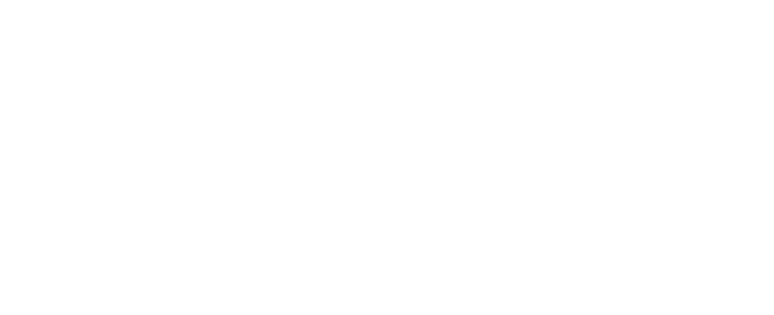
Operations Management Suite

-

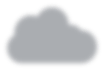
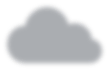
Log Analytics Labs



Modern Workplace

Hands-on lab

AAD Premium, Intune, Office ProPlus





Thursday, August 24, 2017

Version 2.0

*Prepared by*

Gino van Essen & Gido Veekens

Technical Cloud Consultants – Copaco Nederland

*Contributors*

Gino van Essen

Gido Veekens

# Document Revision

## Change Record

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Author | Version | Change Reference |  |
| August 24, 2017 | Gino van Essen | 0.1 |  |  |
| September 19,2017 | Gino van Essen | 1.0 |  |  |
| September 20,2017 | Gino van Essen | 1.1 | New Group |  |
| November 11,2017 | Gino van Essen | 2.0 | WIN 10 Fall creators update |  |
| Name | Version Approved | | Position | Date |
| Gido Veekens | 0.1 | |  | 18/09/2017 |

Gido Veekens 2.0 20/11/2017

Table of Contents

[Document Revision 2](#_Toc493627960)

[Change Record 2](#_Toc493627961)

[Introduction 4](#_Toc493627962)

[Objectives 4](#_Toc493627963)

[Student Materials 5](#_Toc493627964)

[Activity 1: Getting Started 6](#_Toc493627965)

[Objectives 6](#_Toc493627966)

[Exercise 1: Create Windows 10 Enterprise VM 6](#_Toc493627967)

[Activity 2: Prepare Modern workplace with Intune 8](#_Toc493627968)

[Exersize 2: Create AAD Group 8](#_Toc493627969)

[Exercise 3: Configure MDM and MAM Intune settings 10](#_Toc493627970)

[Exercise 4: Activate Self Service Password Reset 11](#_Toc493627971)

[Exercise 5: Company branding 12](#_Toc493627972)

[Exercise 6: Terms & Conditions 13](#_Toc493627973)

[Exercise 7: Device Settings 14](#_Toc493627974)

[Exercise 8: Device Compliance 15](#_Toc493627975)

[Exercise 9: Device Configuration - Windows Device Restrictions 18](#_Toc493627976)

[Exercise 10: Windows 10 Update Rings 28](#_Toc493627977)

[Exercise 11: Office ProPlus Deployment 29](#_Toc493627978)

[Exercise 12: Windows Store for Business 31](#_Toc493627979)

[Activity 3: Windows 10 Enterprise configuration 33](#_Toc493627980)

[Exercise 13: Configure Windows 10 Enterprise Azure Active Directory join (organisatie) 33](#_Toc493627981)

# Introduction

Estimated time to complete this lab

120 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
* Join Windows 10 clients to Azure Active Directory

Prerequisites

* Laptop/computer with Internet browser and wifi connected.
* Hyper-V manager or VMware workstation
* Windows 10 Enterprise
* Enterprise Mobility + Security Suite & Office365 subscriptiton

## 

## 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:

* Credentials for the EM+S and Office365 accounts will be handed out by Copaco
* ISO of Windows 10 Enterprise (1703 or 1709) handed out by Copaco
* Hyper V Manager VM configuration

## Exercise 1: Create Windows 10 Enterprise VM

|  |  |
| --- | --- |
| 1. Open **Hyper-v Manager** |  |
| 1. Create **New > virtual machine** 2. Name **WIN10ENT-1703 / WIN10-MULTI-1709** 3. Generation **Generation 2** 4. Assign Memory **1024 MB** 5. Configure Networking **Connection External** 6. Create VHD **Standard settings** 7. Installation Options **install an OS from a bootable CD/DVD** 8. Image file: “”.iso 9. Finish / complete the configuration |  |
| 1. Start VM **WIN10ENT-1703 or WIN10-MULTI-1709** |  |
| 1. Start Windows installation with **default** settings (**Custom installation)** |  |

# Activity 2: Prepare Modern workplace with Intune

The most important components in this exercise are:

 Azure Active Directory.

 Users and Groups.

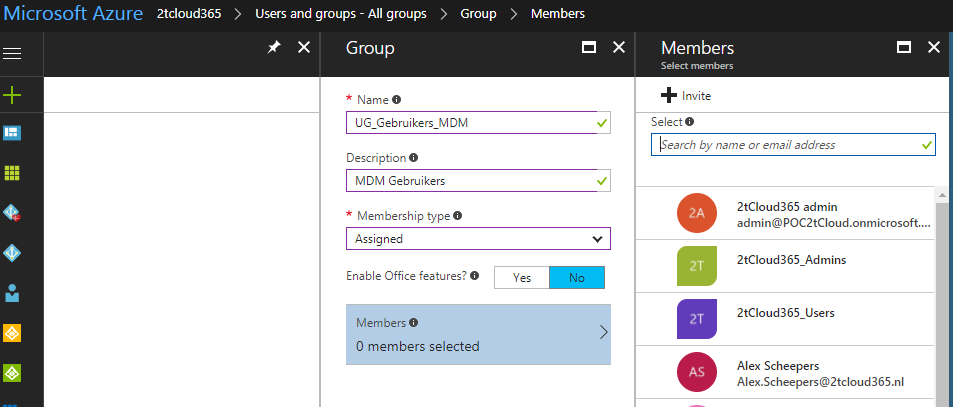
 Intune.

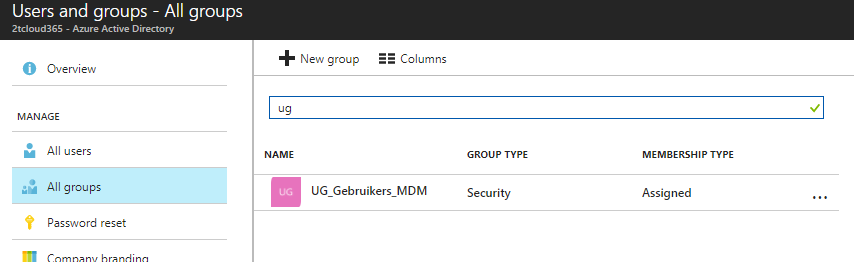
## Exersize 2: Create AAD Group

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

|  |  |
| --- | --- |
| **Kenmerk** | **Waarde** |
| Name | UG\_gebruikers\_MDM |
| Membership type | Assigned |
| Enable Office features? | No |

1. Add Admin account “received by Copaco / x@M365x110445.onmicrosoft.co “ to group **UG\_ Gebruikers\_MDM**

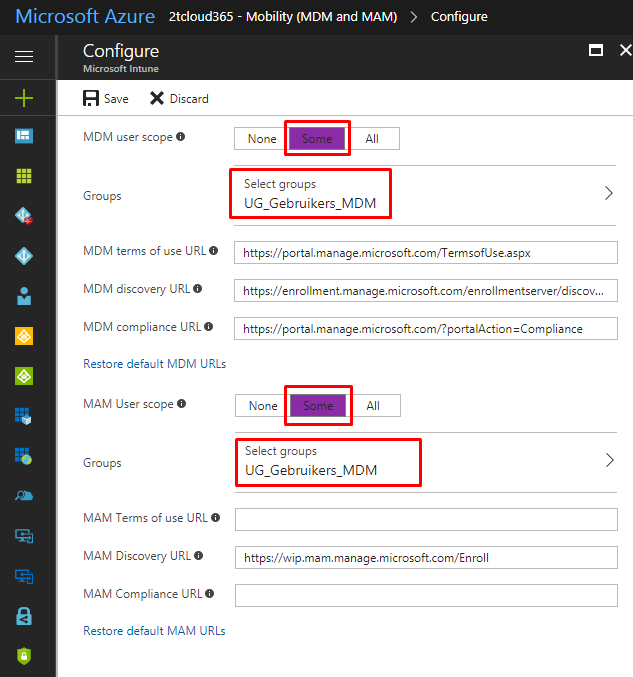




1. AAD Group is created

## Exercise 3: Configure MDM and MAM Intune settings

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



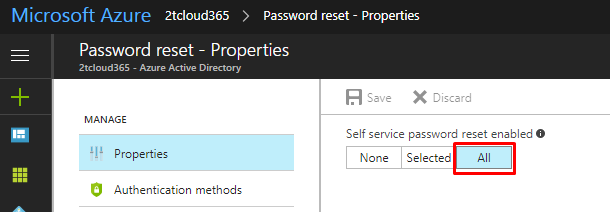
1. Configure the settings ->

|  |  |
| --- | --- |
| **Kenmerk** | **Waarde** |
| MDM User scope | Some |
| Group | UG\_Gebruikers\_MDM |

