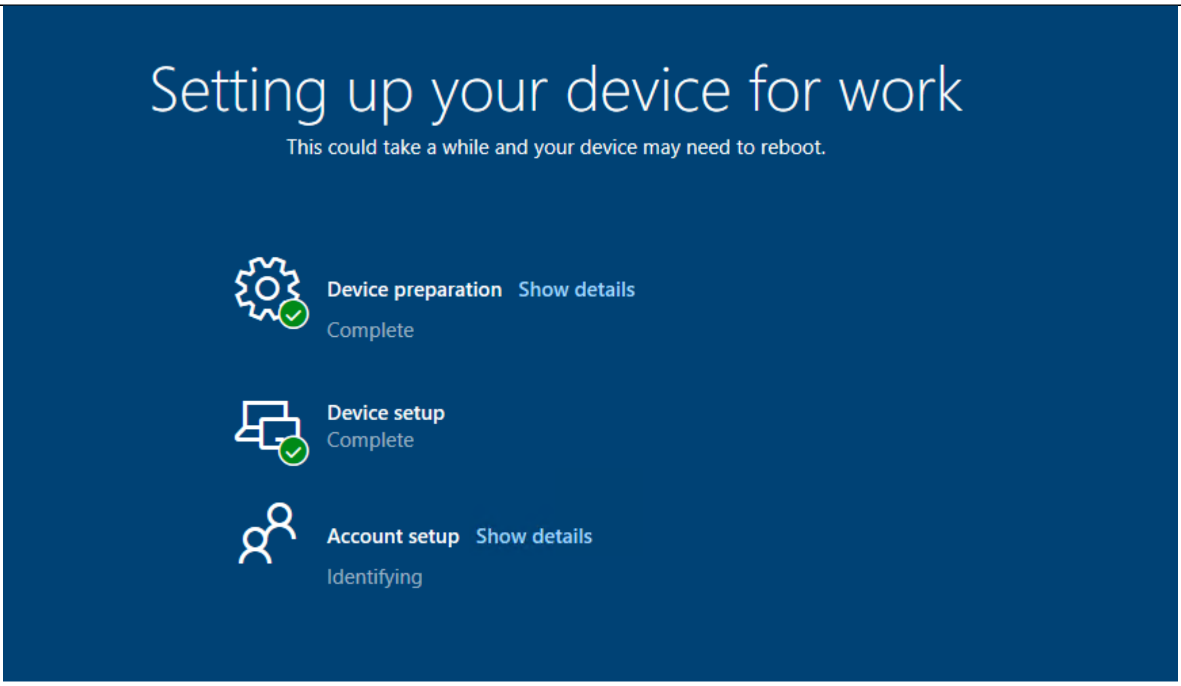


Access work or school

Get access to resources like email, apps, and the network. Connecting means your work or school might control some things on this device, such as which settings you can change. For specific info about this, ask them.

Connected to 2tCloud365's Azure AD
Connected by Gino.van.Essen@2tcloud365.nl

After reboot login with Azure AD account and credentials



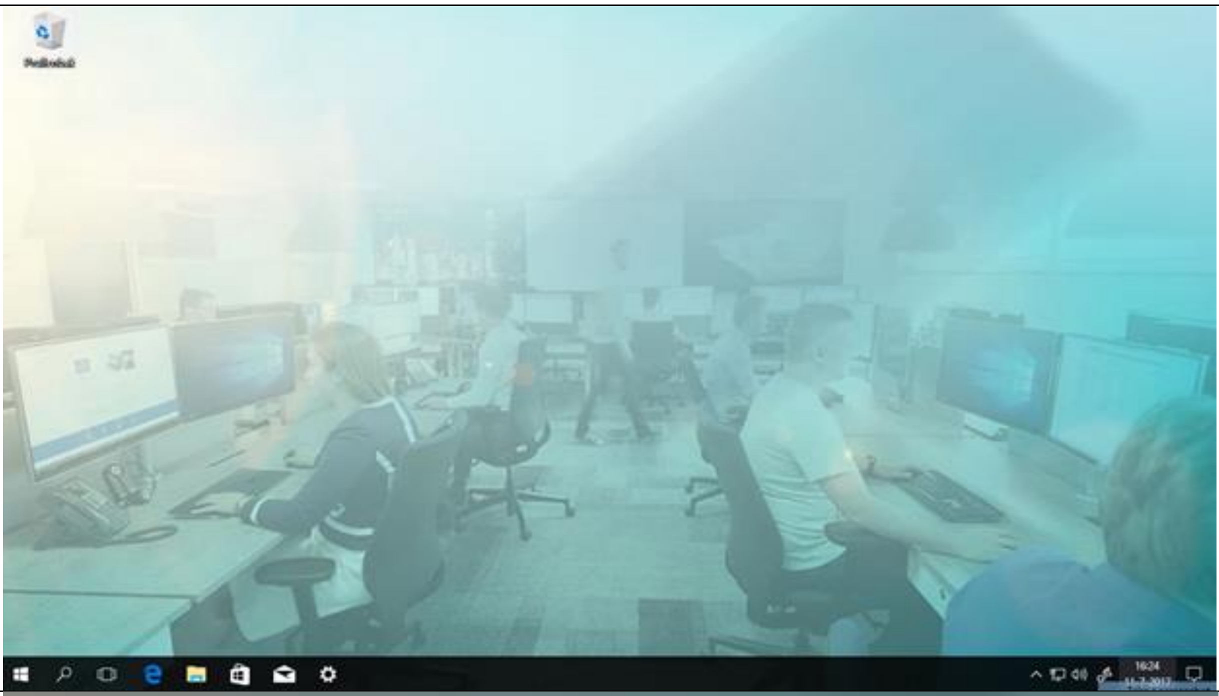
Setting up your device for work

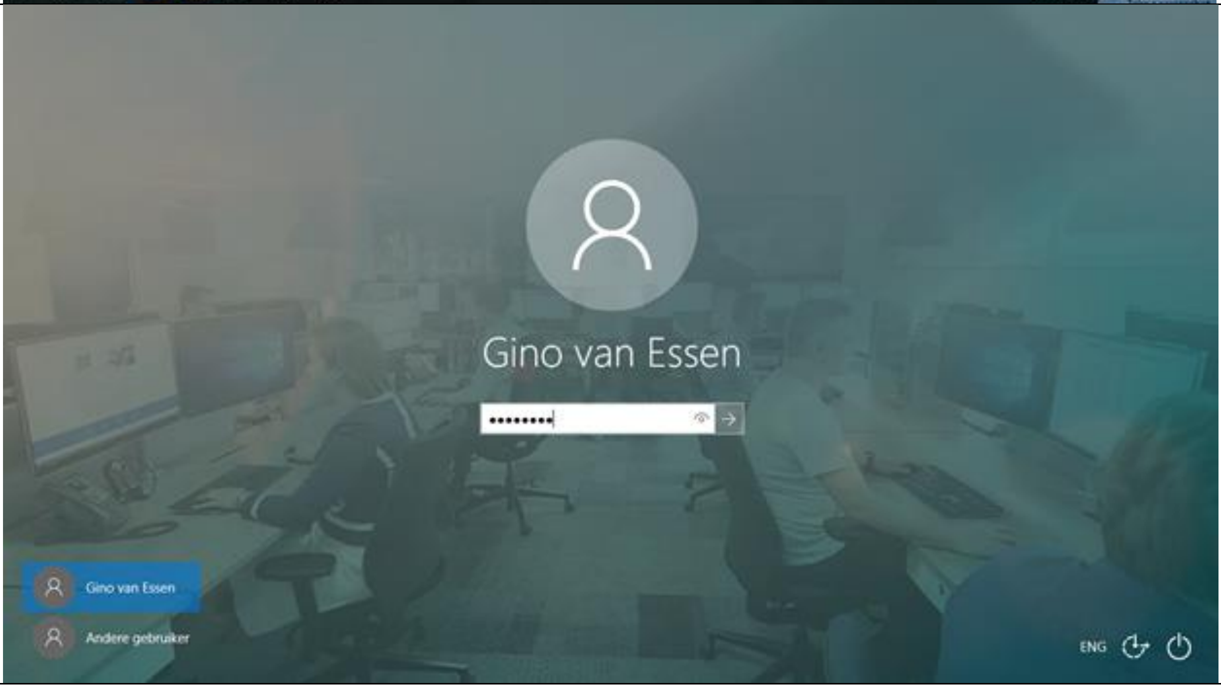
This could take a while and your device may need to reboot.

Device preparation
Complete

Device setup
Complete

Account setup
Identifying

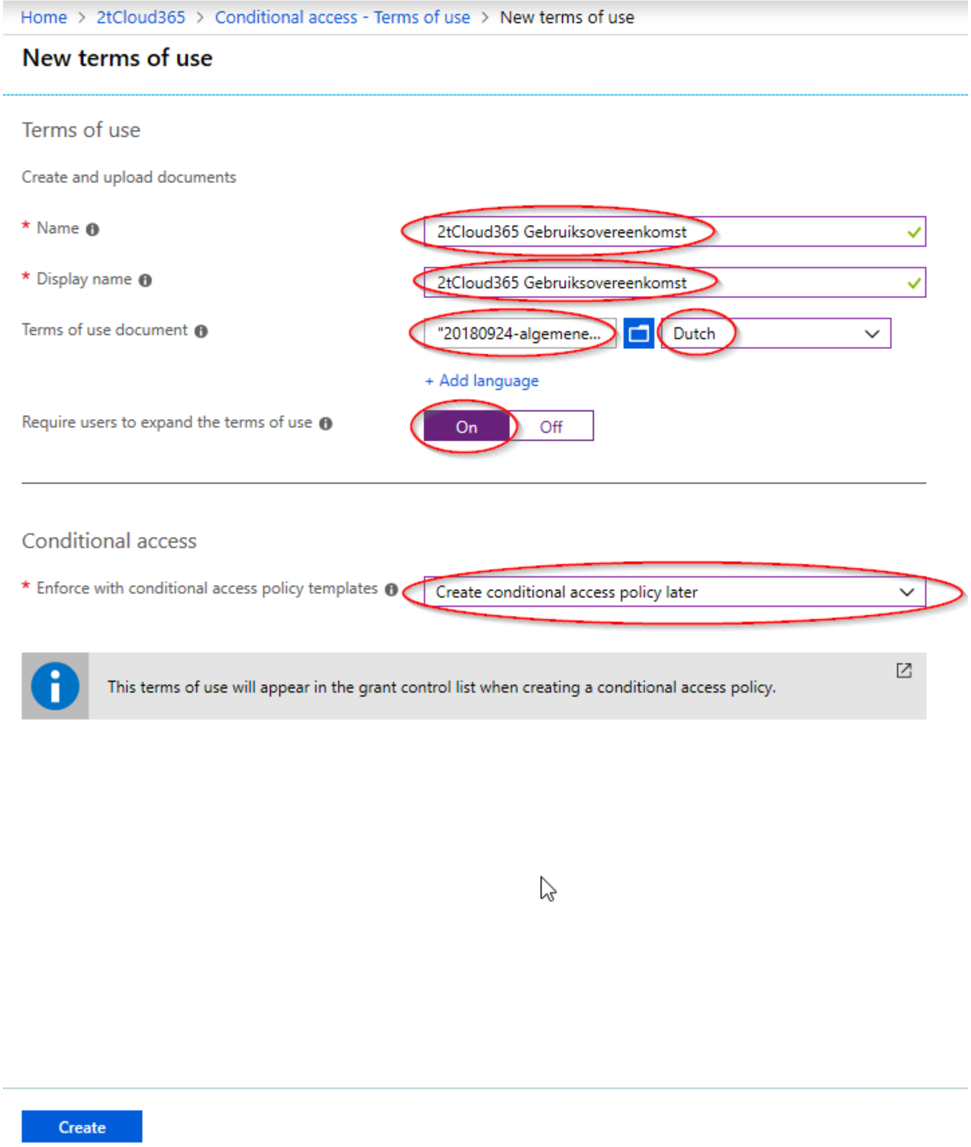

Prullenbak
16:24
11-7-2017


Gino van Essen
••••••••
Gino van Essen
Andere gebruiker
ENG

Activity 4: Configuration Intune

Exercise 7: Terms of use

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



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

New terms of use

Terms of use

Create and upload documents

* Name: 2tCloud365 Gebruiksovereenkomst

* Display name: 2tCloud365 Gebruiksovereenkomst

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

+ Add language

Require users to expand the terms of use: [✓ On] Off

Conditional access

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

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

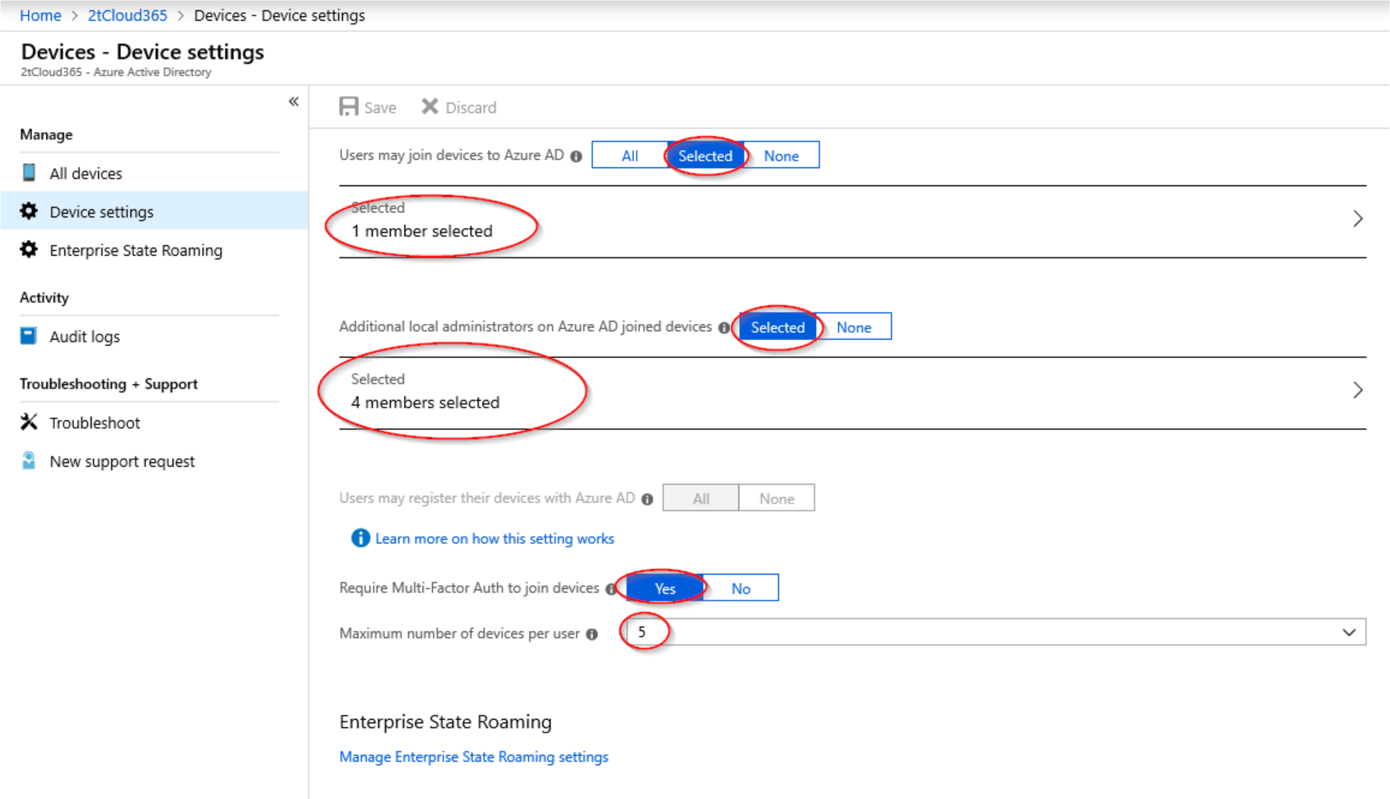
2. Create new -> Configure the settings -> Click **Create**

Name	2tCloud365 Gebruiksovereenkomst or your own
Display name	2tCloud365 Gebruiksovereenkomst or your own
Terms of Use document	Add pdf document
Language	English or Dutch

Enfore with conditional access policy templates	Create conditional access policy later

Exercise 8: Device Settings

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


Home > 2tCloud365 > Devices - Device settings
Devices - Device settings
2tCloud365 - Azure Active Directory
Save
Discard
Manage
All devices
Device settings
Enterprise State Roaming
Activity
Audit logs
Troubleshooting + Support
Troubleshoot
New support request
Learn more on how this setting works
Manage Enterprise State Roaming settings