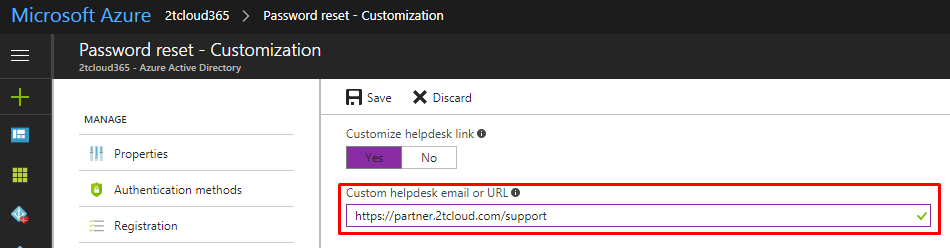
1. Click on **Save**

## Exercise 4: Activate Self Service Password Reset

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



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



1. Configure the settings ->

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

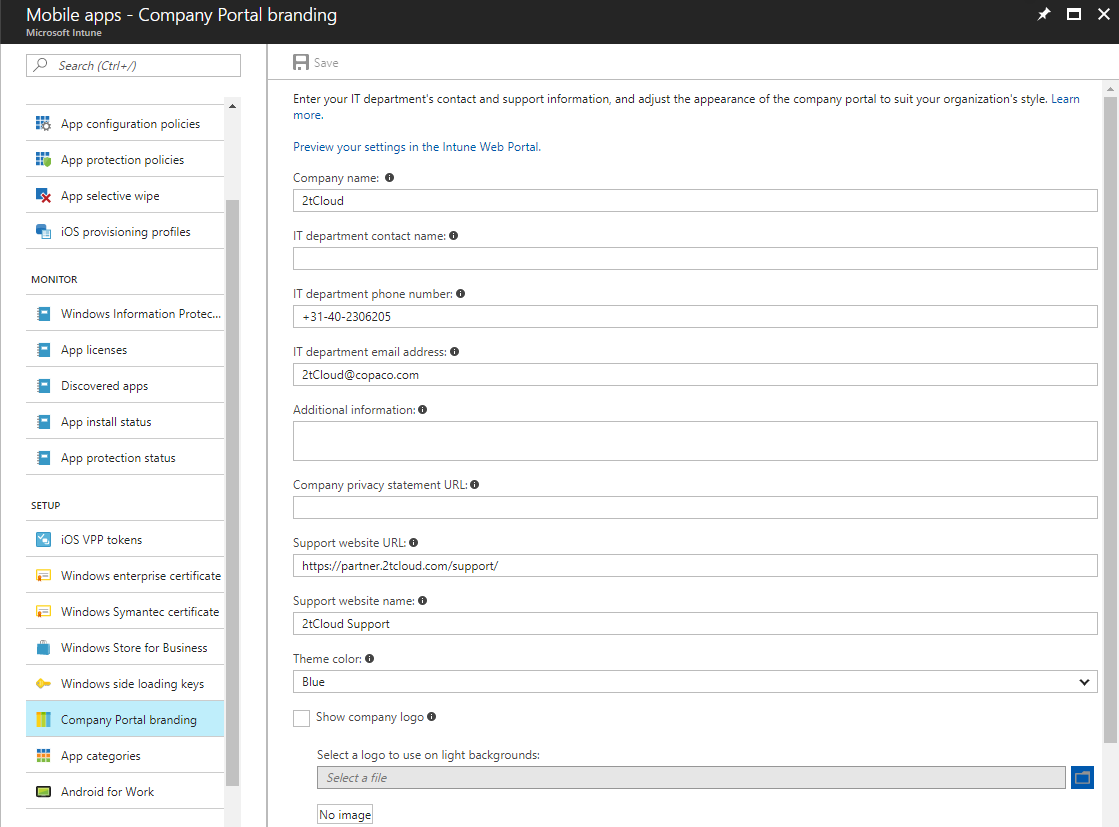
## 

## Exercise 5: Company branding

## 

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

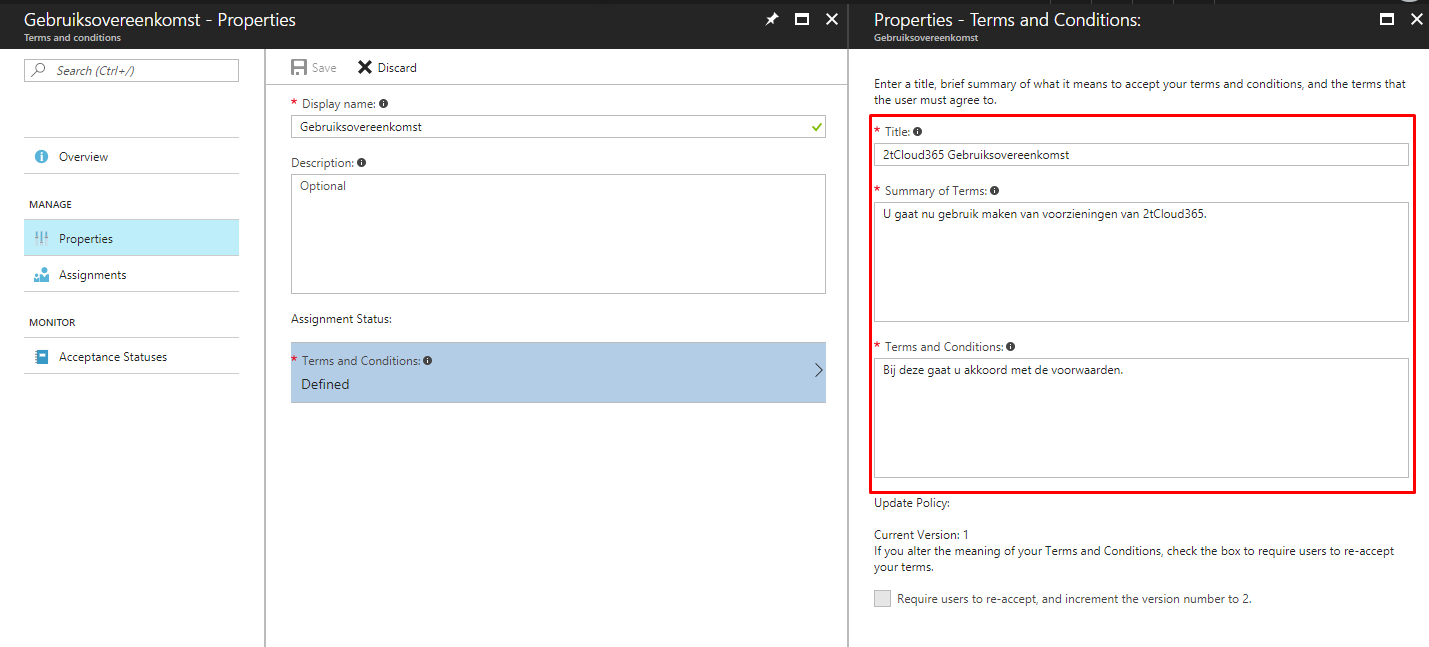
|  |  |
| --- | --- |
| Sign-in page image | Add picture |
| Banner image | Add picture |
| User name hint | [gebruikersnaam@2tcloud365.nl](mailto:gebruikersnaam@2tcloud365.nl) |
| Show option to remain signed in | No |



1. Go to **Intune -> Mobile apps - Company Portal Branding**
2. Configure the settings ->

|  |  |
| --- | --- |
| Company Name | 2tCloud |
| IT Department contact name | Add picture |
| IT Department email address | [gebruikersnaam@2tcloud365.nl](mailto:gebruikersnaam@2tcloud365.nl) |
| Support Website URL | No |
| Support website name | 2tCloud Support |