Users may join devices to Azure AD: All [✓ Selected] None

Selected
1 member selected

Additional local administrators on Azure AD joined devices: [✓ Selected] None

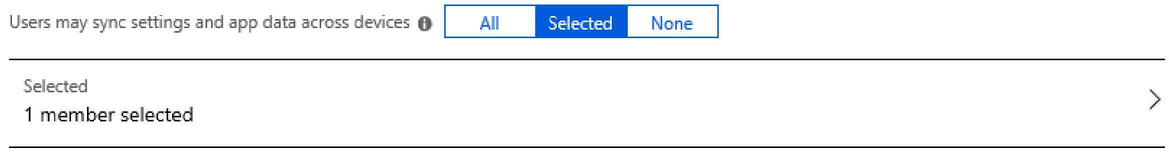
Selected
4 members selected

Users may register their devices with Azure AD: All None

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

Maximum number of devices per user: 5

Enterprise State Roaming



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

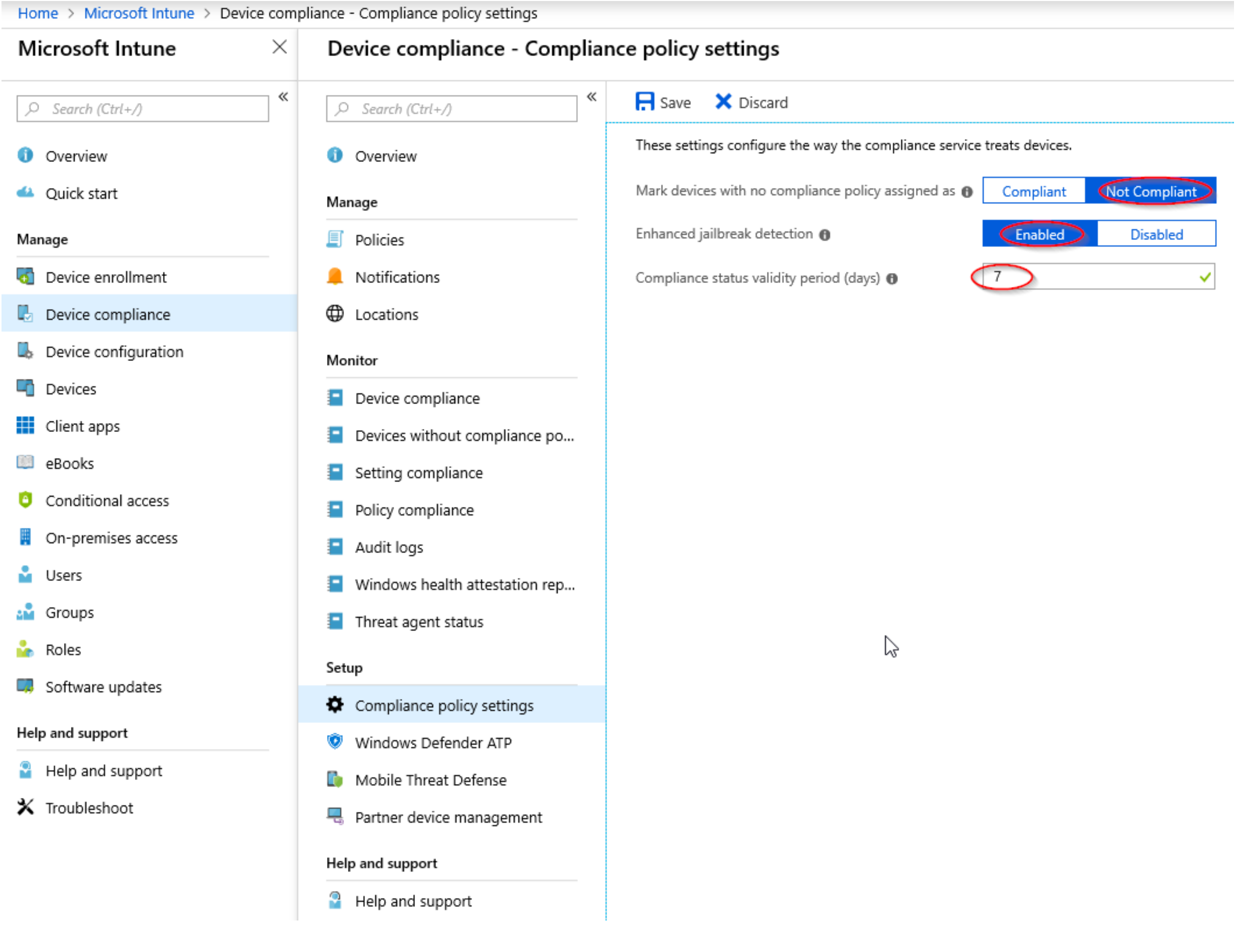
Selected
1 member selected

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

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

Exercise 9: Device Compliance

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



These settings configure the way the compliance service treats devices.

Mark devices with no compliance policy assigned as: Compliant [✓ Not Compliant]

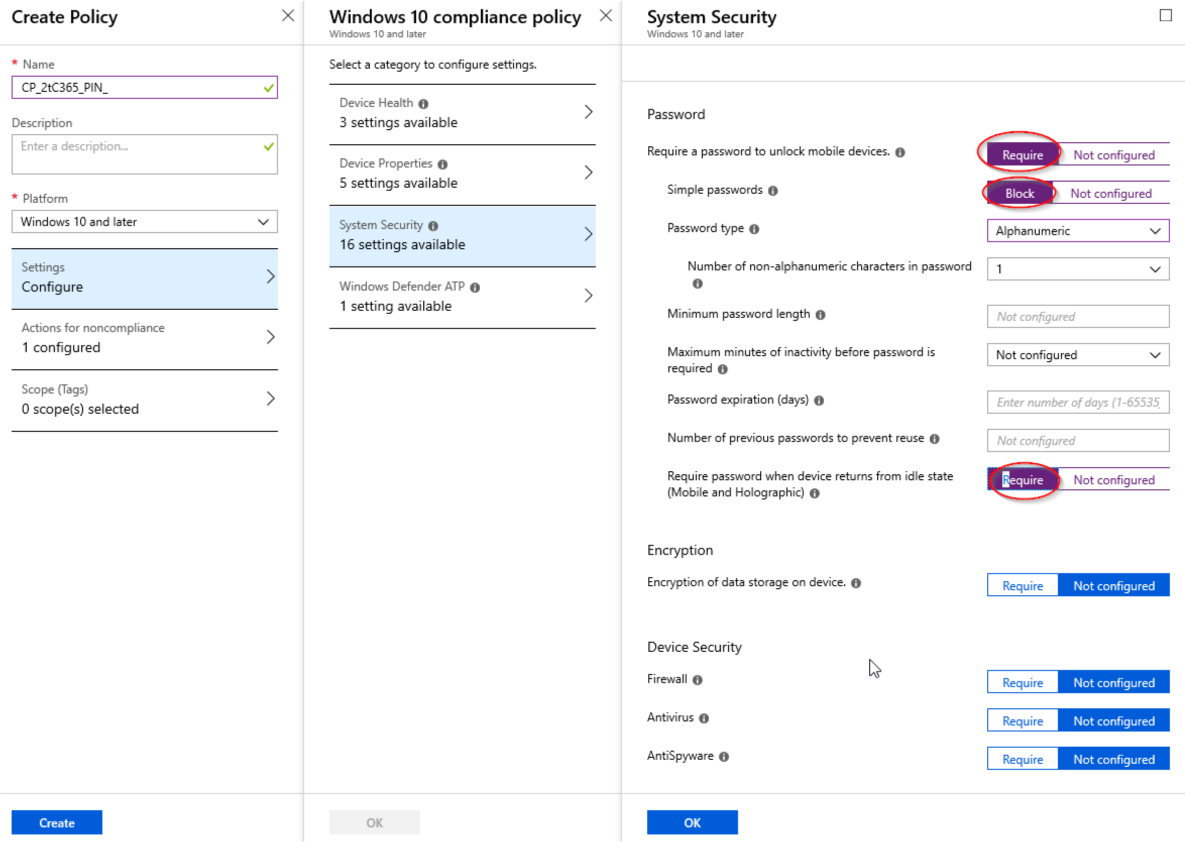
Enhanced jailbreak detection: [✓ Enabled] Disabled

Compliance status validity period (days): 7

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

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

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



Create Policy

* Name: CP_2tC365_PIN_

Description: Enter a description...

* Platform: Windows 10 and later

Settings: Configure

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

Windows 10 compliance policy — Windows 10 and later

Select a category to configure settings.

Device Health: 3 settings available

Device Properties: 5 settings available

System Security: 16 settings available

Windows Defender ATP: 1 setting available

System Security — Windows 10 and later

Password

Require a password to unlock mobile devices.: [✓ Require] Not configured

Simple passwords: [✓ Block] Not configured

Password type: Alphanumeric

Number of non-alphanumeric characters in password: 1

Minimum password length: Not configured

Maximum minutes of inactivity before password is required: Not configured

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

Number of previous passwords to prevent reuse: Not configured

Require password when device returns from idle state (Mobile and Holographic): [✓ Require] Not configured

Encryption

Encryption of data storage on device.: Require [✓ Not configured]

Device Security

Firewall: Require [✓ Not configured]

Antivirus: Require [✓ Not configured]

AntiSpyware: Require [✓ Not configured]

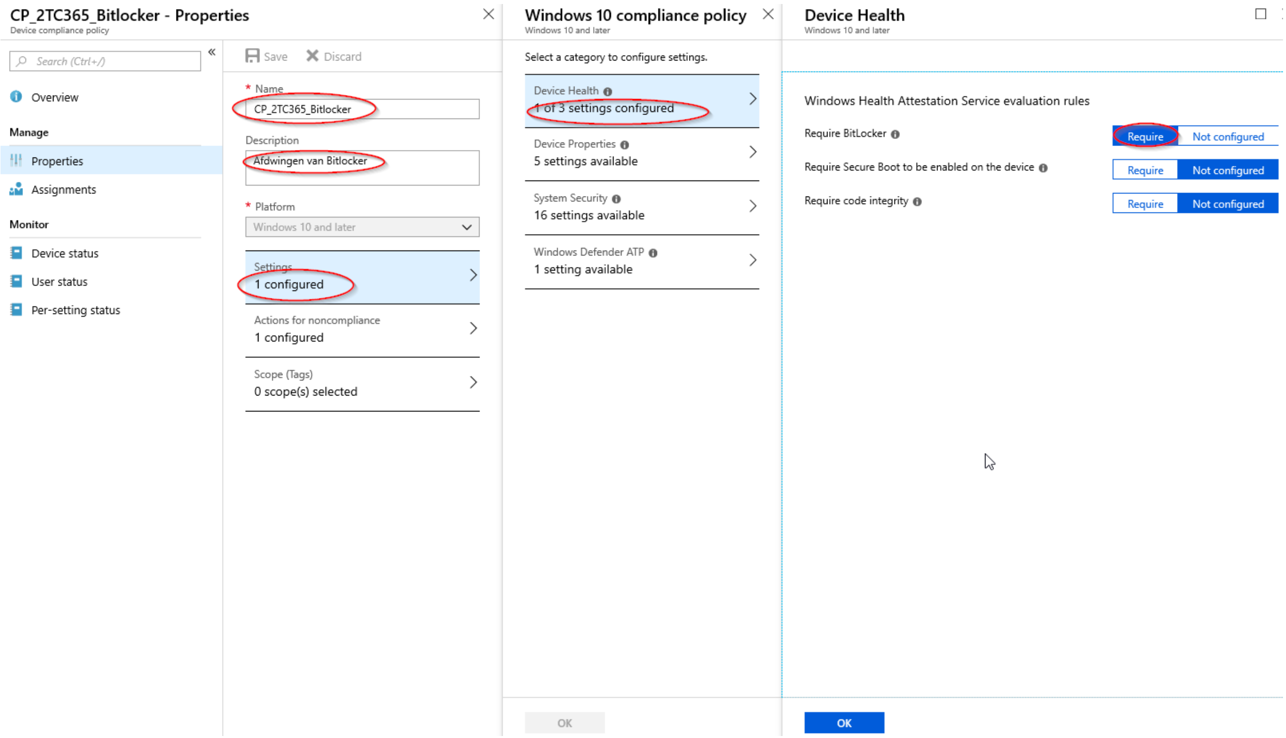
2. Configure the settings >

Name	CP_2tC365_PIN
Platform	Windows 10 and later

3. Click on **Configure**

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

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



CP_2TC365_Bitlocker - Properties
Device compliance policy

Search (Ctrl+/)

Overview

Manage

Properties

Assignments

Monitor

Device status

User status

Per-setting status

Save Discard

* Name: CP_2TC365_Bitlocker

Description: Afdwingen van Bitlocker

* Platform: Windows 10 and later

Settings: 1 configured

Actions for noncompliance: 1 configured

Scope (Tags): 0 scope(s) selected

Windows 10 compliance policy
Windows 10 and later

Select a category to configure settings.

Device Health: 1 of 3 settings configured

Device Properties: 5 settings available

System Security: 16 settings available

Windows Defender ATP: 1 setting available

OK

Device Health
Windows 10 and later

Windows Health Attestation Service evaluation rules

Require BitLocker	[✓ Require] Not configured
Require Secure Boot to be enabled on the device	Require [✓ Not configured]
Require code integrity	Require [✓ Not configured]

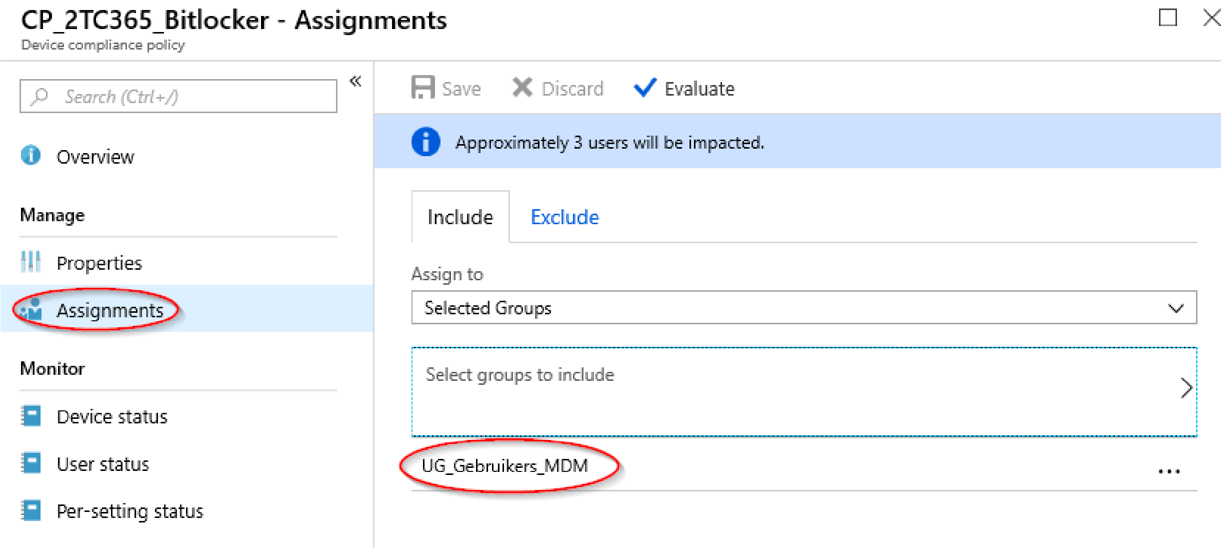
OK

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

Name	CP_2TC365_Bitlocker
Description	Afdwingen van Bitlocker
Platform	Windows 10 and later

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

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



CP_2TC365_Bitlocker - Assignments

Device compliance policy

Approximately 3 users will be impacted.

Assign to: Selected Groups

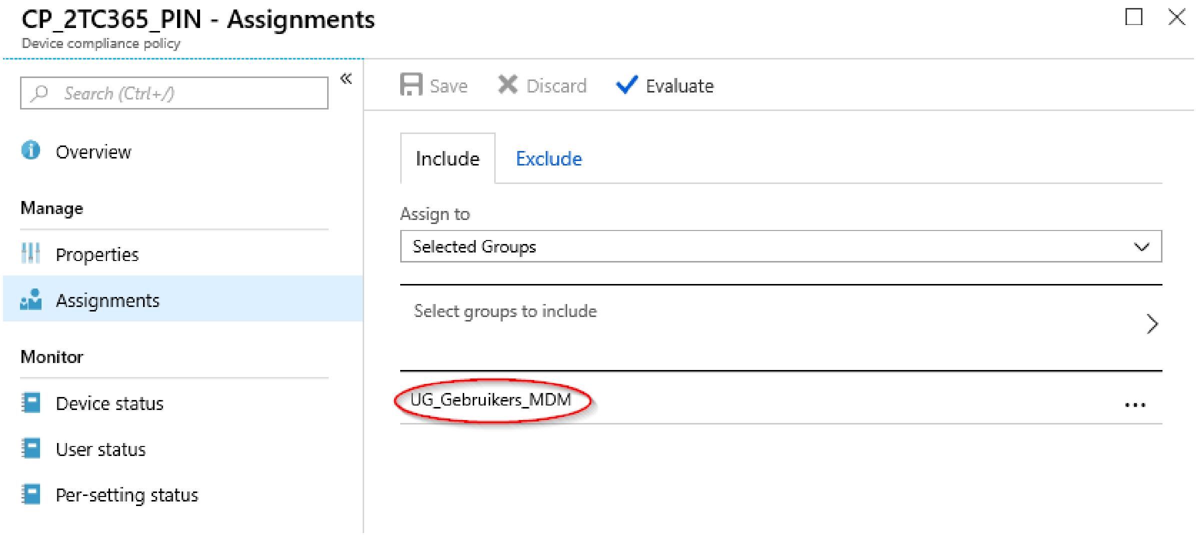
Select groups to include

UG_Gebruikers_MDM

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

Groups	UG_Gebruikers_MDM

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



CP_2TC365_PIN - Assignments

Device compliance policy

Assign to: Selected Groups

Select groups to include

UG_Gebruikers_MDM

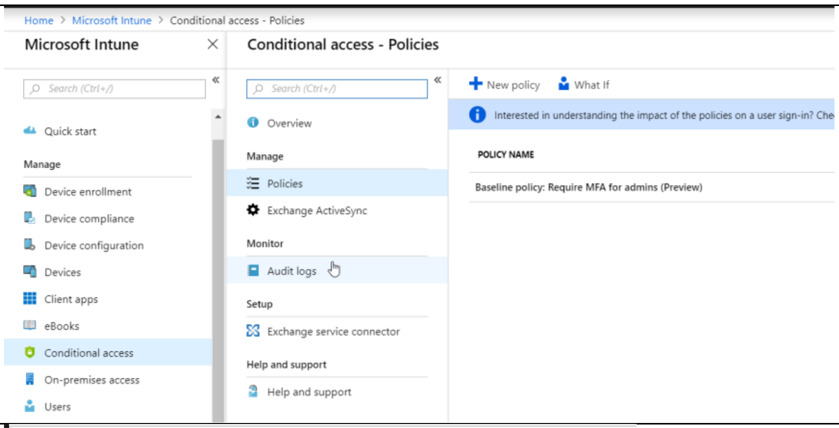
10. Configure the settings > Click **Save**

Groups	UG_Gebruikers_MDM

Exercise 10: Conditional Access

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

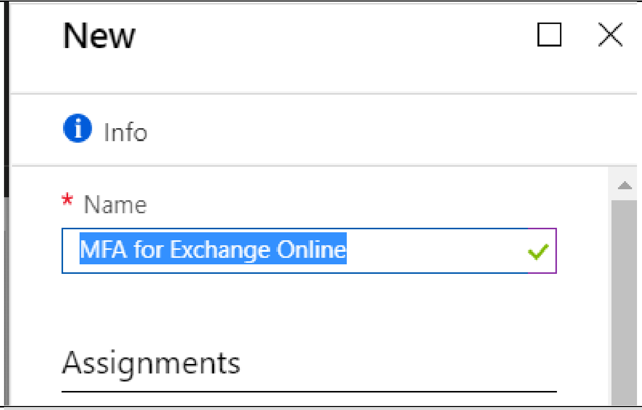
1. Go to Microsoft Intune → Conditional access and select New Policy



Interested in understanding the impact of the policies on a user sign-in? Che

POLICY NAME
Baseline policy: Require MFA for admins (Preview)

2. Give the policy a name: MFA for Exchange Online



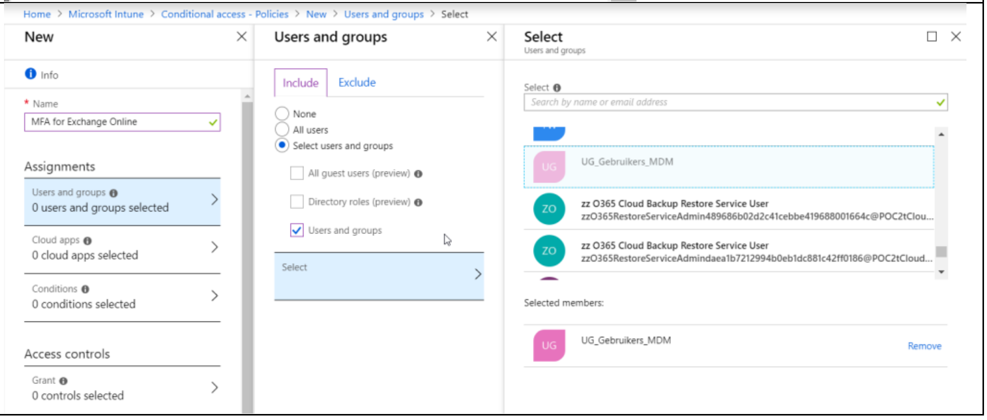
* Name: MFA for Exchange Online

3. Select Users and groups

4. Select: Select users and Groups

5. Check Users and groups

6. Select the group “UG_Gebruikers_MDM”



* Name: MFA for Exchange Online

Users and groups: 0 users and groups selected

Cloud apps: 0 cloud apps selected

Conditions: 0 conditions selected

Grant: 0 controls selected

○ None
○ All users
● Select users and groups

□ All guest users (preview)
□ Directory roles (preview)
☑ Users and groups

Select: Search by name or email address

UG_Gebruikers_MDM

zz O365 Cloud Backup Restore Service User
zzO365RestoreServiceAdmin489686b02d2c41cebbe419688001664c@POC2tClou...

zz O365 Cloud Backup Restore Service User
zzO365RestoreServiceAdmindaea1b7212994b0eb1dc881c42ff0186@POC2tCloud...