## Exercise 6: Terms & Conditions

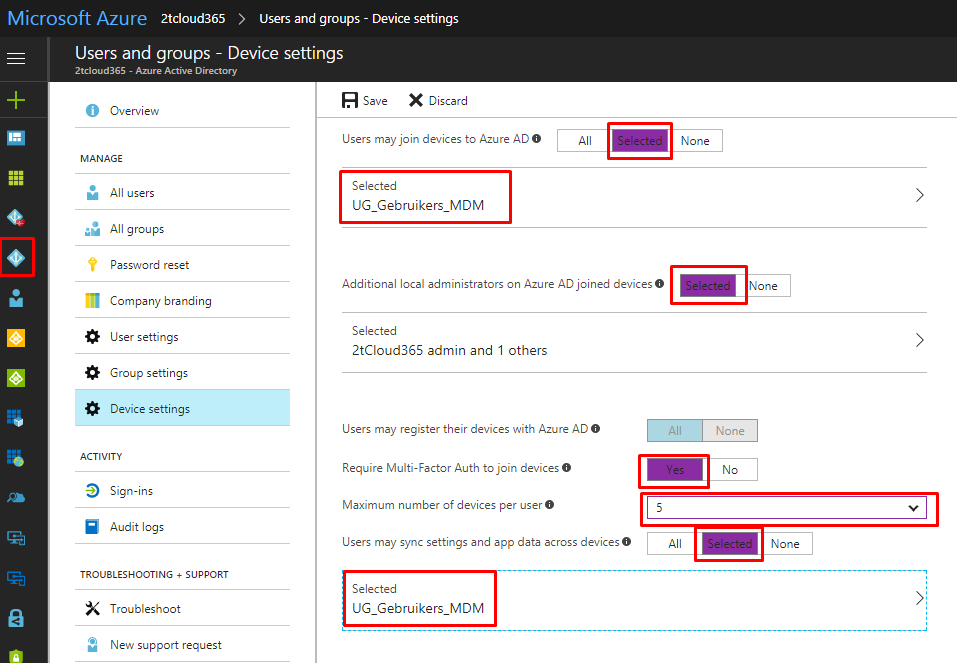


1. Go to **Intune -> Device Enrollment – Terms & Conditions**
2. Create new
3. Configure the settings ->

|  |  |
| --- | --- |
| Display name | Gebruikersovereenkomst |
| IT Department contact name | Add picture |
| Title | 2tcloud gebruikersovereenkomst |
| Summary of Terms | Enter terms summary |
| Terms and conditions | Enter terms |

1. Click on **Save**
2. Click on **Assignments** and assign to group **UG\_Gebruikers\_MDM**

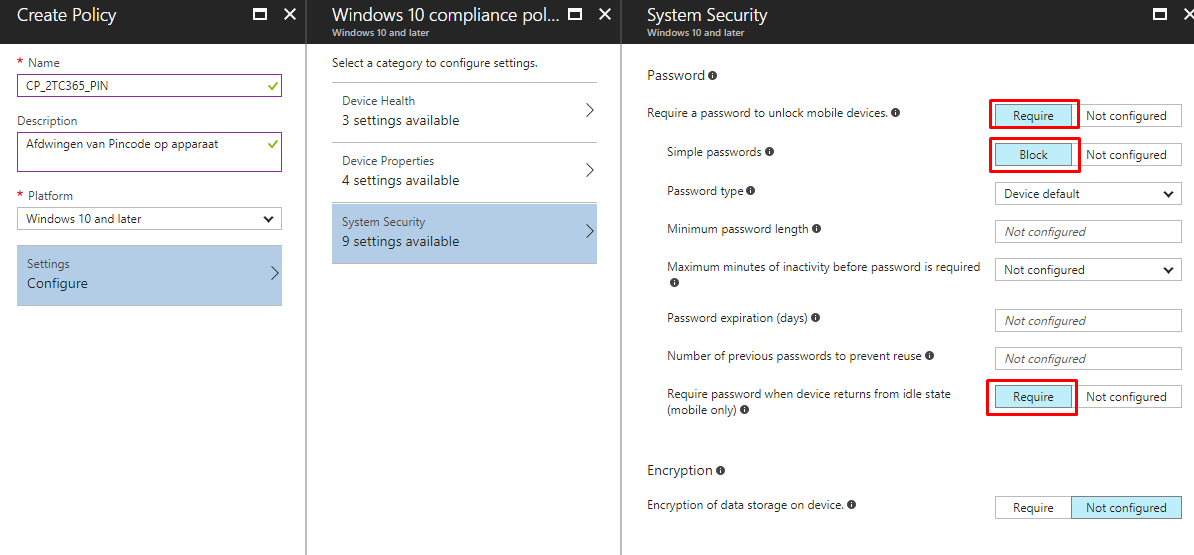
## Exercise 7: Device Settings



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

|  |  |
| --- | --- |
| 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 |

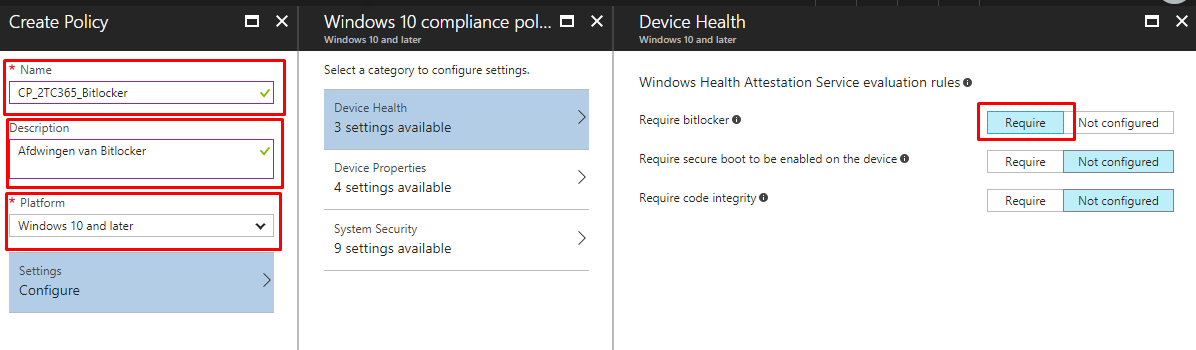
## Exercise 8: Device Compliance



1. Go to **Intune->Device Compliance->Policies->Create Policy;**
2. Configure the settings >

|  |  |
| --- | --- |
| Name | CP\_2tC365\_PIN |
| Platform | Windows 10 and later |

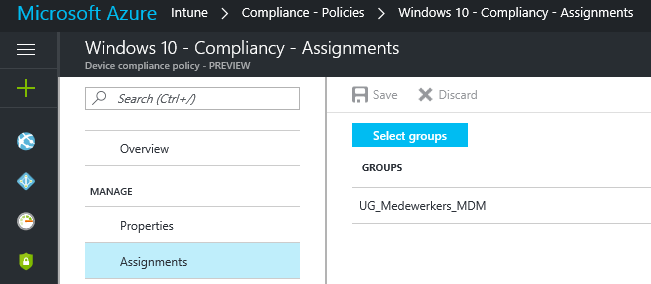
1. Click on **Configure**
2. Configure settings as showed on the screenshot



1. Configure the settings ->

|  |  |
| --- | --- |
| Name | CP\_2TC365\_Bitlocker |
| Platform | Windows 10 and later |

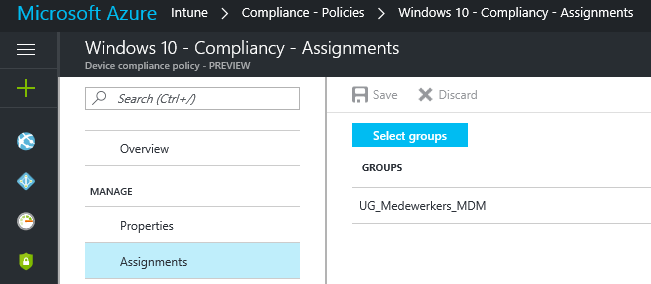
1. Click on **Configure**
2. Configure settings as showed on the screenshot
3. Go to Intune->Device Compliance->Policies-> **CP\_2TC365\_Bitlocker->**Assignments->Select groups;