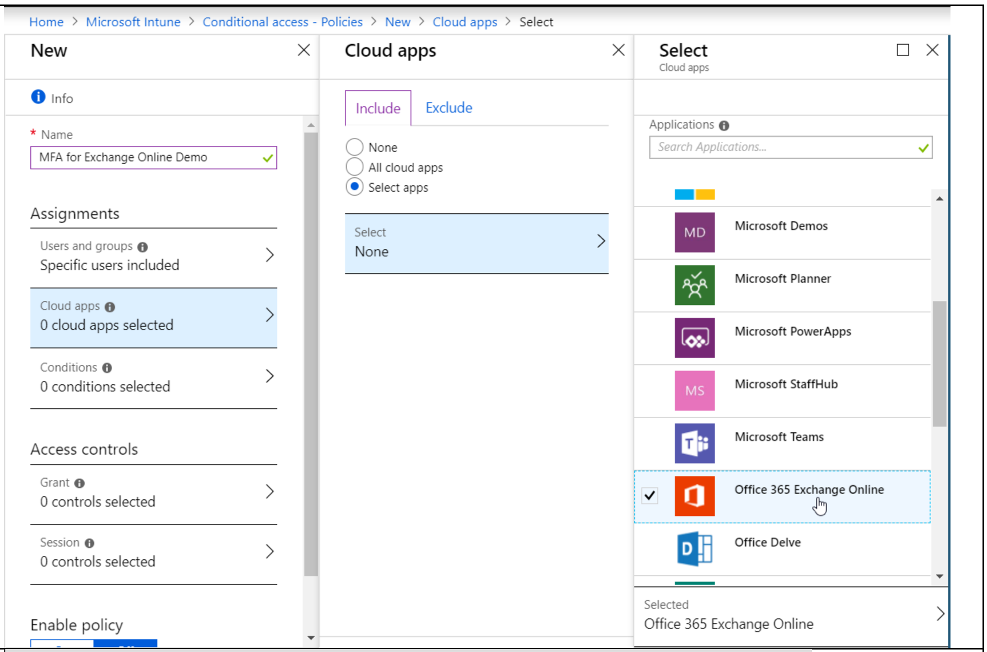
Selected members: UG_Gebruikers_MDM

7. Select Cloud apps

8. Check Selects apps

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

10. Choose Done



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

New

Info

* Name: MFA for Exchange Online Demo

Assignments

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

Access controls

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

Enable policy

Cloud apps

Include | Exclude

○ None
○ All cloud apps
● Select apps

Select: None

Select
Cloud apps

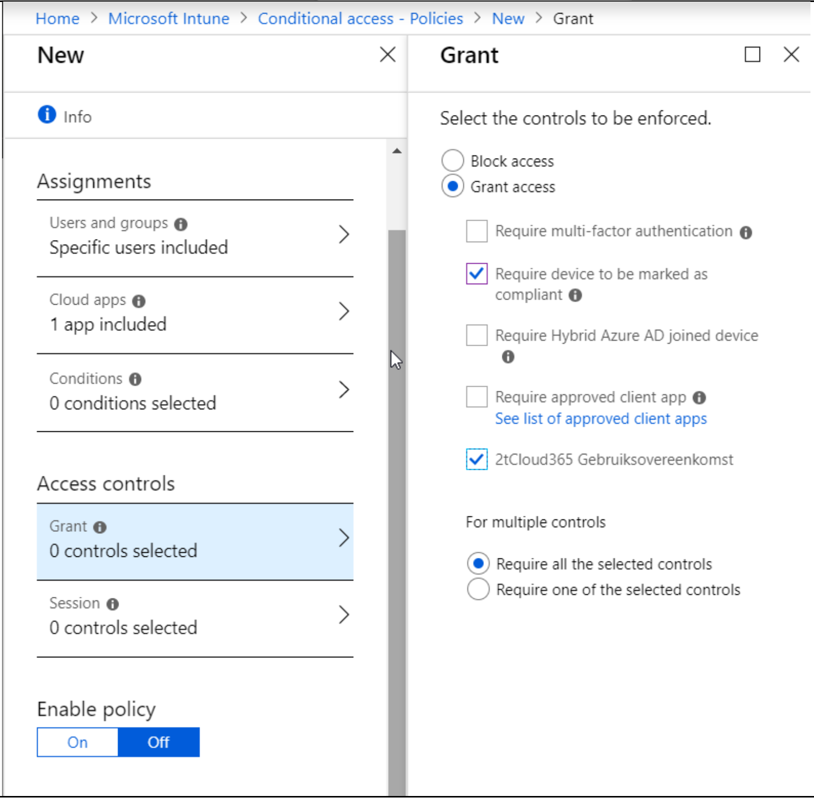
Applications: Search Applications...

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

Selected: Office 365 Exchange Online

11. Under Access controls select Grant

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



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

New

Info

Assignments

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

Access controls

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

Enable policy: On | **Off**

Grant

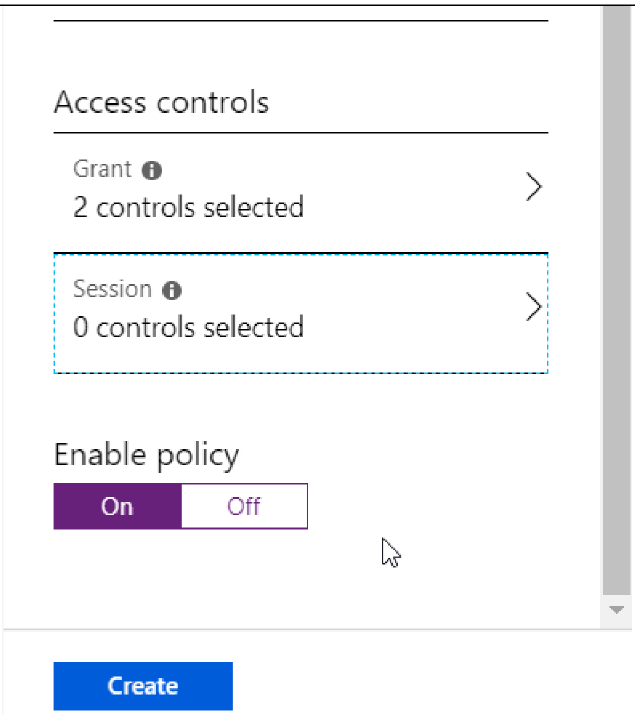
Select the controls to be enforced.

○ Block access
● Grant access

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

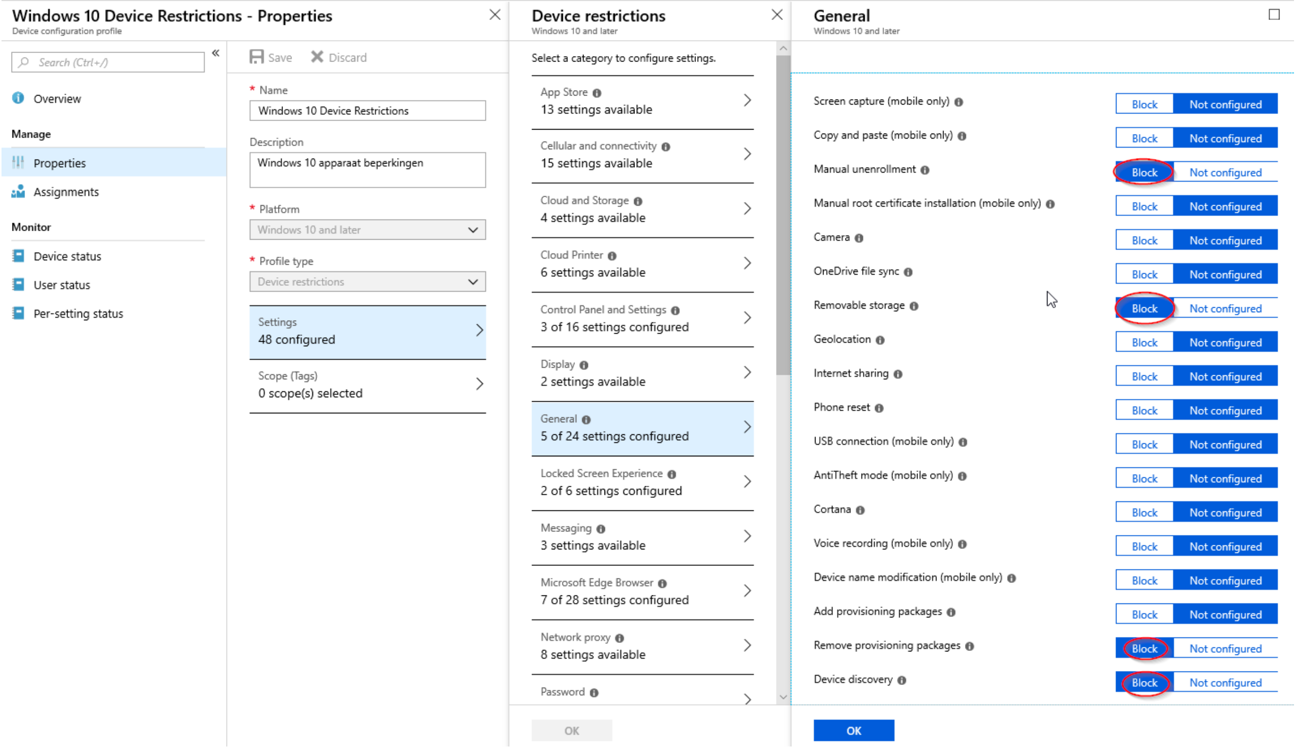
For multiple controls

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

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

Exercise 10a: Device Configuration - Windows Device Restrictions

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



Windows 10 Device Restrictions - Properties
Device configuration profile

Search (Ctrl+/)

- Overview

Manage
- Properties
- Assignments

Monitor
- Device status
- User status
- Per-setting status

Save | Discard

* Name: Windows 10 Device Restrictions

Description: Windows 10 apparaat beperkingen

* Platform: Windows 10 and later

* Profile type: Device restrictions

Settings: 48 configured

Scope (Tags): 0 scope(s) selected

Device restrictions
Windows 10 and later

Select a category to configure settings.

- App Store: 13 settings available
- Cellular and connectivity: 15 settings available
- Cloud and Storage: 4 settings available
- Cloud Printer: 6 settings available
- Control Panel and Settings: 3 of 16 settings configured
- Display: 2 settings available
- General: 5 of 24 settings configured
- Locked Screen Experience: 2 of 6 settings configured
- Messaging: 3 settings available
- Microsoft Edge Browser: 7 of 28 settings configured
- Network proxy: 8 settings available
- Password

OK

General
Windows 10 and later

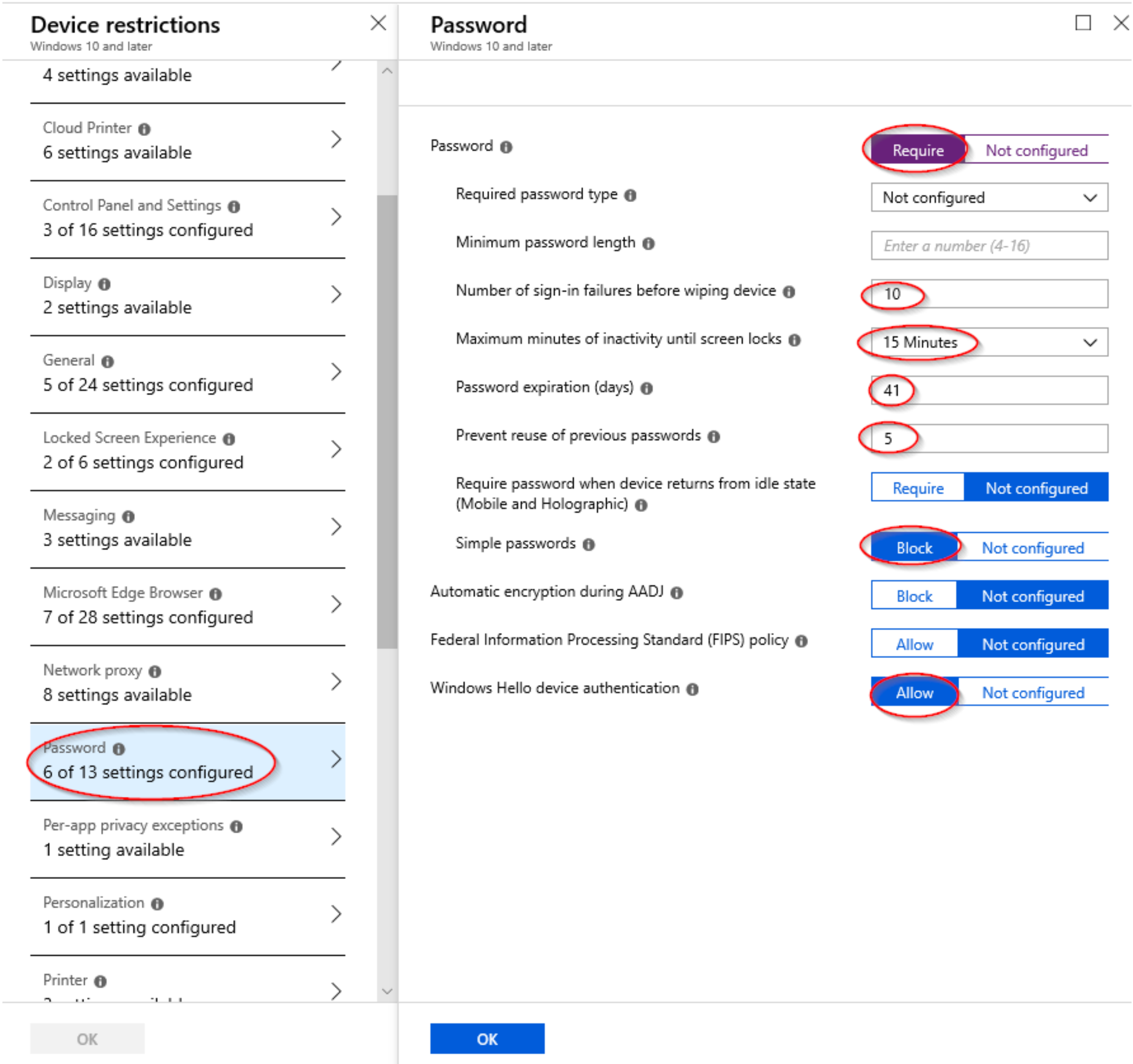
Screen capture (mobile only)	Block [✓ Not configured]
Copy and paste (mobile only)	Block [✓ Not configured]
Manual unenrollment	[✓ Block] Not configured
Manual root certificate installation (mobile only)	Block [✓ Not configured]
Camera	Block [✓ Not configured]
OneDrive file sync	Block [✓ Not configured]
Removable storage	[✓ Block] Not configured
Geolocation	Block [✓ Not configured]
Internet sharing	Block [✓ Not configured]
Phone reset	Block [✓ Not configured]
USB connection (mobile only)	Block [✓ Not configured]
AntiTheft mode (mobile only)	Block [✓ Not configured]
Cortana	Block [✓ Not configured]
Voice recording (mobile only)	Block [✓ Not configured]
Device name modification (mobile only)	Block [✓ Not configured]
Add provisioning packages	Block [✓ Not configured]
Remove provisioning packages	[✓ Block] Not configured
Device discovery	[✓ Block] Not configured

OK

2. Configure the settings >

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

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



Device restrictions
Windows 10 and later

4 settings available

Cloud Printer
6 settings available

Control Panel and Settings
3 of 16 settings configured

Display
2 settings available

General
5 of 24 settings configured

Locked Screen Experience
2 of 6 settings configured

Messaging
3 settings available

Microsoft Edge Browser
7 of 28 settings configured

Network proxy
8 settings available

Password
6 of 13 settings configured

Per-app privacy exceptions
1 setting available

Personalization
1 of 1 setting configured

Printer

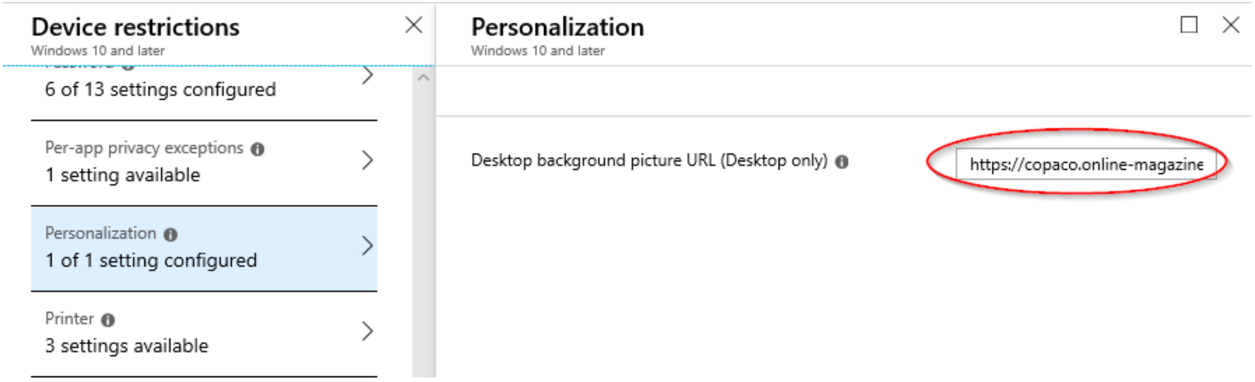
OK

Password
Windows 10 and later

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

OK

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



Device restrictions
Windows 10 and later

6 of 13 settings configured

Per-app privacy exceptions
1 setting available

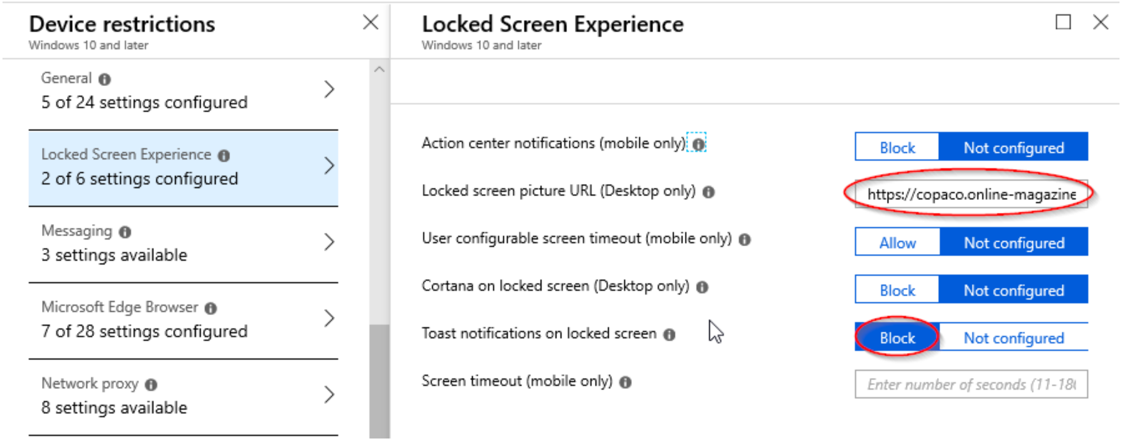
Personalization
1 of 1 setting configured

Printer
3 settings available

Personalization
Windows 10 and later

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

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



Device restrictions
Windows 10 and later

General
5 of 24 settings configured

Locked Screen Experience
2 of 6 settings configured

Messaging
3 settings available

Microsoft Edge Browser
7 of 28 settings configured

Network proxy
8 settings available

Locked Screen Experience
Windows 10 and later

Action center notifications (mobile only) — Block [✓ Not configured]

Locked screen picture URL (Desktop only) — https://copaco.online-magazine

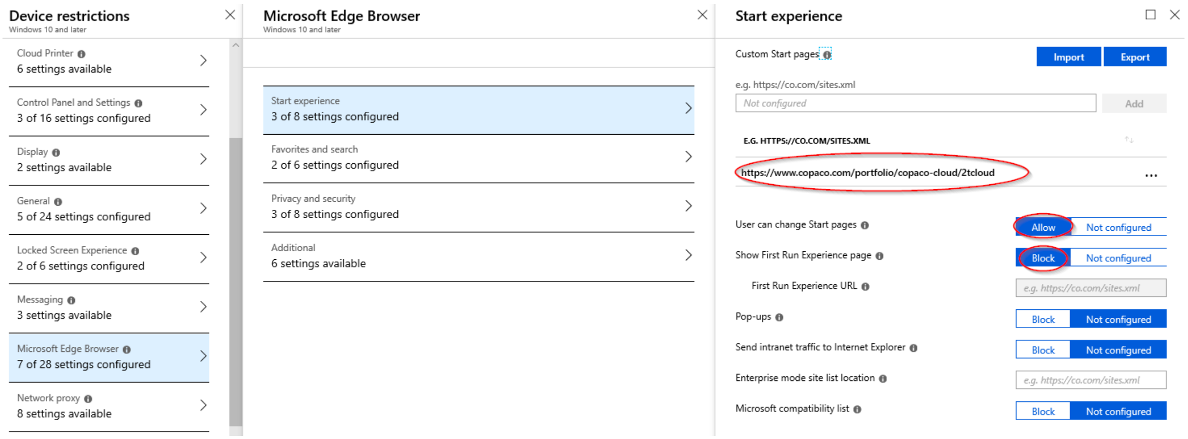
User configurable screen timeout (mobile only) — Allow [✓ Not configured]

Cortana on locked screen (Desktop only) — Block [✓ Not configured]

Toast notifications on locked screen — [✓ Block] Not configured

Screen timeout (mobile only) — Enter number of seconds (11-18(

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



Device restrictions
Windows 10 and later

Cloud Printer
6 settings available

Control Panel and Settings
3 of 16 settings configured

Display
2 settings available

General
5 of 24 settings configured

Locked Screen Experience
2 of 6 settings configured

Messaging
3 settings available

Microsoft Edge Browser
7 of 28 settings configured

Network proxy
8 settings available

Microsoft Edge Browser
Windows 10 and later

Start experience
3 of 8 settings configured

Favorites and search
2 of 6 settings configured

Privacy and security
3 of 8 settings configured

Additional
6 settings available

Start experience

Custom Start pages — Import | Export

e.g. https://co.com/sites.xml
Not configured — Add

E.G. HTTPS://CO.COM/SITES.XML
https://www.copaco.com/portfolio/copaco-cloud/2tcloud ...

User can change Start pages — [✓ Allow] Not configured

Show First Run Experience page — [✓ Block] Not configured

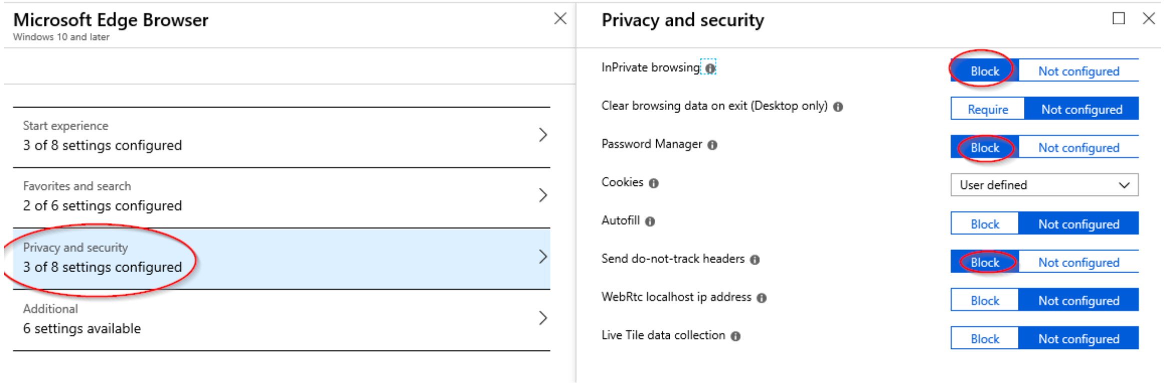
First Run Experience URL — e.g. https://co.com/sites.xml

Pop-ups — Block [✓ Not configured]

Send intranet traffic to Internet Explorer — Block [✓ Not configured]

Enterprise mode site list location — e.g. https://co.com/sites.xml

Microsoft compatibility list — Block [✓ Not configured]



Microsoft Edge Browser
Windows 10 and later

Start experience
3 of 8 settings configured

Favorites and search
2 of 6 settings configured

Privacy and security
3 of 8 settings configured

Additional
6 settings available

Privacy and security

InPrivate browsing — [✓ Block] Not configured

Clear browsing data on exit (Desktop only) — Require [✓ Not configured]

Password Manager — [✓ Block] Not configured

Cookies — User defined

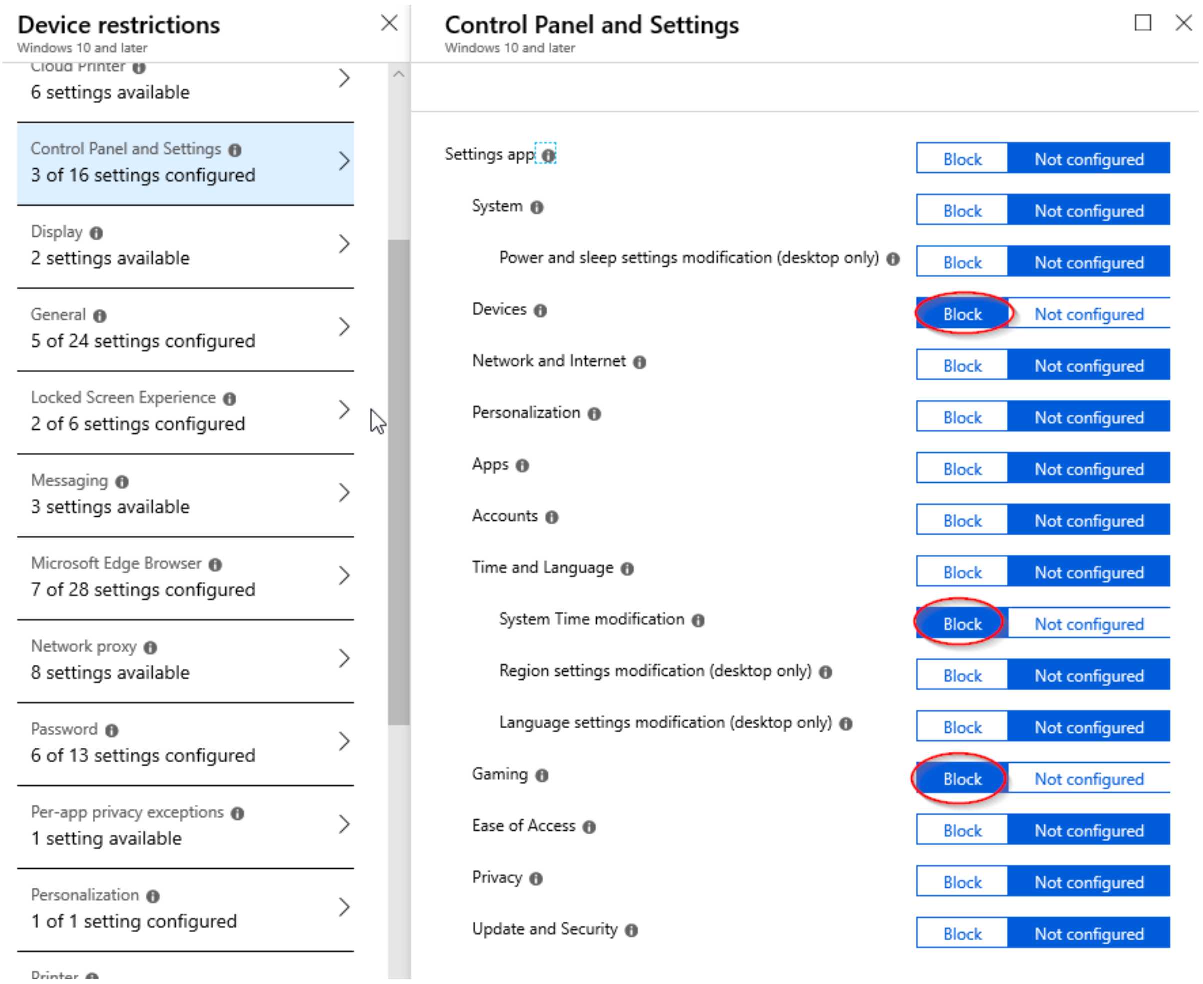
Autofill — Block [✓ Not configured]

Send do-not-track headers — [✓ Block] Not configured

WebRtc localhost ip address — Block [✓ Not configured]

Live Tile data collection — Block [✓ Not configured]

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



Device restrictions
Windows 10 and later

Cloud Printer
6 settings available

Control Panel and Settings
3 of 16 settings configured

Display
2 settings available

General
5 of 24 settings configured

Locked Screen Experience
2 of 6 settings configured

Messaging
3 settings available

Microsoft Edge Browser
7 of 28 settings configured

Network proxy
8 settings available

Password
6 of 13 settings configured

Per-app privacy exceptions
1 setting available

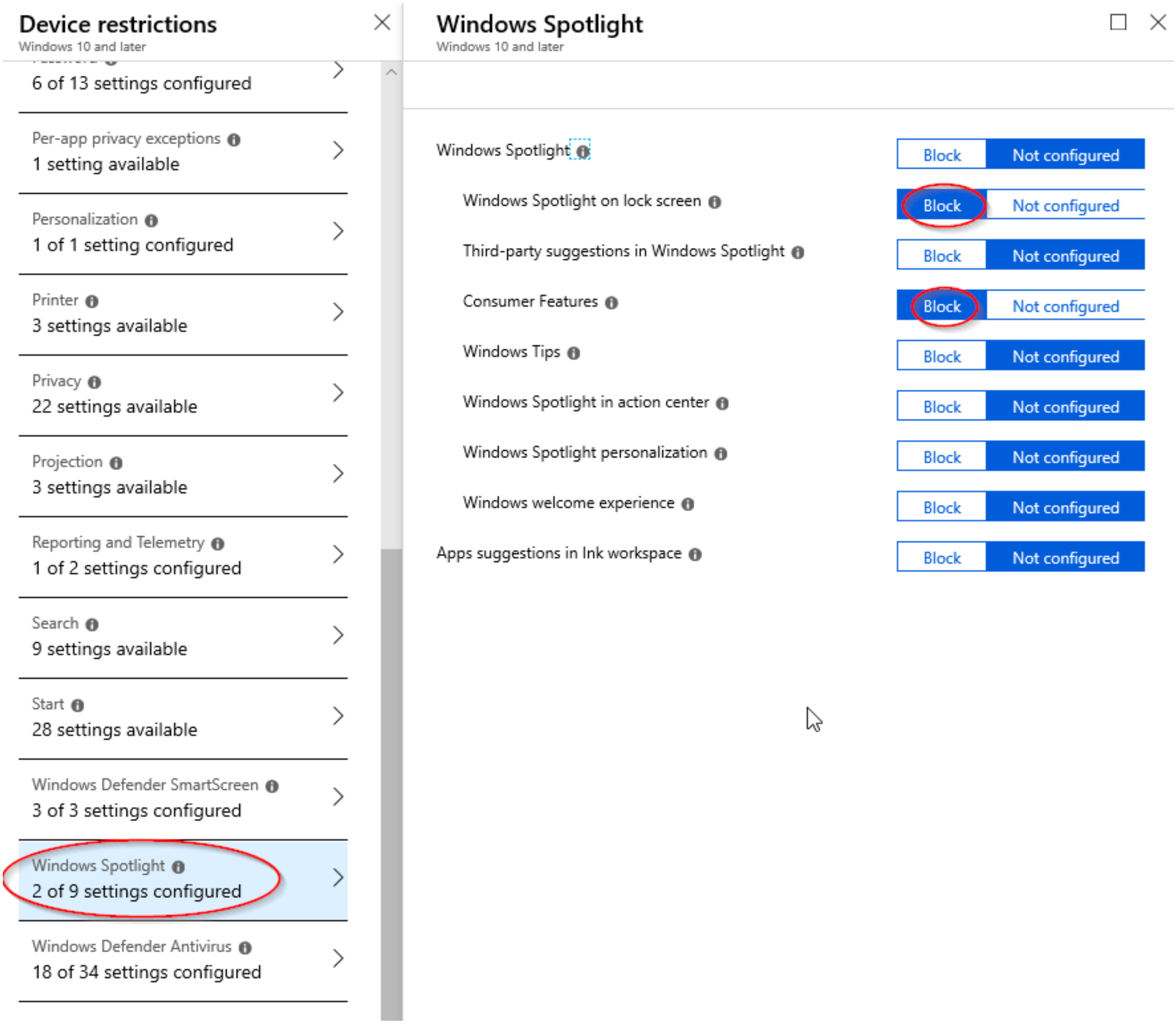
Personalization
1 of 1 setting configured

Printer

Control Panel and Settings
Windows 10 and later

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

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



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

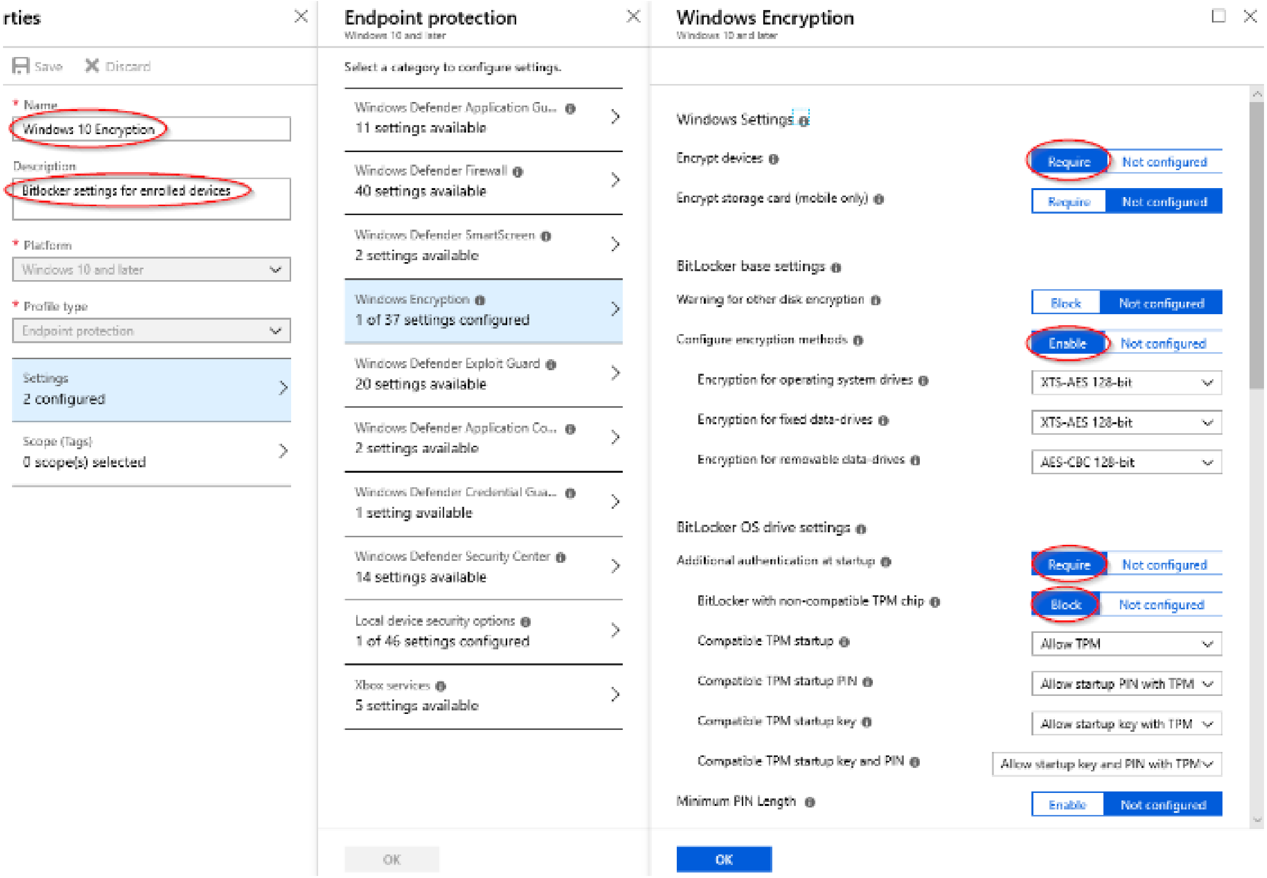
Windows Spotlight
Windows 10 and later

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

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

Exercise 10b: Device Configuration - Windows Device Configuration

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



rties

* Name: Windows 10 Encryption

Description: Bitlocker settings for enrolled devices

* Platform: Windows 10 and later

* Profile type: Endpoint protection

Settings: 2 configured

Scope (Tags): 0 scope(s) selected

Endpoint protection
Windows 10 and later

Select a category to configure settings.