1. Configure the settings >

|  |  |
| --- | --- |
| Groups | UG\_Gebruikers\_MDM |

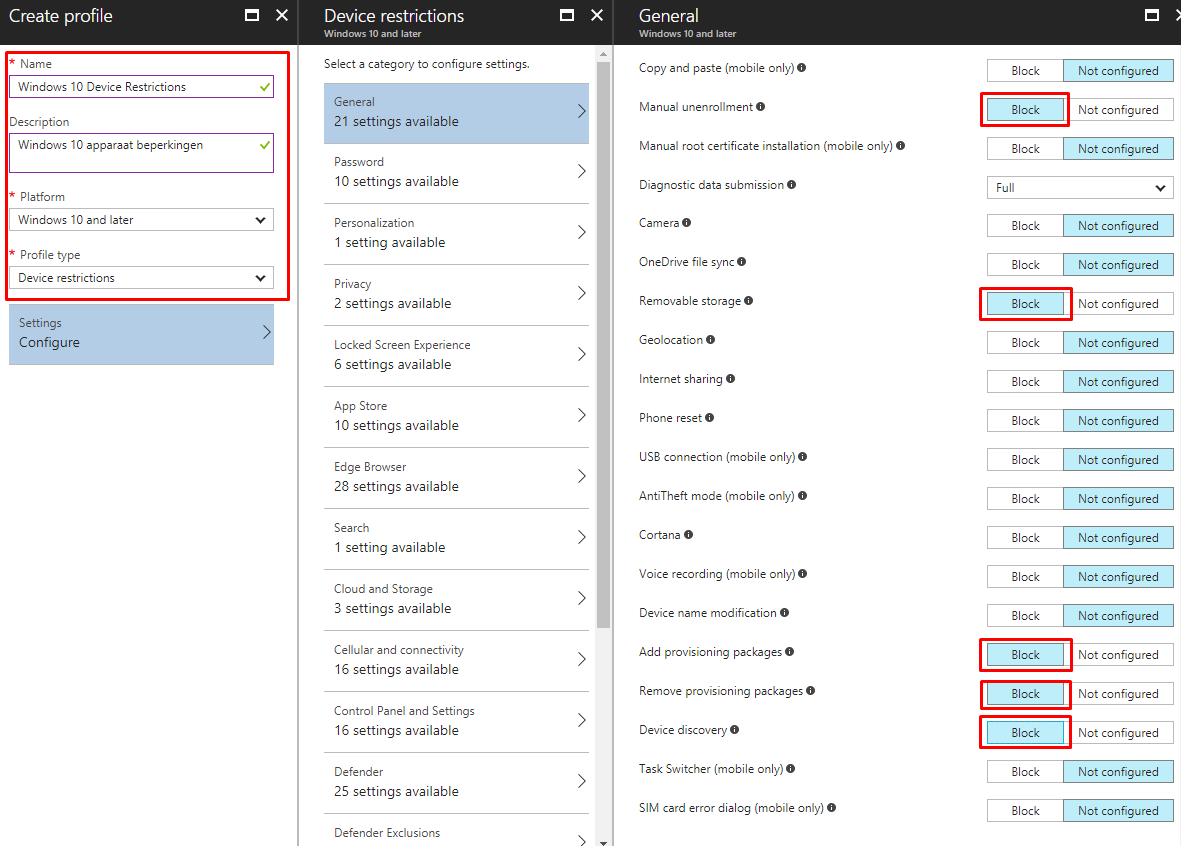
Go to Intune->Device Compliance->Policies-> **CP\_2tC365\_PIN** ->Assignments->Select groups;



1. Configure the settings >

|  |  |
| --- | --- |
| Groups | UG\_Gebruikers\_MDM |

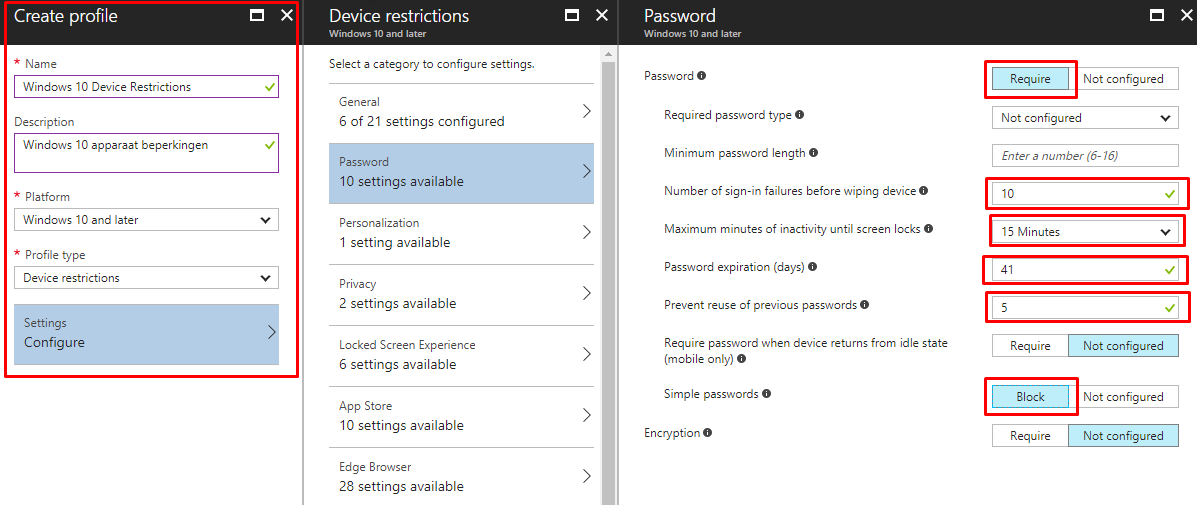
## Exercise 9: Device Configuration - Windows Device Restrictions



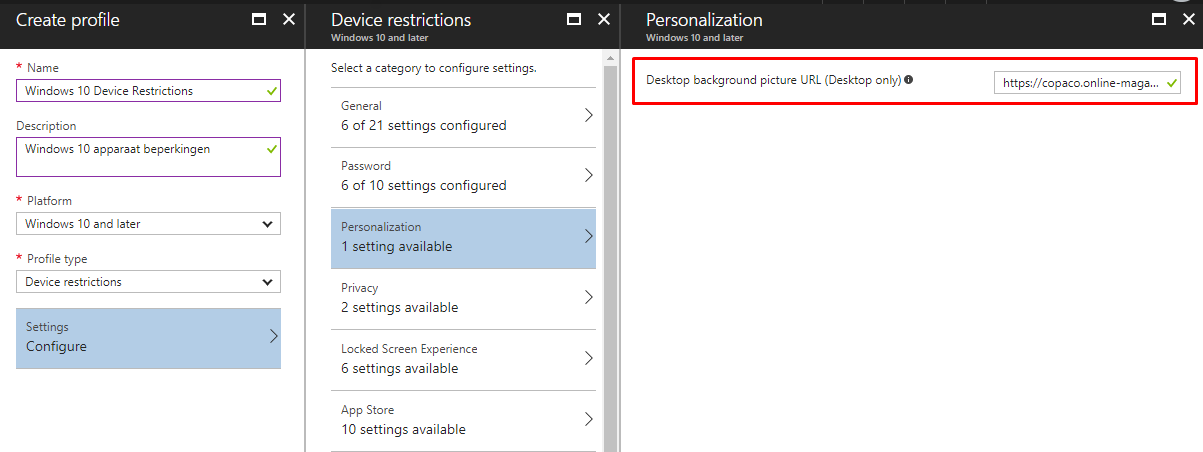
1. Go to **Intune->Device Configuration->Profiles->Create Profile;**
2. Configure the settings >

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

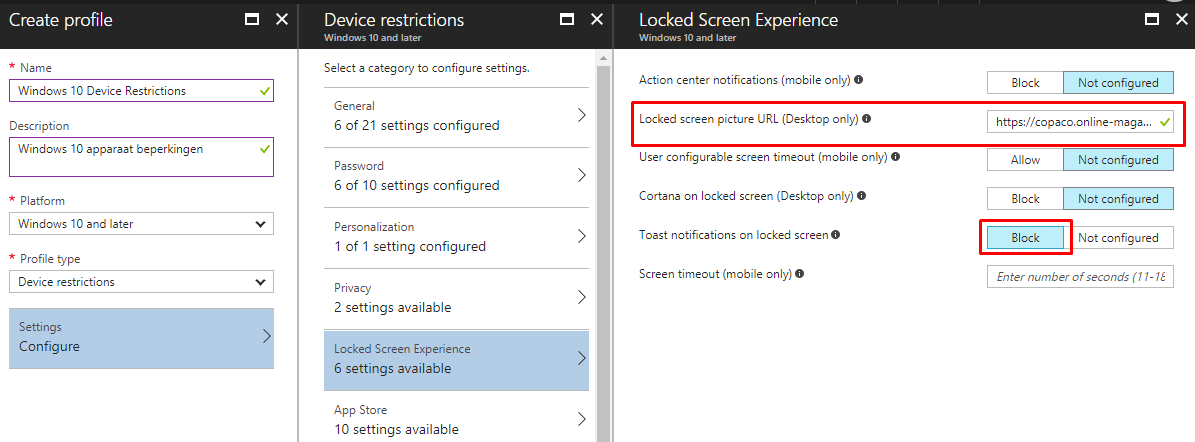
1. Configure settings as showed on the screenshot (General)



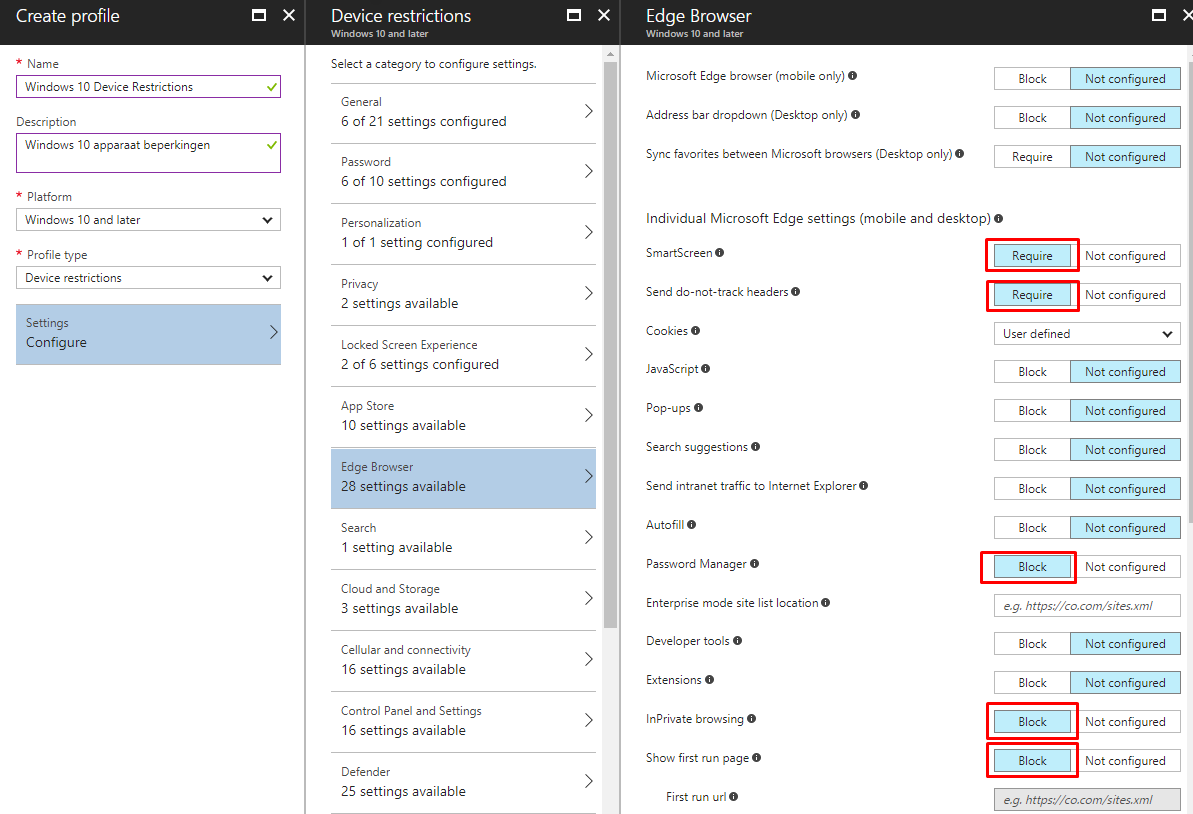
1. Configure settings as showed on the screenshot (Password)