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

Windows Encryption
Windows 10 and later

Windows Settings

Encrypt devices: [✓ Require] Not configured

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

BitLocker base settings

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

Configure encryption methods: [✓ Enable] Not configured

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

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

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

BitLocker OS drive settings

Additional authentication at startup: [✓ Require] Not configured

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

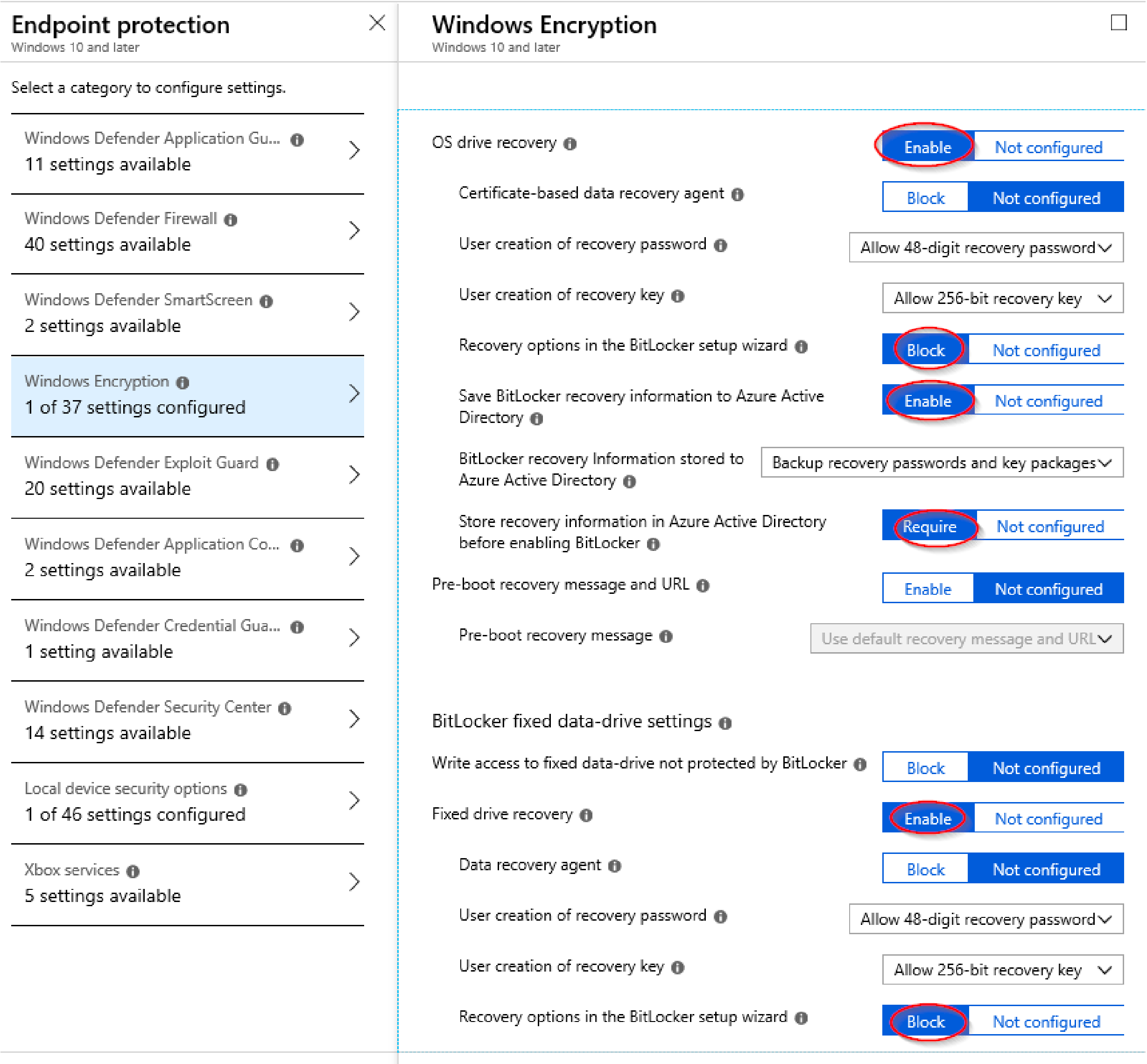
Compatible TPM startup: Allow TPM

Compatible TPM startup PIN: Allow startup PIN with TPM

Compatible TPM startup key: Allow startup key with TPM

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

Minimum PIN Length: Enable [✓ Not configured]



Endpoint protection
Windows 10 and later

Select a category to configure settings.

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

Windows Encryption
Windows 10 and later

OS drive recovery	[✓ Enable] Not configured
Certificate-based data recovery agent	Block [✓ Not configured]
User creation of recovery password	Allow 48-digit recovery password
User creation of recovery key	Allow 256-bit recovery key
Recovery options in the BitLocker setup wizard	[✓ Block] Not configured
Save BitLocker recovery information to Azure Active Directory	[✓ Enable] Not configured
BitLocker recovery Information stored to Azure Active Directory	Backup recovery passwords and key packages
Store recovery information in Azure Active Directory before enabling BitLocker	[✓ Require] Not configured
Pre-boot recovery message and URL	Enable [✓ Not configured]
Pre-boot recovery message	Use default recovery message and URL

BitLocker fixed data-drive settings

Write access to fixed data-drive not protected by BitLocker	Block [✓ Not configured]
Fixed drive recovery	[✓ Enable] Not configured
Data recovery agent	Block [✓ Not configured]
User creation of recovery password	Allow 48-digit recovery password
User creation of recovery key	Allow 256-bit recovery key
Recovery options in the BitLocker setup wizard	[✓ Block] Not configured

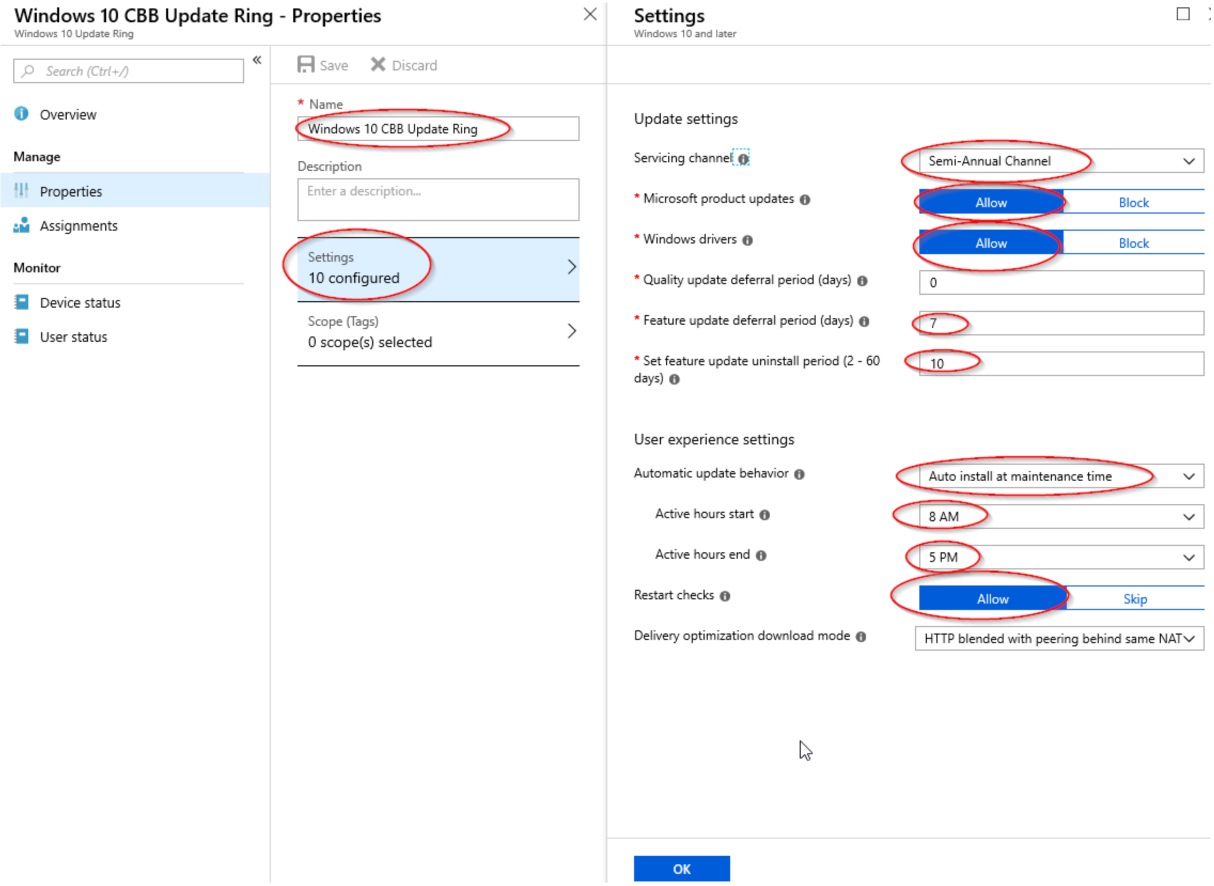
Configure the settings > Click **Ok**

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

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

Exercise 11: Windows 10 Update Rings

1. Go to **Intune -> Software Updates -> Windows 10 Update Rings**
2. Click “Create”
3. Configure the settings -> Click **Settings**
4. Configure settings as showed on the screenshot



* Name: Windows 10 CBB Update Ring

Description: Enter a description...

Settings: 10 configured

Scope (Tags): 0 scope(s) selected

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

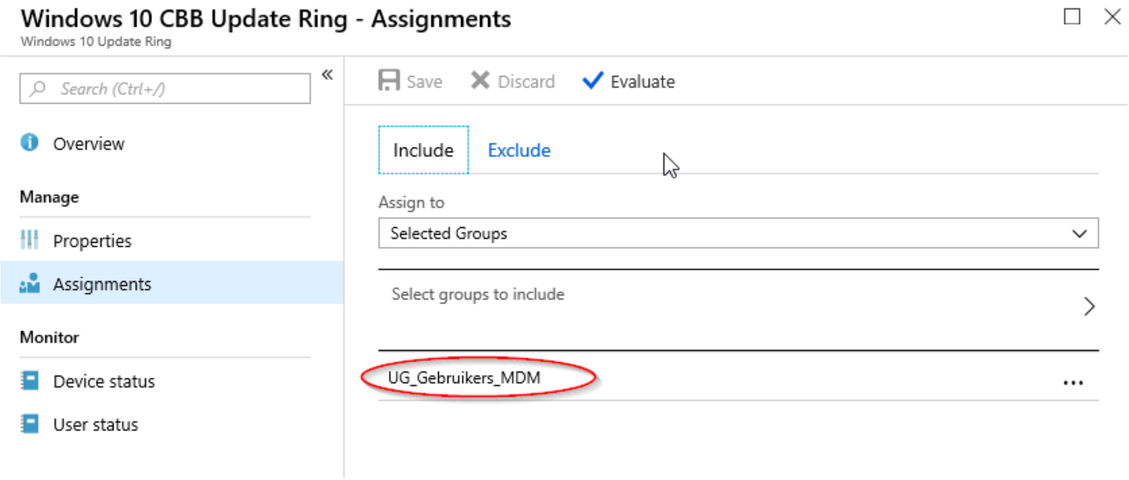
Active hours start: 8 AM

Active hours end: 5 PM

Restart checks: Allow | Skip

Delivery optimization download mode: HTTP blended with peering behind same NAT

5. Assign the Windows 10 Update Ring to Group “UG_Gebruikers_MDM”



Windows 10 CBB Update Ring - Assignments

Windows 10 Update Ring

Assign to: Selected Groups

Select groups to include

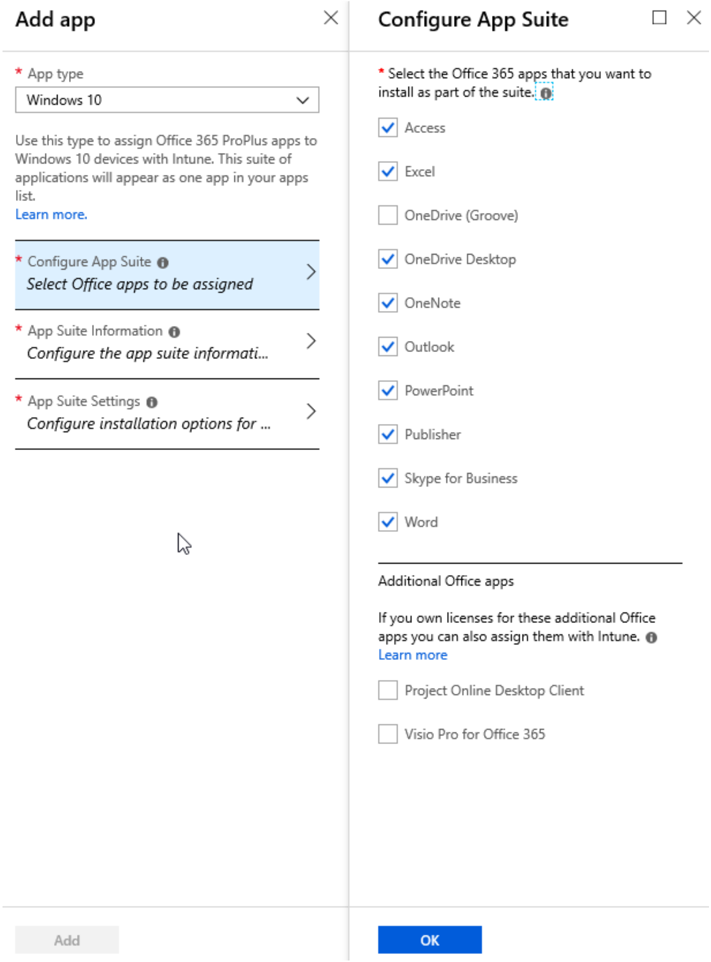
UG_Gebruikers_MDM

Exercise 12: Office ProPlus Deployment via Intune

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

Try to create the Office365 Proplus App and assign it to group **UG_Gebruikers_MDM**

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



Add app

* App type

Windows 10

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

* Configure App Suite
Select Office apps to be assigned

* App Suite Information
Configure the app suite informati...

* App Suite Settings
Configure installation options for ...

Add

Configure App Suite

* Select the Office 365 apps that you want to install as part of the suite.

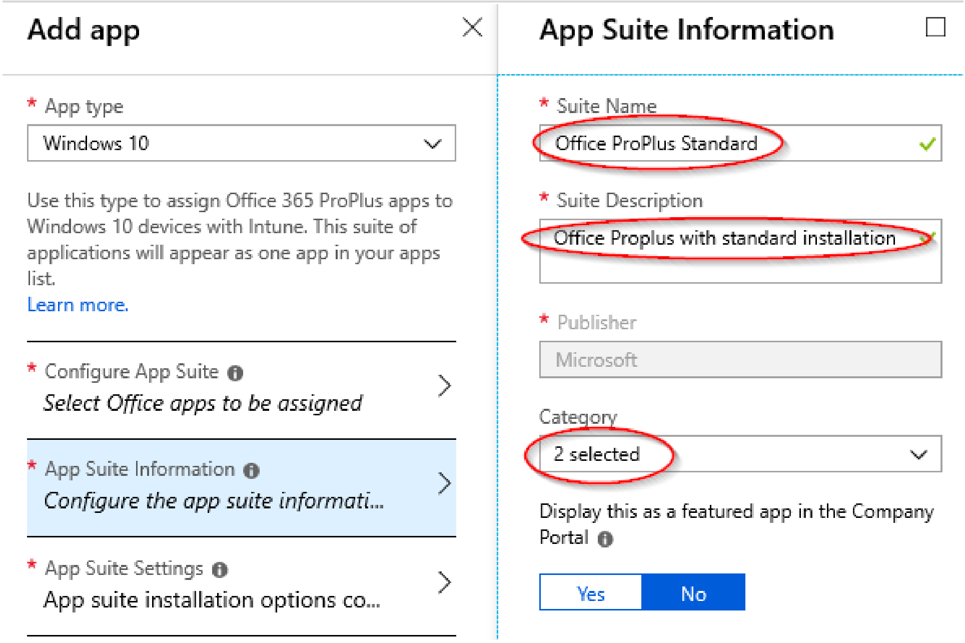
☑ Access
☑ Excel
☐ OneDrive (Groove)
☑ OneDrive Desktop
☑ OneNote
☑ Outlook
☑ PowerPoint
☑ Publisher
☑ Skype for Business
☑ Word

Additional Office apps

If you own licenses for these additional Office apps you can also assign them with Intune.
Learn more

☐ Project Online Desktop Client
☐ Visio Pro for Office 365

OK



Add app

* App type

Windows 10

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

* Configure App Suite
Select Office apps to be assigned

* App Suite Information
Configure the app suite informati...