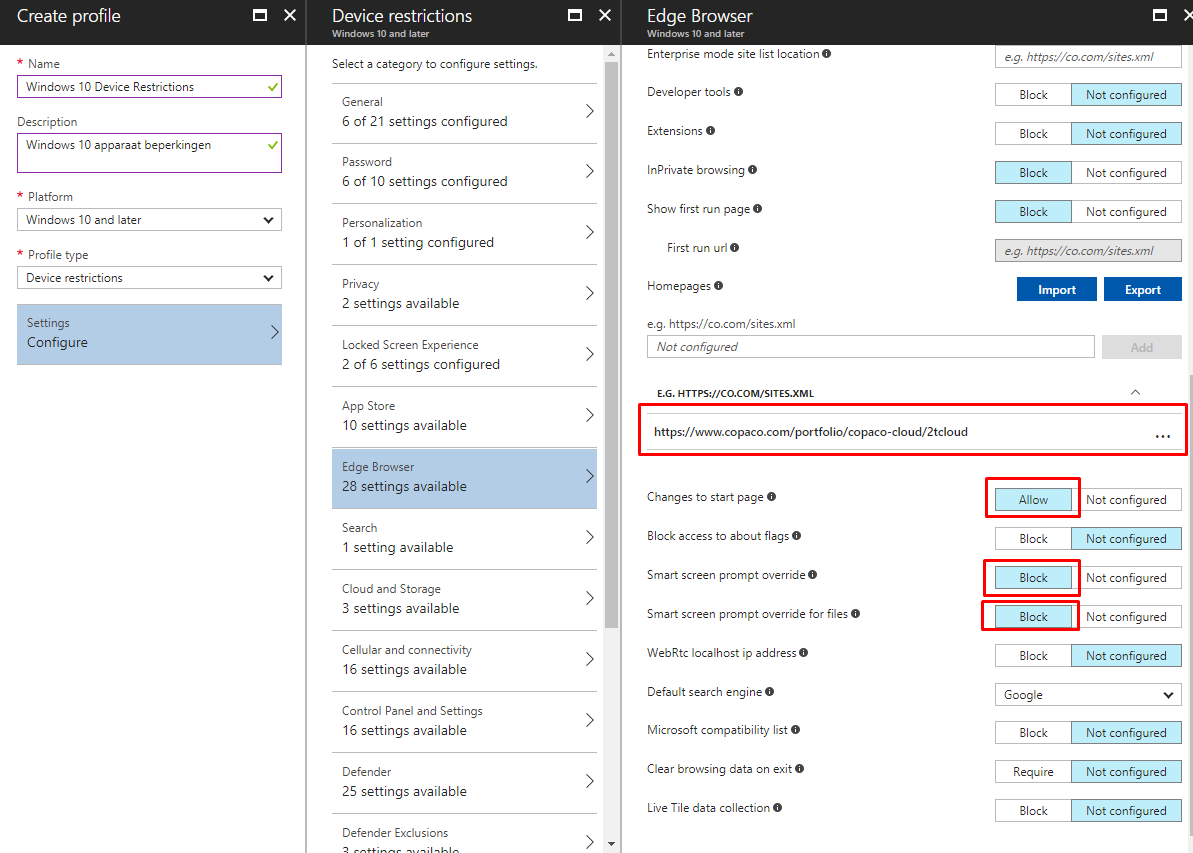


1. Configure settings as showed on the screenshot (Personalization)

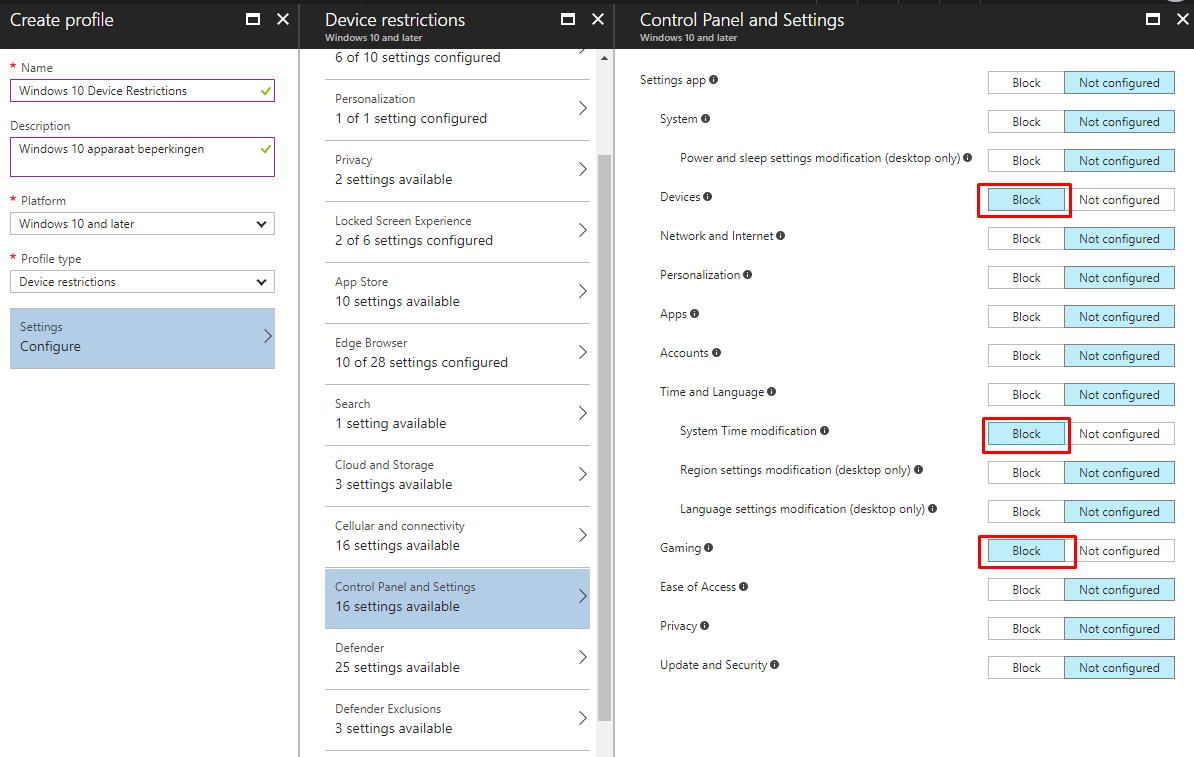


1. Configure settings as showed on the screenshot (Lock Screen Experience)

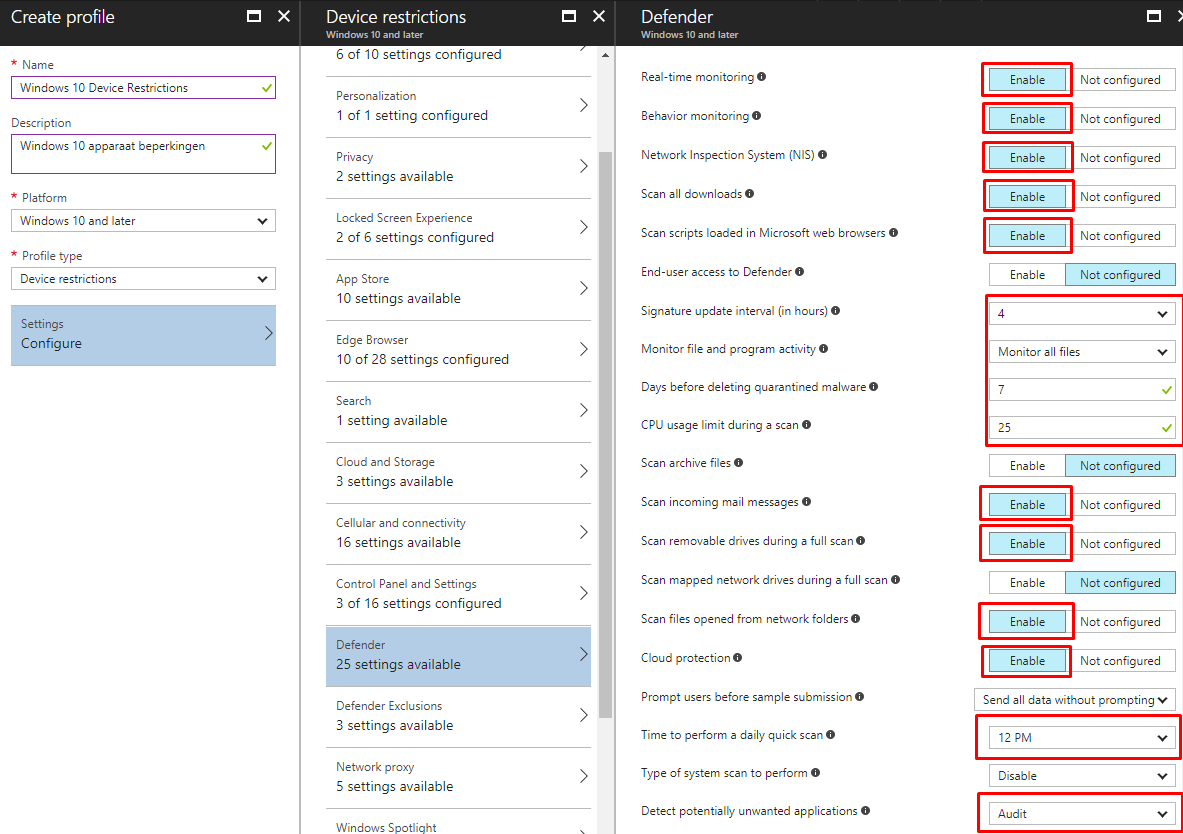


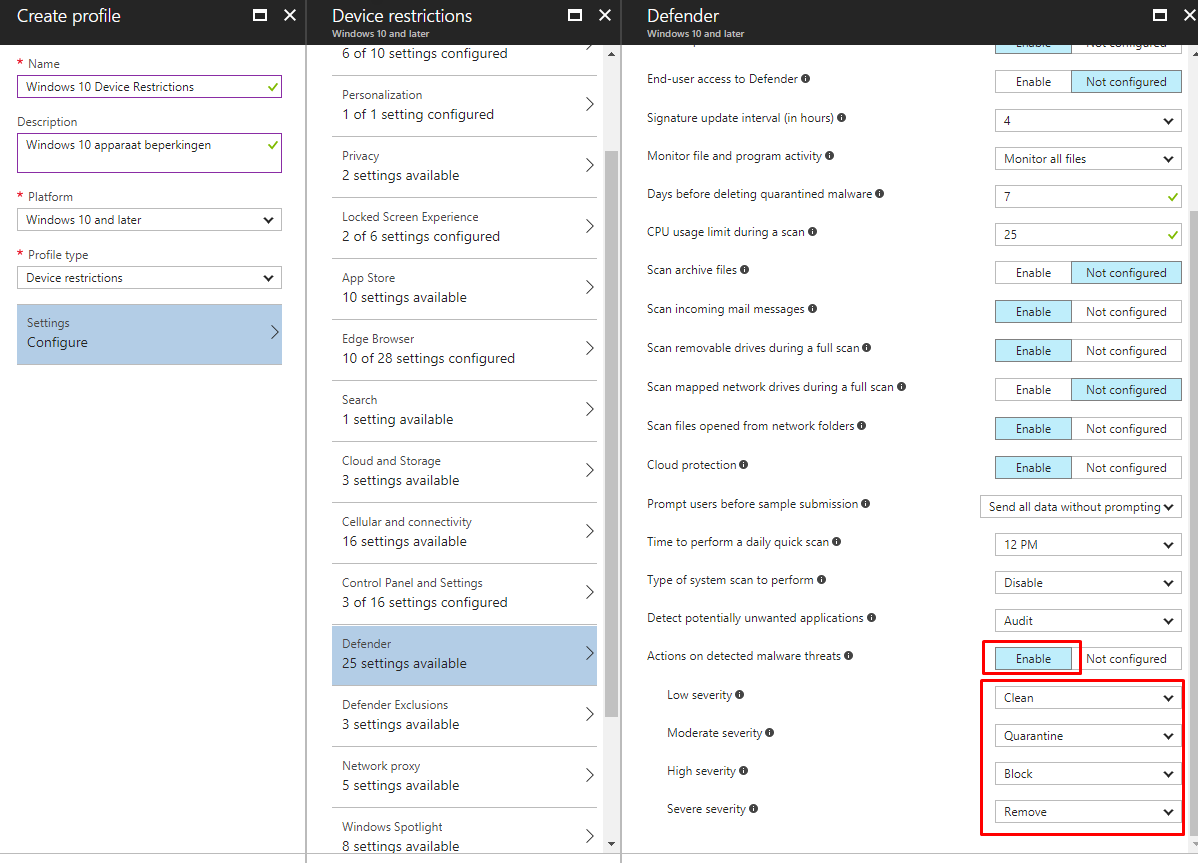


1. Configure settings as showed on the screenshots (Edge Browser)

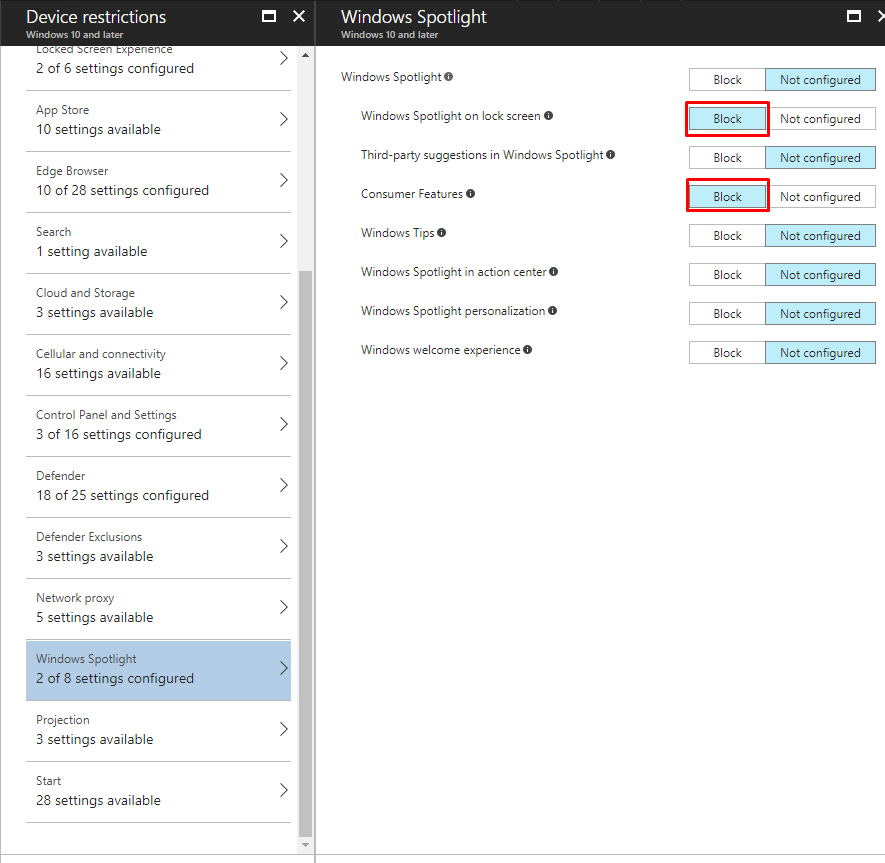


1. Configure settings as showed on the screenshot (Control Panel and Settings)

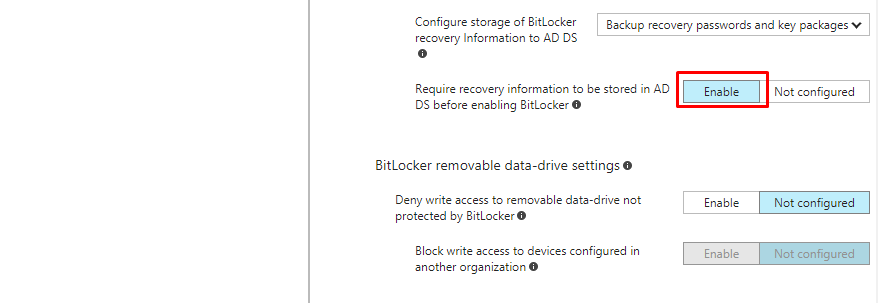