* App Suite Settings
App suite installation options co...

App Suite Information

* Suite Name: Office ProPlus Standard ✓

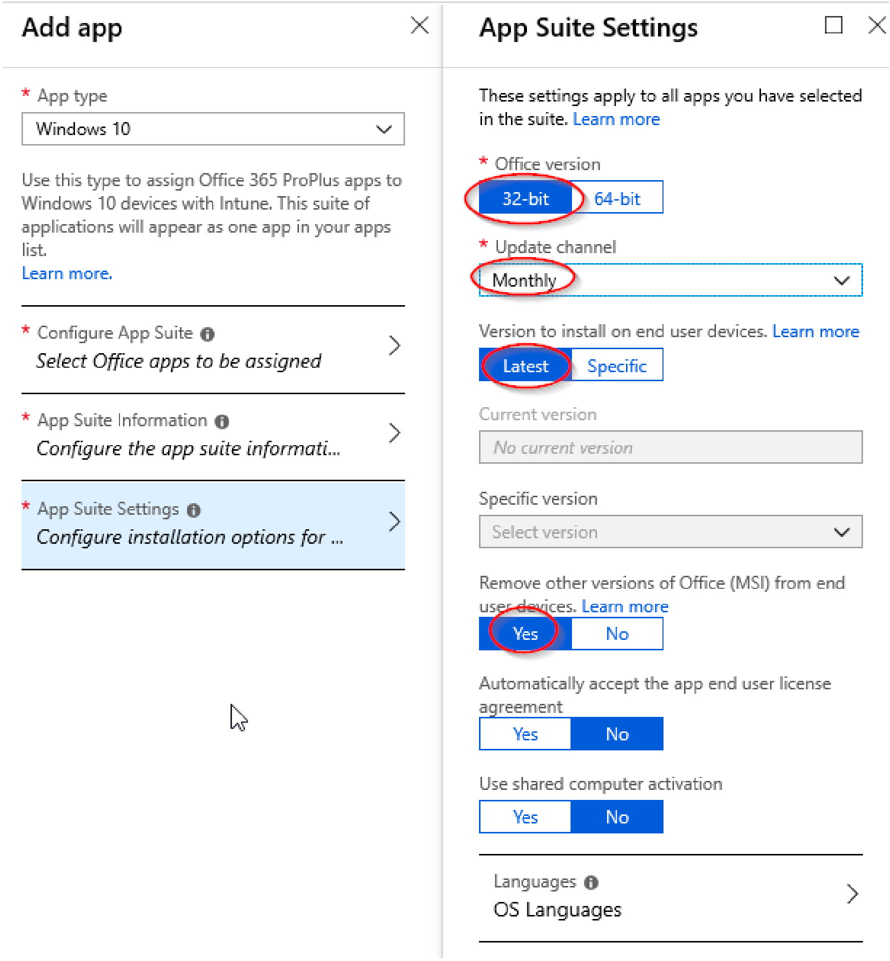
* Suite Description: Office Proplus with standard installation ✓

* Publisher: Microsoft

Category: 2 selected

Display this as a featured app in the Company Portal

Yes [✓ No]



Add app

* App type

Windows 10

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

* Configure App Suite
Select Office apps to be assigned

* App Suite Information
Configure the app suite informati...

* App Suite Settings
Configure installation options for ...

App Suite Settings

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

* Office version: [✓ 32-bit] 64-bit

* Update channel: Monthly

Version to install on end user devices. Learn more

[✓ Latest] Specific

Current version: *No current version*

Specific version: Select version

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

[✓ Yes] No

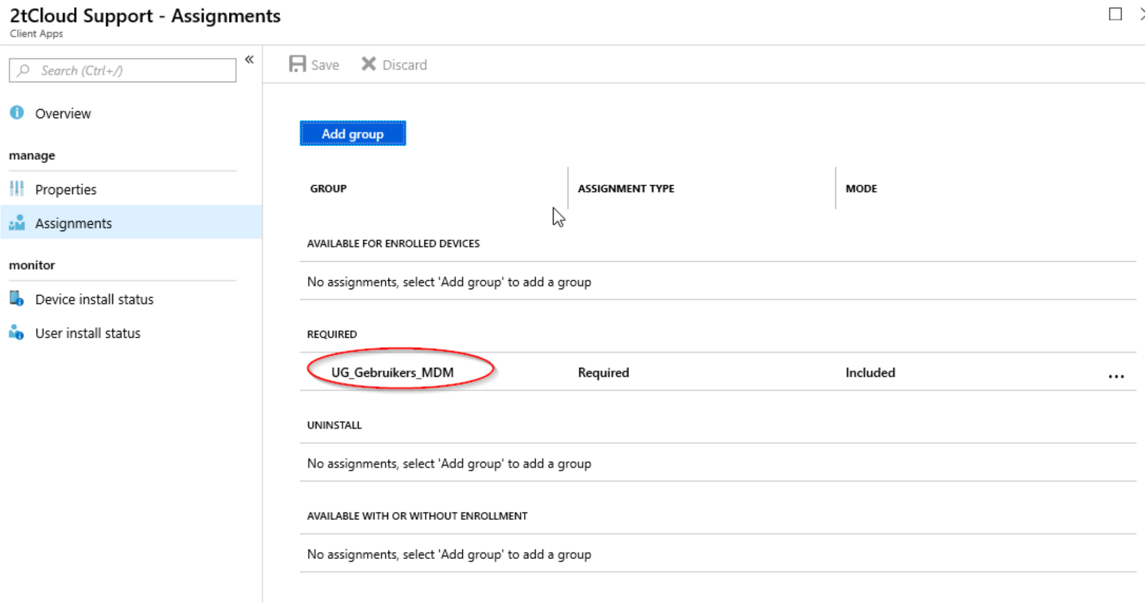
Automatically accept the app end user license agreement

Yes [✓ No]

Use shared computer activation

Yes [✓ No]

Languages
OS Languages



2tCloud Support - Assignments

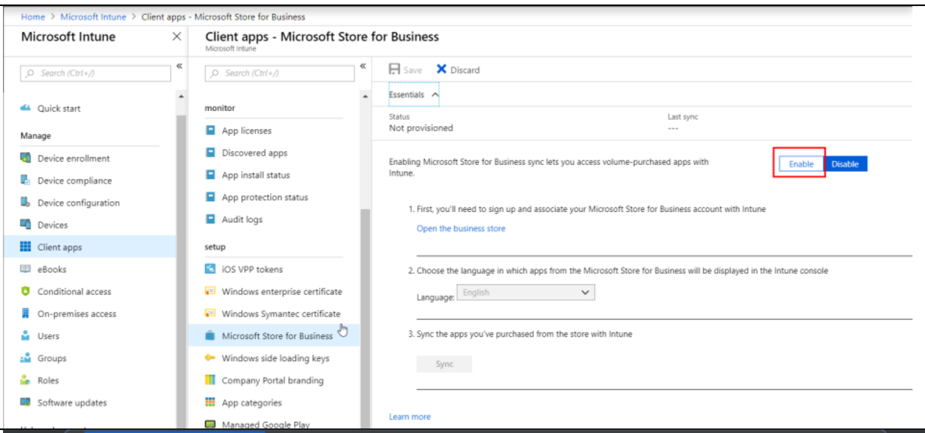
Client Apps

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

Exercise 13: Windows Store for Business

Go to Microsoft Intune → Client Apps → Microsoft store for Business

1. There you select Enable and press Save



Status: Not provisioned

Last sync: ---

Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune.

1. First, you'll need to sign up and associate your Microsoft Store for Business account with Intune

   Open the business store

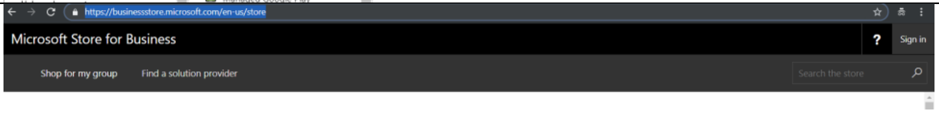
2. Choose the language in which apps from the Microsoft Store for Business will be displayed in the Intune console

   Language: English

3. Sync the apps you've purchased from the store with Intune

2. After that you can select the link open Open the business store

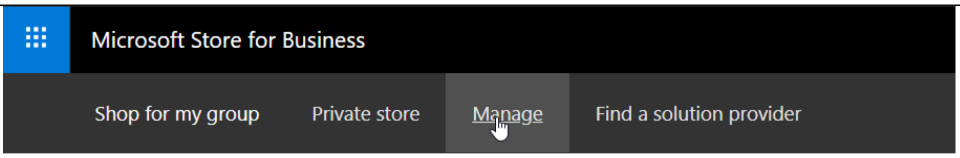
3. Sign in with your AAD account



https://businessstore.microsoft.com/en-us/store

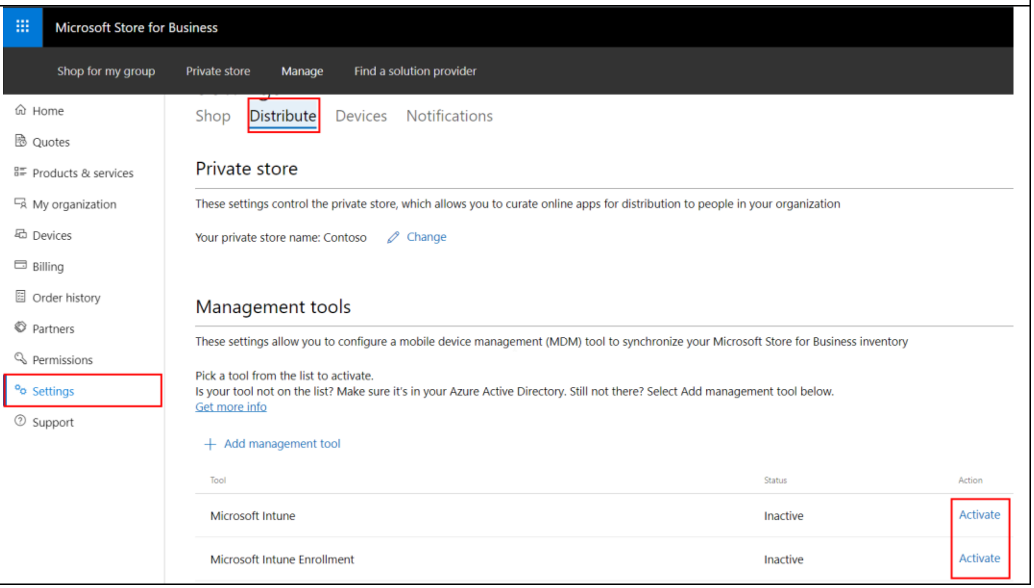
4. Once your signed in select manage

5. Accept any terms and license agreements



Go to settings → Distribute

6. Activate Microsoft Intune and Microsoft Intune Enrollment



Private store

These settings control the private store, which allows you to curate online apps for distribution to people in your organization

Your private store name: Contoso   Change

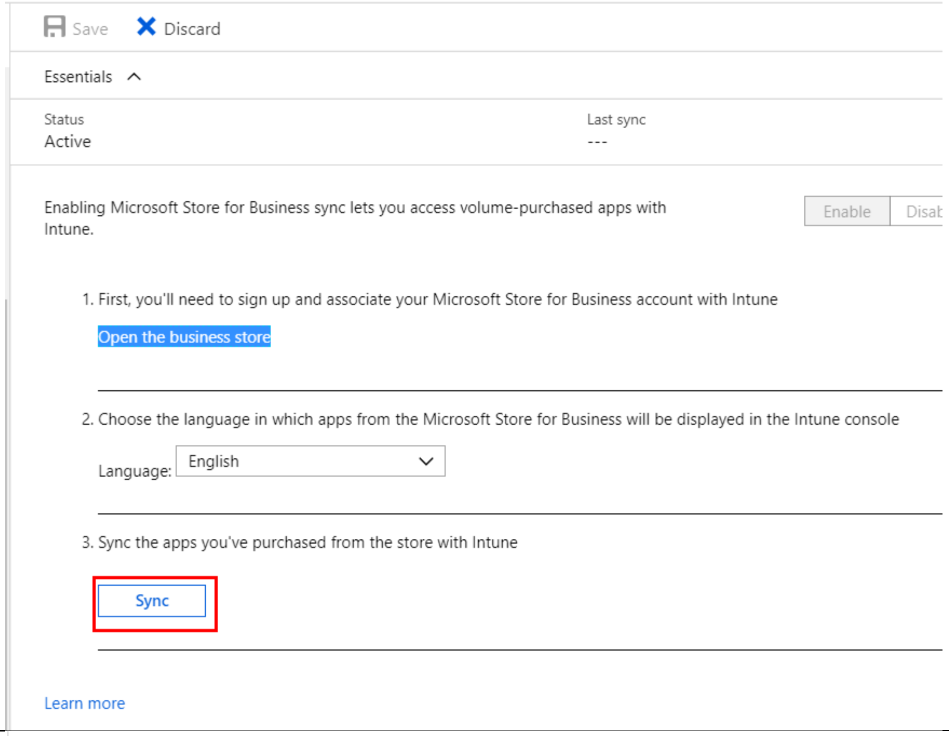
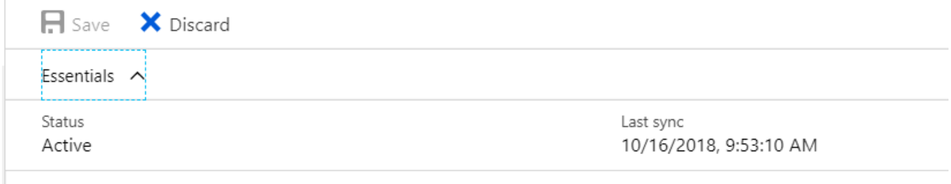
Management tools

These settings allow you to configure a mobile device management (MDM) tool to synchronize your Microsoft Store for Business inventory

Pick a tool from the list to activate.
Is your tool not on the list? Make sure it's in your Azure Active Directory. Still not there? Select Add management tool below.
Get more info

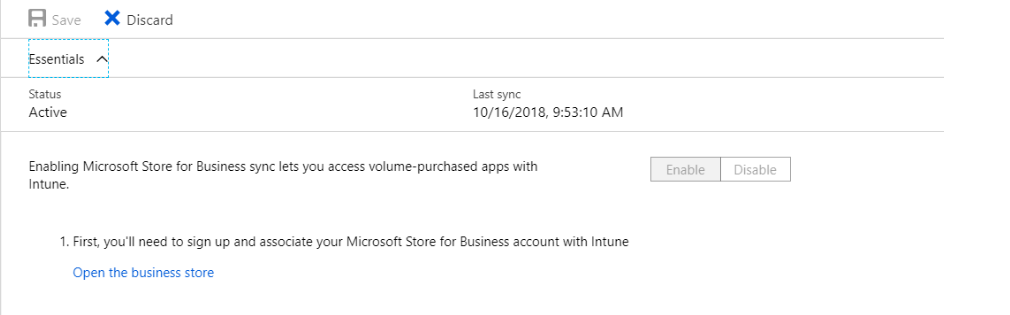
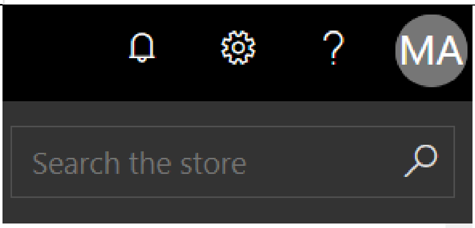
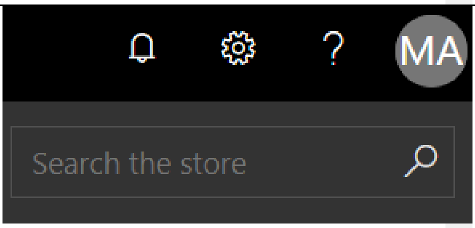
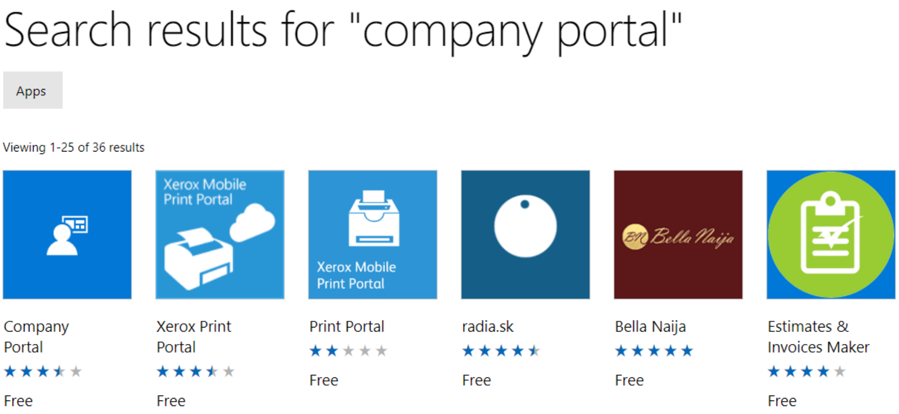
+ Add management tool

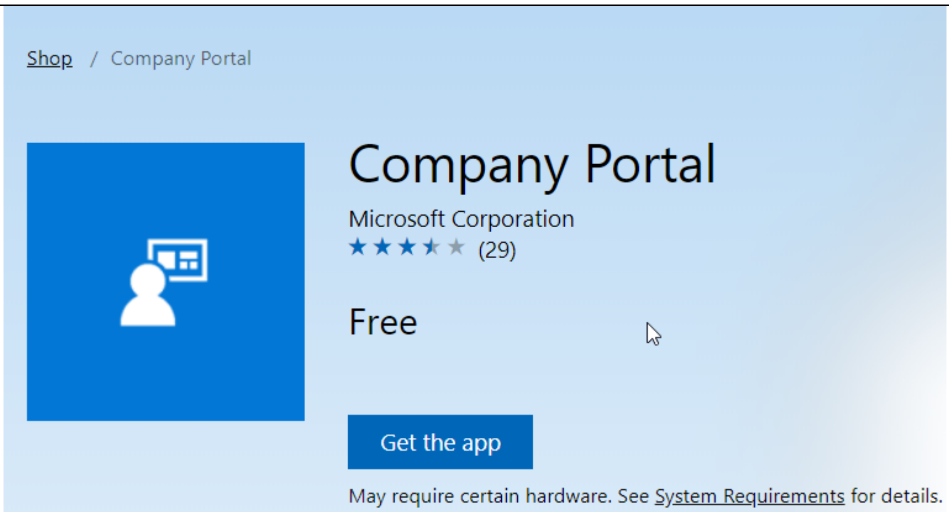
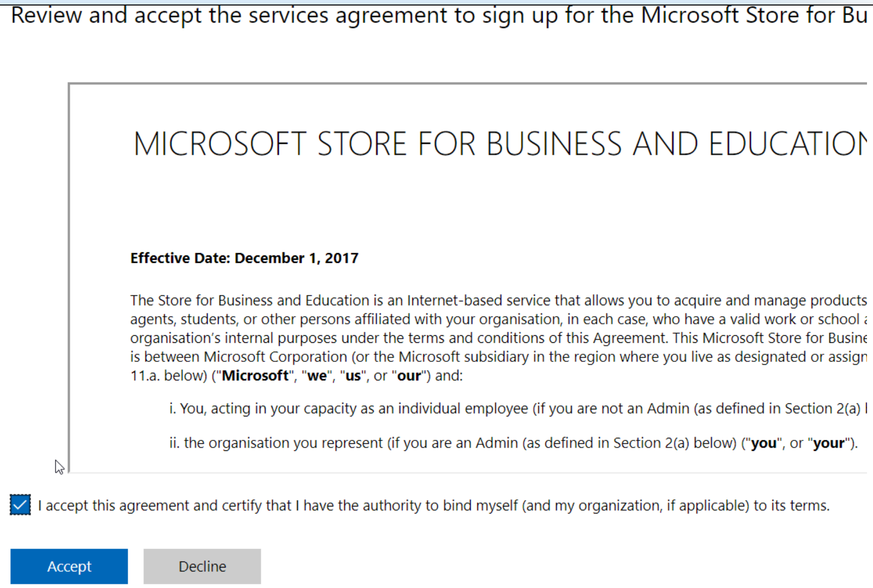
Tool	Status	Action
Microsoft Intune	Inactive	Activate
Microsoft Intune Enrollment	Inactive	Activate

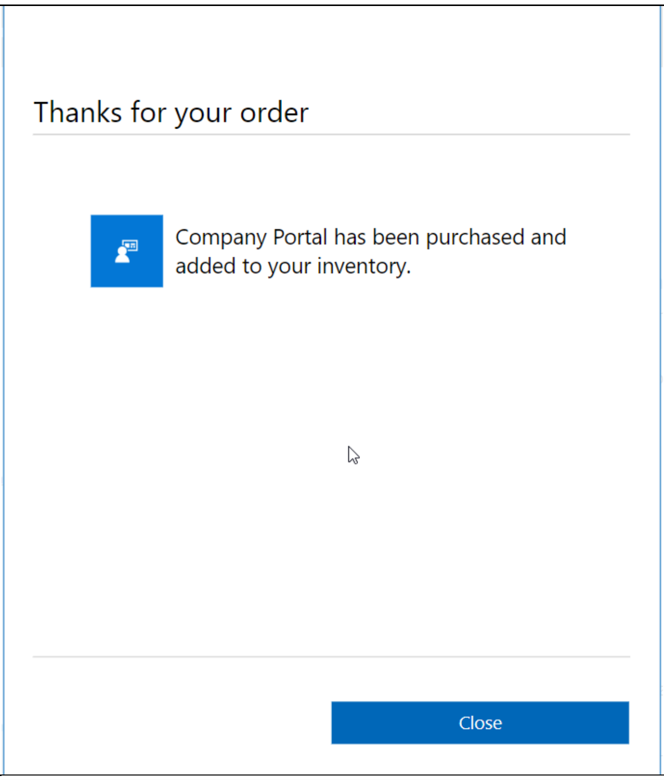
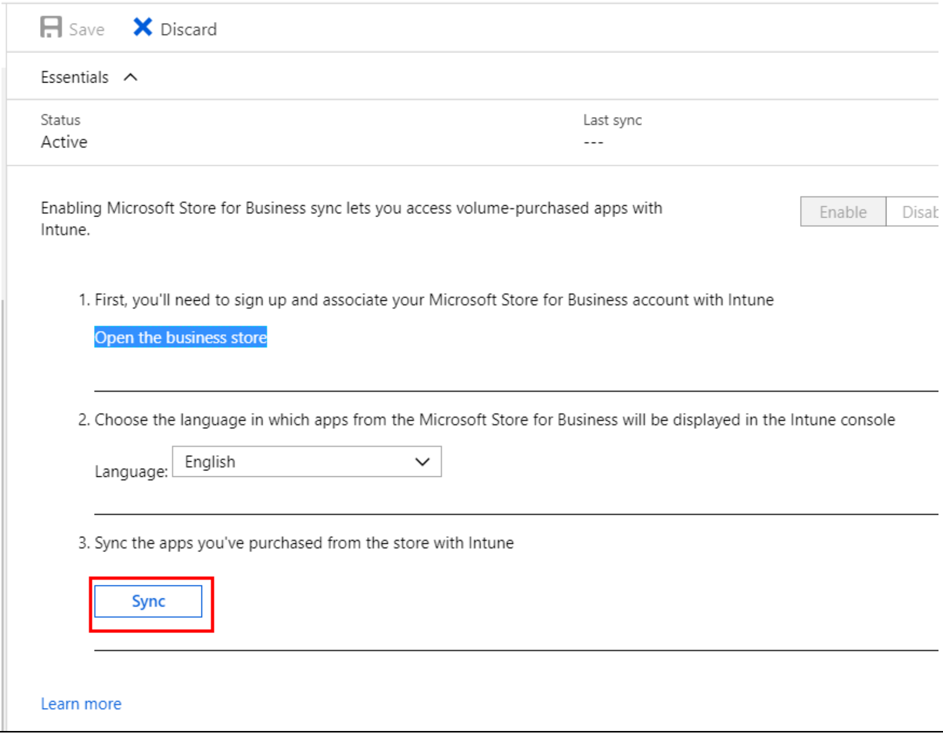
7. Go back to the Intune Portal and Select Sync	 Save Discard Essentials Status: Active Last sync: --- Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. Enable Disat 1. First, you'll need to sign up and associate your Microsoft Store for Business account with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

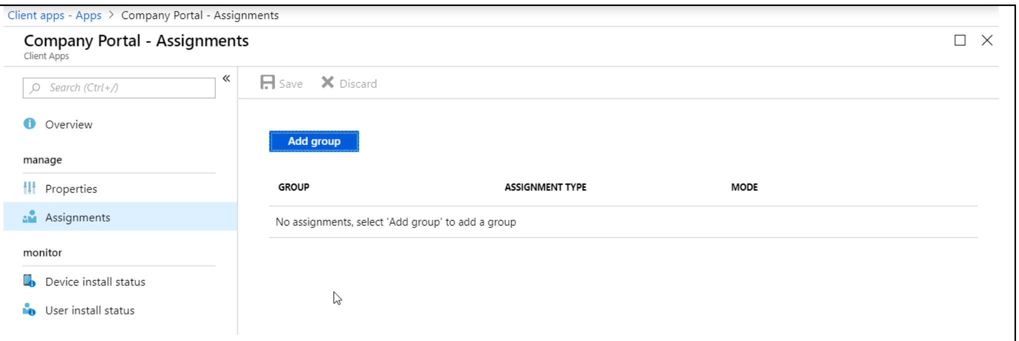
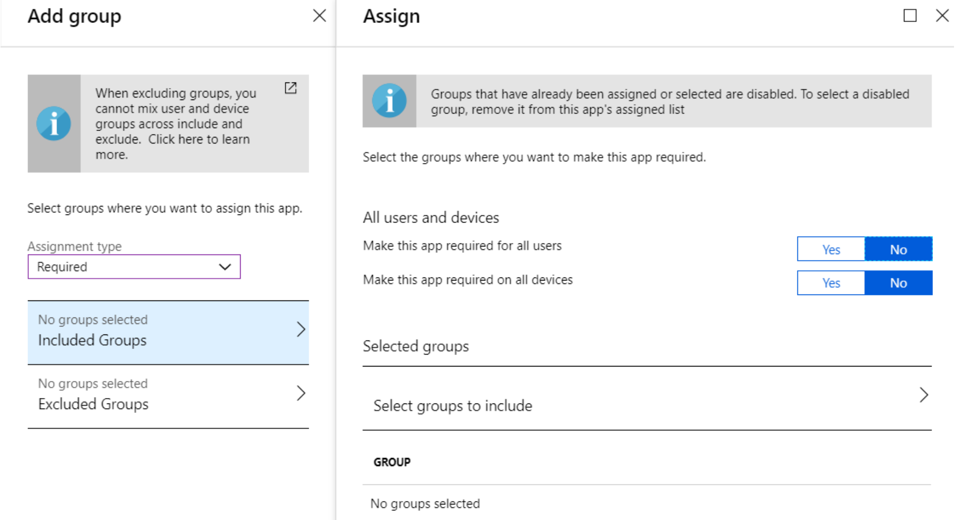
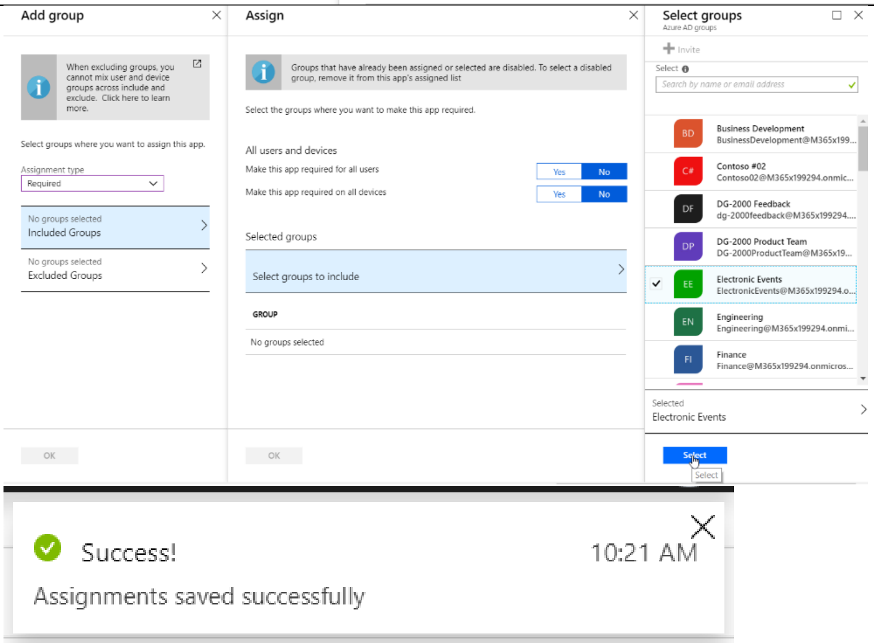
Exercise 14: Company portal

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

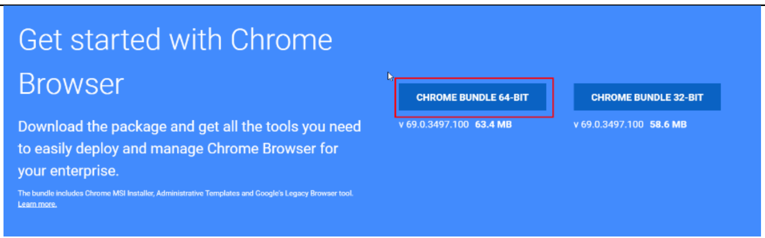
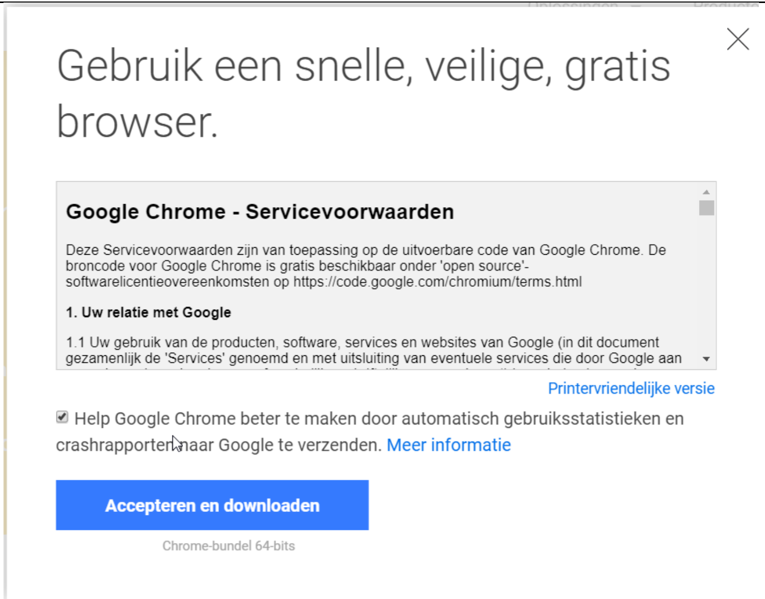
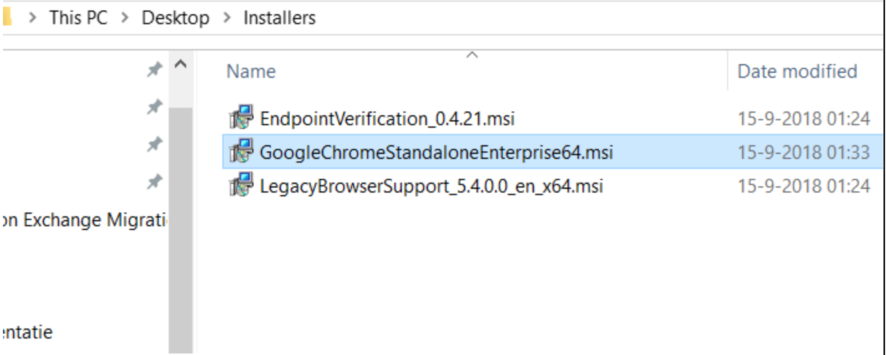
Go to Microsoft Intune → Client Apps → Microsoft store for Business 1. Select open the business store	 Status Active Last sync 10/16/2018, 9:53:10 AM Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. 1. First, you'll need to sign up and associate your Microsoft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

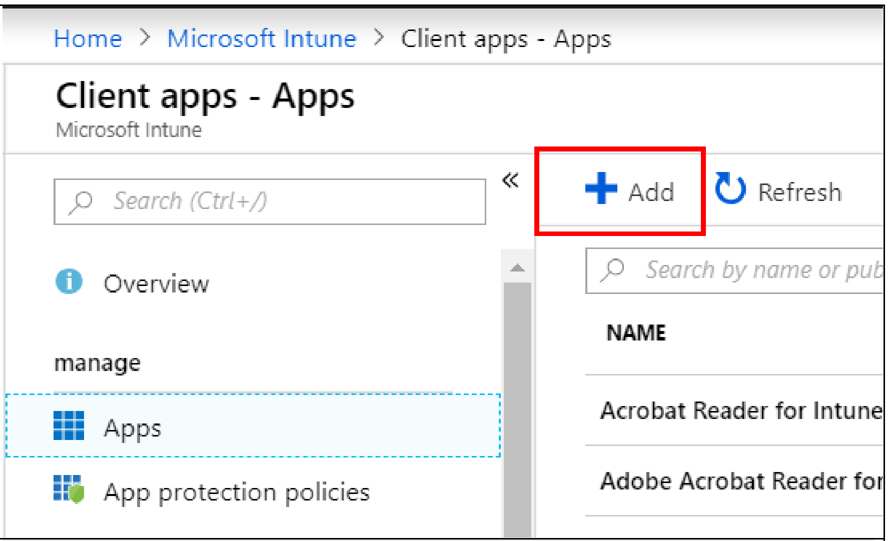
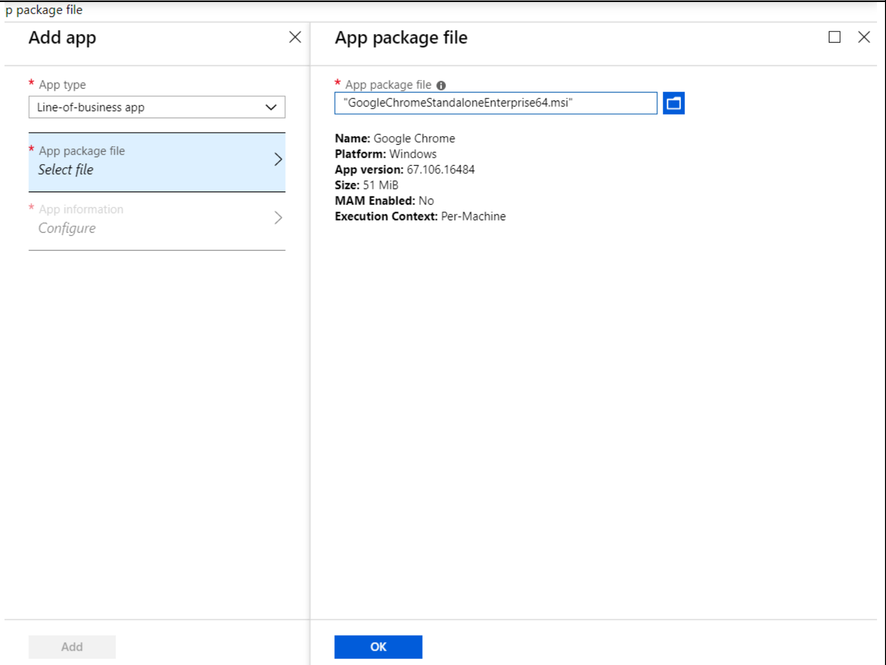
5. Select Get the app	 Shop / Company Portal Company Portal Microsoft Corporation ★★★★☆ (29) Free Get the app May require certain hardware. See System Requirements for details.
6. Accept the agreement	 Review and accept the services agreement to sign up for the Microsoft Store for Bu MICROSOFT STORE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