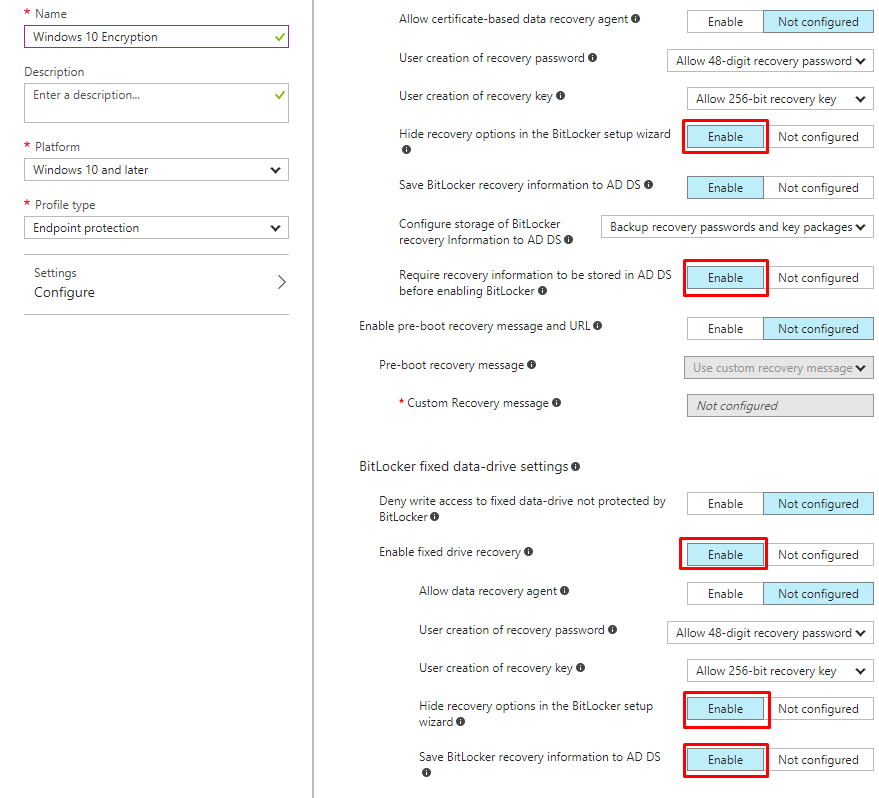
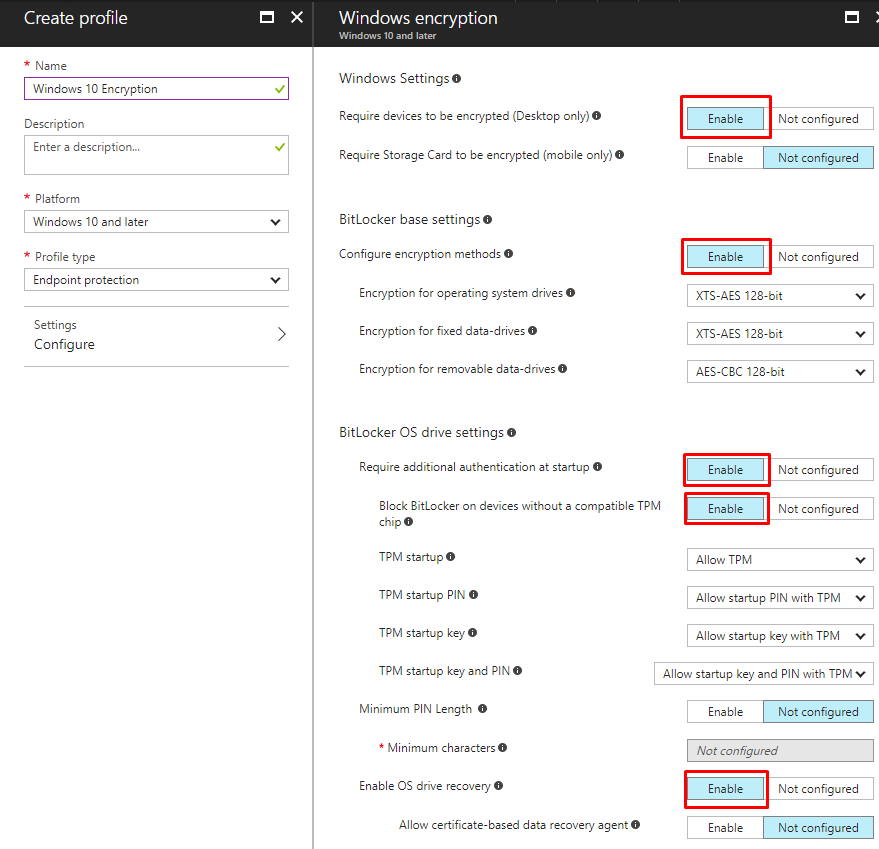




1. Configure settings as showed on the screenshot (Defender)



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

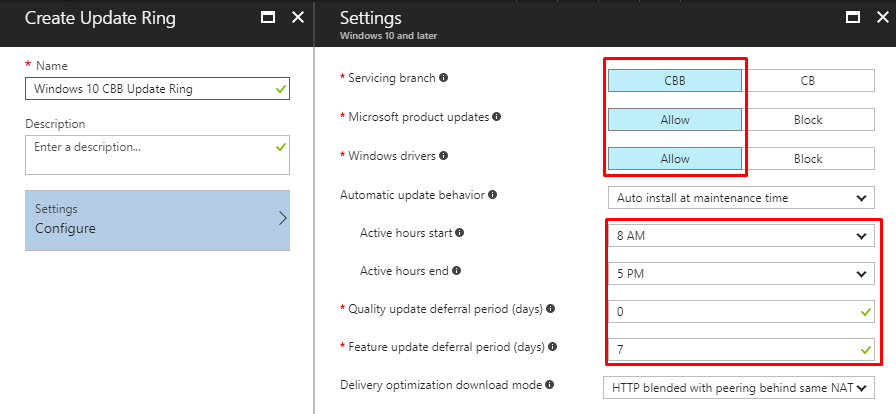


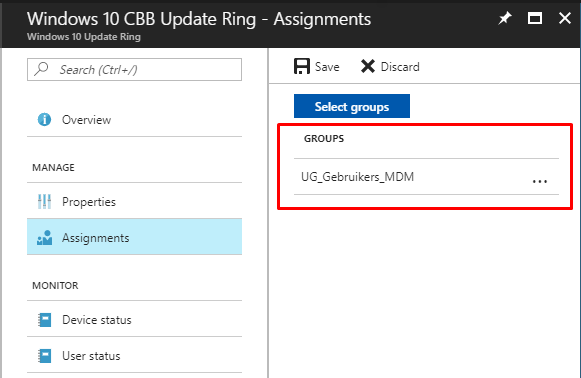
1. Go to **Intune->Device Configuration->Profiles->Create Profile;**
2. Configure the settings >

|  |  |
| --- | --- |
| Name | Windows 10 Encryption |
| Platform | Windows 10 and later |
| Profile type | Endpoint protection |