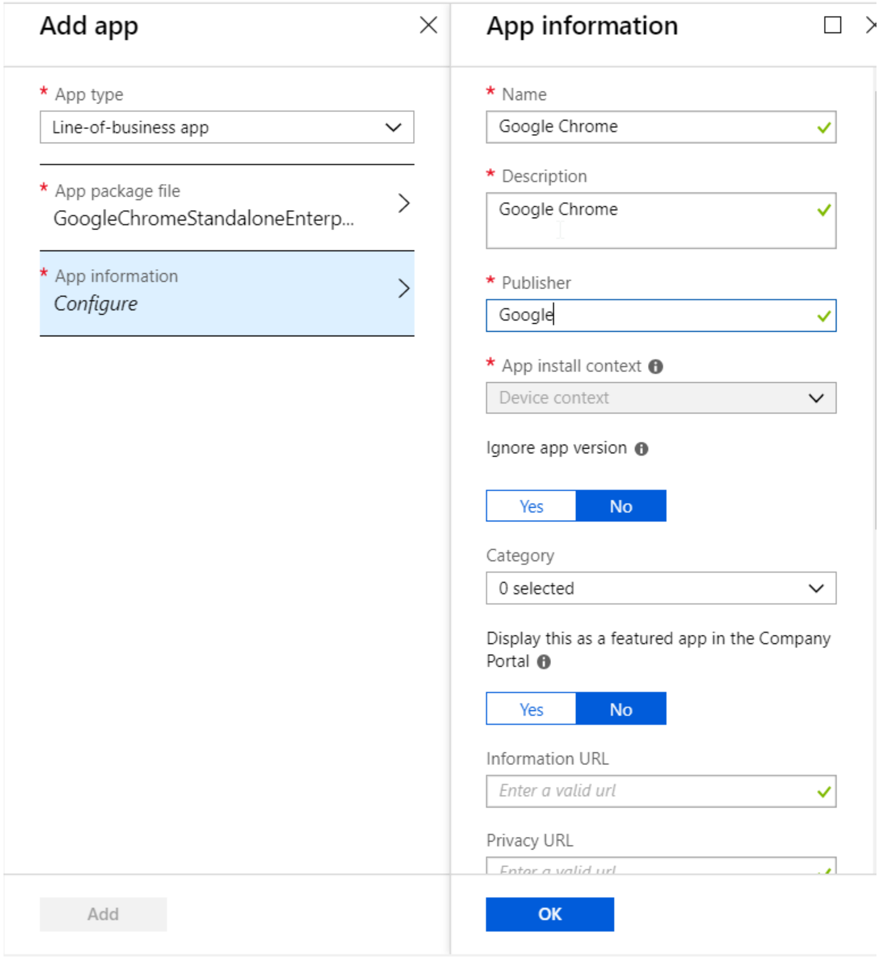
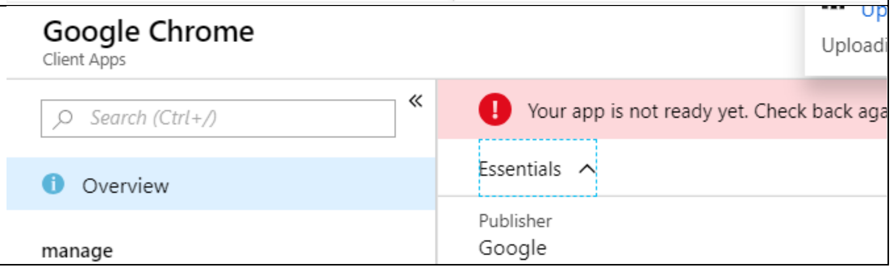
7. After that the app is added	 Thanks for your order Company Portal has been purchased and added to your inventory.
8. Go back to the Intune Portal and Select Sync	 Status: Active Last sync: --- Enabling Microsoft Store for Business sync lets you access volume-purchased apps with Intune. 1. First, you'll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

After the sync is completed go to Microsoft Intune → Client apps – Apps There you should find The company portal. Note that the Type is Microsoft Store for Business app 9. Select Company Portal and click on Assignments	 Client apps - Apps > Company Portal - Assignments Company Portal - Assignments Client Apps Search (Ctrl+/) Overview manage Properties Assignments monitor Device install status User install status Save Discard Add group GROUP | ASSIGNMENT TYPE | MODE No assignments, select 'Add group' to add a group
10. Select Add group 11. On Assignment Type choose required 12. Then select group and select the MDM group that you have created.	 Add group When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more. Select groups where you want to assign this app. Assignment type: Required No groups selected Included Groups No groups selected Excluded Groups Assign Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list Select the groups where you want to make this app required. All users and devices Make this app required for all users: Yes [✓ No] Make this app required on all devices: Yes [✓ No] Selected groups Select groups to include GROUP No groups selected
13. Then select group and select the MDM group that you have created. 14. Then click OK 15. Then Click OK again 16. Click Save	 Add group When excluding groups, you cannot mix user and device groups across include and exclude. Click here to learn more. Select groups where you want to assign this app. Assignment type: Required No groups selected Included Groups No groups selected Excluded Groups OK Assign Groups that have already been assigned or selected are disabled. To select a disabled group, remove it from this app's assigned list Select the groups where you want to make this app required. All users and devices Make this app required for all users: Yes [✓ No] Make this app required on all devices: Yes [✓ No] Selected groups Select groups to include GROUP No groups selected OK Select groups Azure AD groups Invite Select Search by name or email address BD Business Development BusinessDevelopment@M365x199... C# Contoso #02 Contoso02@M365x199294.onmic... DF DG-2000 Feedback dg-2000feedback@M365x199294.... DP DG-2000 Product Team DG-2000ProductTeam@M365x19... ✓ EE Electronic Events ElectronicEvents@M365x199294.o... EN Engineering Engineering@M365x199294.onmi... FI Finance Finance@M365x199294.onmicros... Selected Electronic Events Select Success! 10:21 AM Assignments saved successfully

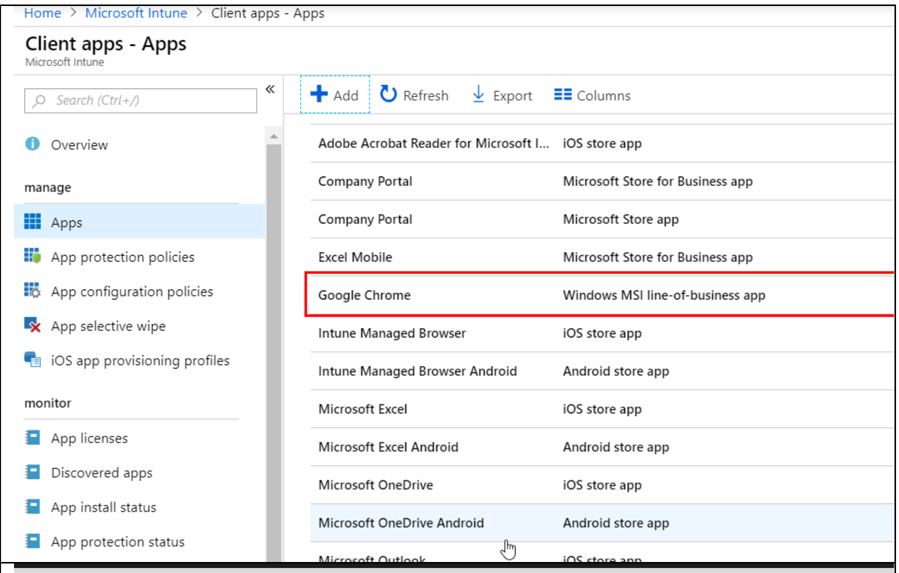
Exercise 15: MSI app deployment

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

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

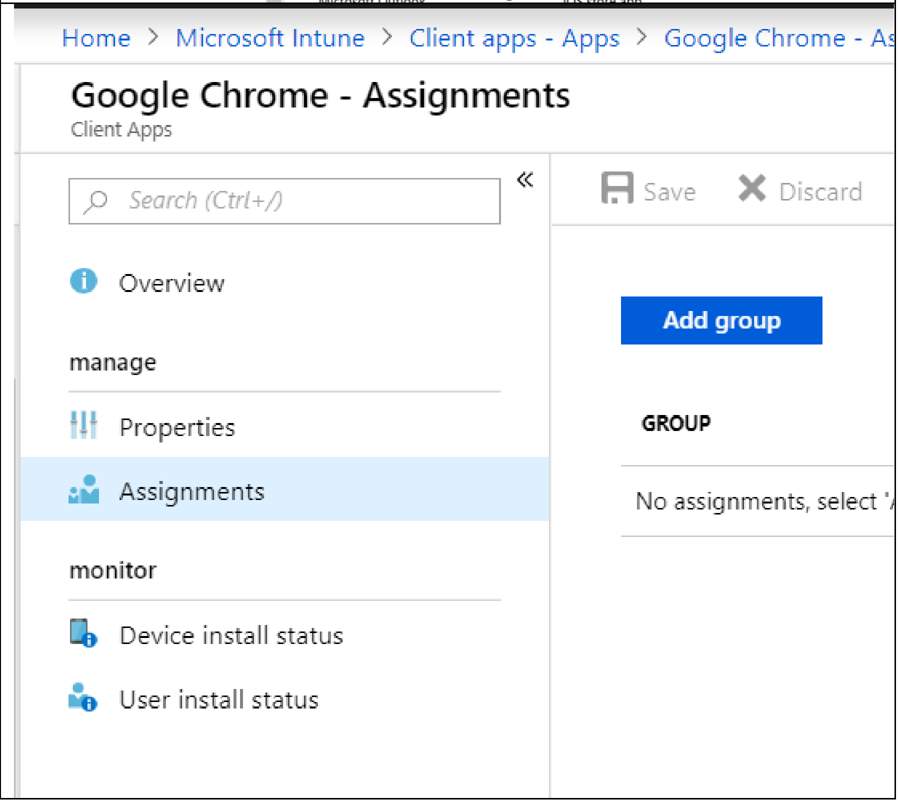
4. Select App information 5. Enter a Description 6. Enter a Publisher 7. Select OK 8. Select ADD	 Add app * App type Line-of-business app * App package file GoogleChromeStandaloneEnterp... * App information Configure Add App information * Name Google Chrome * Description Google Chrome * Publisher Google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

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



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

11. Select Assignments and add group



No assignments, select '

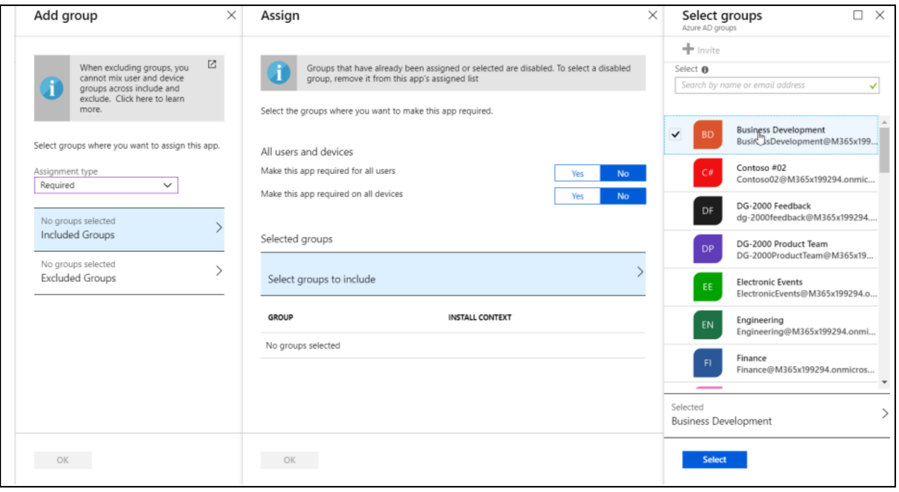
12. At assignment type choose Required

13. Select the group you created and choose Select

14. Choose OK

15. And OK again

16. Finally press Save



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

Select groups where you want to assign this app.

Assignment type: Required

No groups selected
Included Groups

No groups selected
Excluded Groups

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

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

All users and devices

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

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

Selected groups

Select groups to include

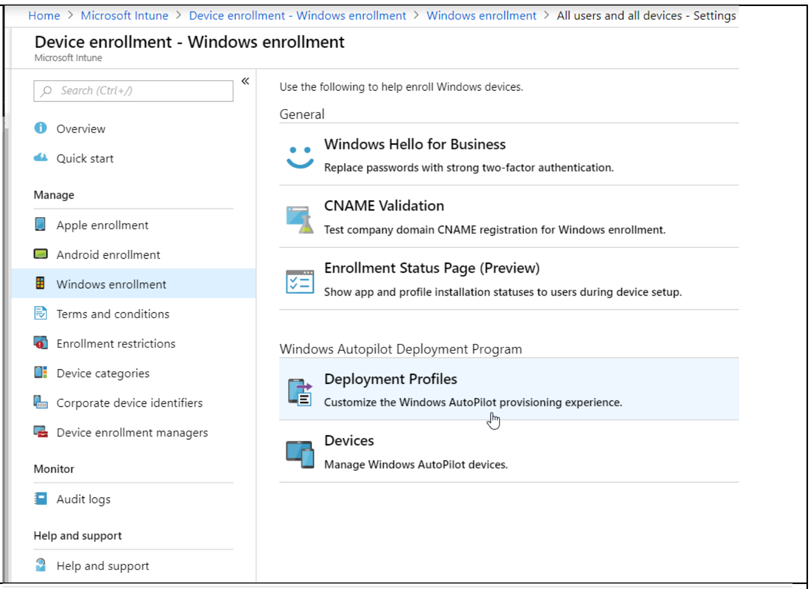
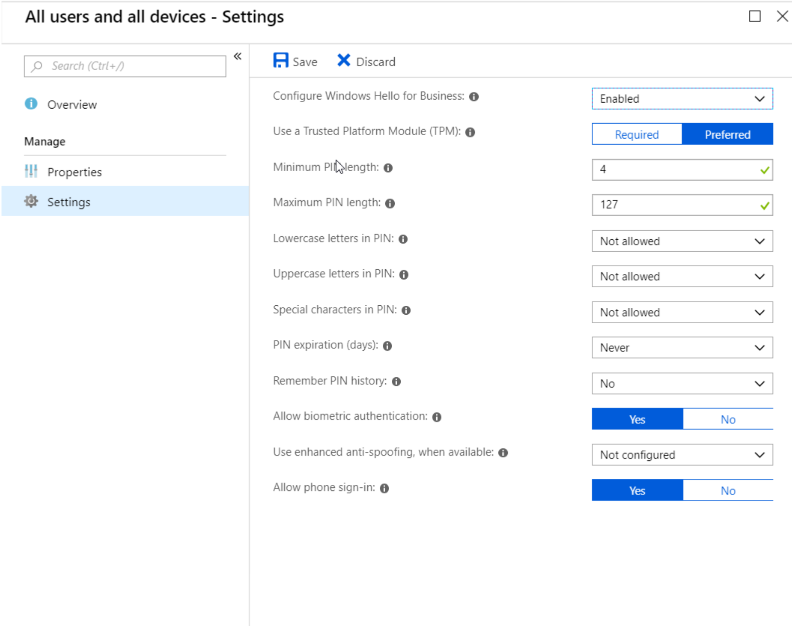
GROUP	INSTALL CONTEXT
No groups selected	

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

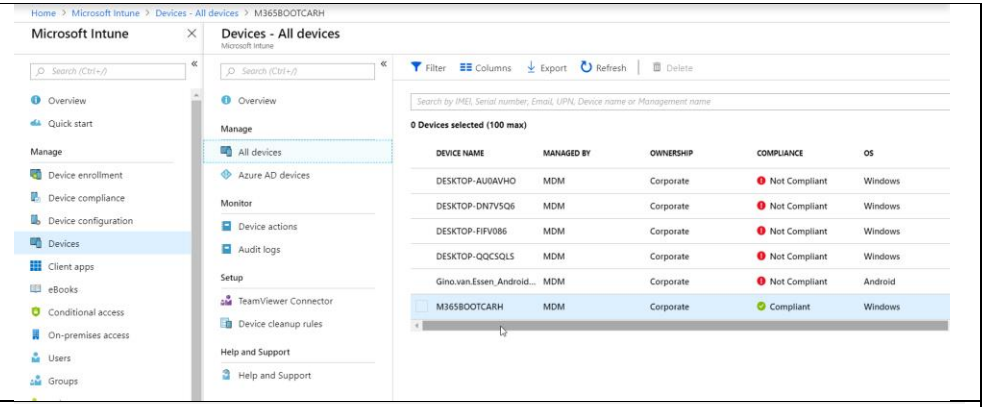
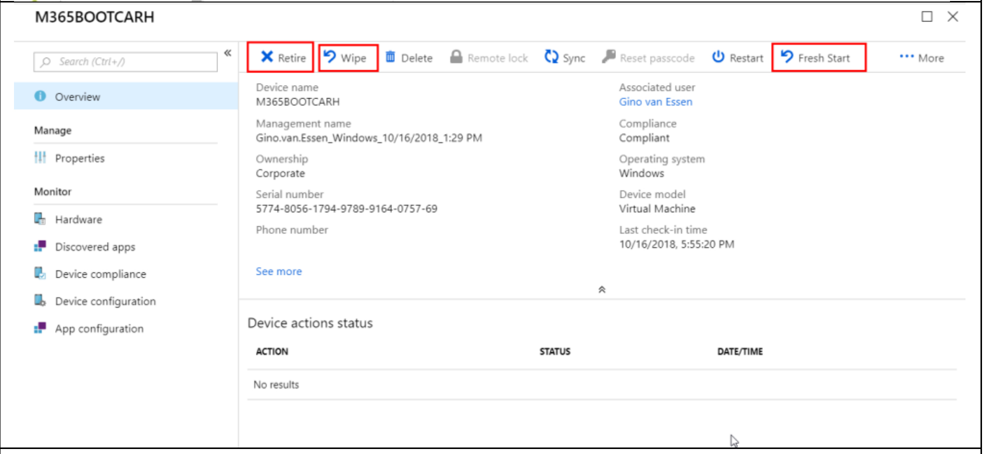
Selected: Business Development

Exercise 16: Windows Hello

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

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

Activity 5: Selective Wipe

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

Home > Microsoft Intune > Devices - All devices > M365BOOTCARH

Devices - All devices
Microsoft Intune

0 Devices selected (100 max)

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

M365BOOTCARH

Device name
M365BOOTCARH

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

Ownership
Corporate

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

Phone number

Associated user
Gino van Essen

Compliance
Compliant

Operating system
Windows

Device model
Virtual Machine

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

Device actions status

ACTION	STATUS	DATE/TIME
No results		

This is the end of the lab.

Extra resources:

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

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

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

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