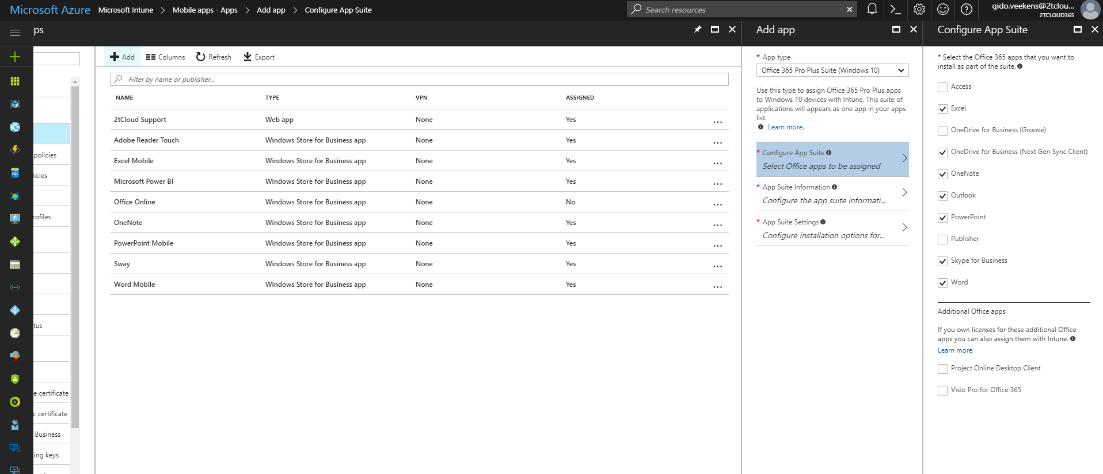
1. Configure settings as showed on the screenshots (3)

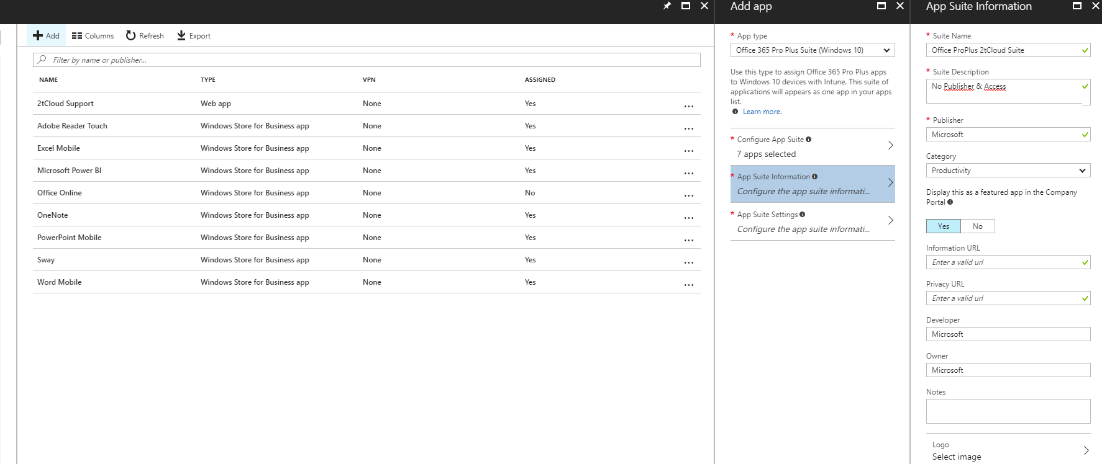
## Exercise 10: Windows 10 Update Rings

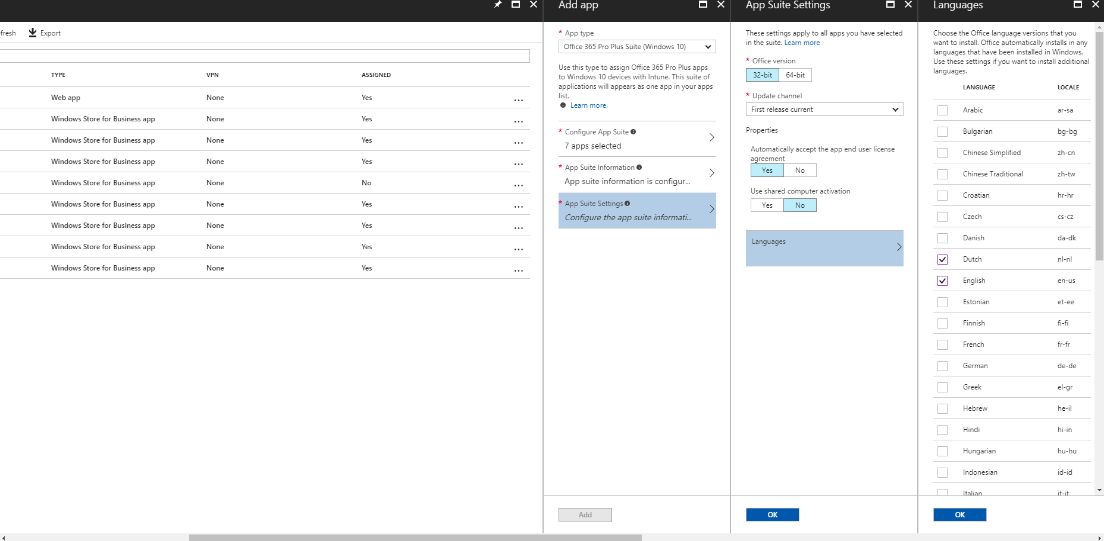


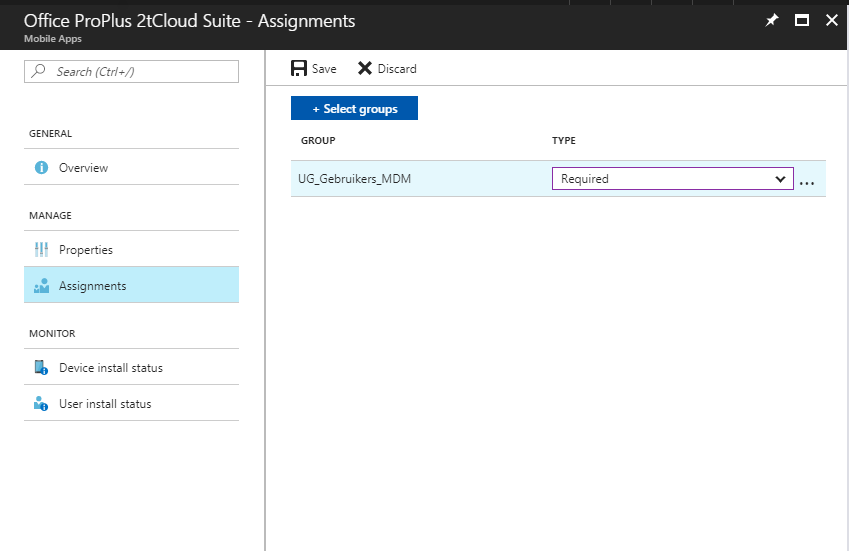


## Exercise 11: Office ProPlus Deployment









.

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

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

# Activity 3: Windows 10 PRO / Enterprise configuration

## Exercise 13: Configure Windows 10 Enterprise Azure Active Directory join (organisatie)

1. Go to the **Windows 10 Enterprise VM or WIN10-MULTI VM** In **Hyper-V manager** and **Connect to the VM.**

|  |  |
| --- | --- |
| Select **Instellen voor een organisatie** |  |
| Enter Azure Active Directory “**username”** and click on **Volgende** |  |
| Enter **Password** |  |
| If multi-factor authentication is enabled you will receive and test message or phone call |  |
| Click on **Akkoord** |  |
| Read the terms of use and click on **Accepteren** |  |
| Login will be accepted and configuration policies will be applied. Windows will be rebooted. |  |
| Enter **Password** (same as entered before) |  |
| Windows Hello is required click on **Pincode Instellen** |  |
| User is logged in. Configuration Policies are applied. |  |
| Look around and test some extra policies.  Reboot to apply. |  |

**This is the end of the lab.**

**Extra resources:**

**Microsoft 365 Enterprise**

<https://docs.microsoft.com/en-us/microsoft-365-enterprise/>

**Microsoft 365 ENT dev/test**

<https://blogs.technet.microsoft.com/solutions_advisory_board/2017/08/22/new-microsoft-365-enterprise-devtest-environment/>

**LAB / DEMO Opportunities**

<https://onedrive.live.com/?authkey=%21ADKhaqnHzWNv0zs&cid=8A8EC4F6612625E0&id=8A8EC4F6612625E0%21219&parId=8A8EC4F6612625E0%21218&o=OneUp>

**MAM policies for your Microsoft 365 dev/test environment**

<https://technet.microsoft.com/library/mt764059.aspx>

**Advanced Security Management for your Office 365 dev/test environment**

<https://technet.microsoft.com/library/mt757250.aspx>

**Advanced Threat Protection for your Office 365 dev/test environment**

<https://technet.microsoft.com/library/mt490479.aspx>

**Intune virtual labs**

<https://technet.microsoft.com/en-us/virtuallabs/bb467605.aspx>