Windows 365 Enterprise – The ultimate step-by-step deployment guide – By Robin Hobo

-Published on Mar6,2023

Windows 365 is a cloud-based service that provides Cloud PCs to end users. It's is not just a virtual machine running in Azure. Beside an own personalized desktop in the cloud, which can be accessed from anywhere on any device, and which is optimized for Microsoft 365 including Microsoft Teams AV redirection, it comes with some nice and unique features that can be offered to end users. For example, an option to restore the Cloud PC from a snapshot without the need for an IT administrator.

For the IT administrator, Windows 365 is optimized for simplicity. It can be deployed in a few clicks (I will show that step-by-step in this post). It is fully integrated in the Microsoft Intune admin center where you can apply the same policies and publish the same applications as you do on your current Intune managed devices. So, no need for additional VDI knowledge, no need to create a complete other policy set and no need to manage separate IT environments. It also comes with a fixed price per-user per-month, no matter you many hours you use the Cloud PC in a month.

Table of content

In this post I will cover the following steps:

1. Windows 365 Enterprise requirements
2. Assign Windows 365 licenses to the users
3. Configure User settings
4. Create an Azure network connection (optional)
5. Create a Custom image (optional)
6. Create a Provisioning Policy
7. Connect to the Windows 365 Cloud PC

## 1 - Windows 365 Enterprise requirements

The following requisites needs to be in place before you can start with the Windows 365 Enterprise Cloud PC deployment.

- An Azure subscription (if you want to make use of an own hosted vNet)
- Windows 365 Enterprise license

- Microsoft Intune + Windows 10/11 Enterprise + Azure AD P1 (or Microsoft 365 F3/E3/E5/A3/A5 licenses or Microsoft 365 Business Premium or Microsoft 365 Education Student Use Benefit subscriptions)
- Azure AD environment up and running
- Microsoft Intune environment up and running
- Optional: Azure Network configuration (vNet) up and running (including correct DNS configuration).
- Optional: "on-premises" Active directory up and running
- Optional: Site-to-Site VPN / Express route to have access to the domain controllers within the Azure Network (as an alternative the domain controllers can also run in Azure itself)
- Optional: Azure AD Connect up and running with Hybrid Azure AD configuration (computer objects for Cloud PC needs to sync to Azure)

2 - Assign Windows 365 licenses to the users

There are several ways to assign licenses to users, for example in the Microsoft Entra portal, in the Azure AD portal and in the Microsoft 365 admin center. In the Microsoft 365 admin center, there is also an option to request a free trail license, so I will cover this way.
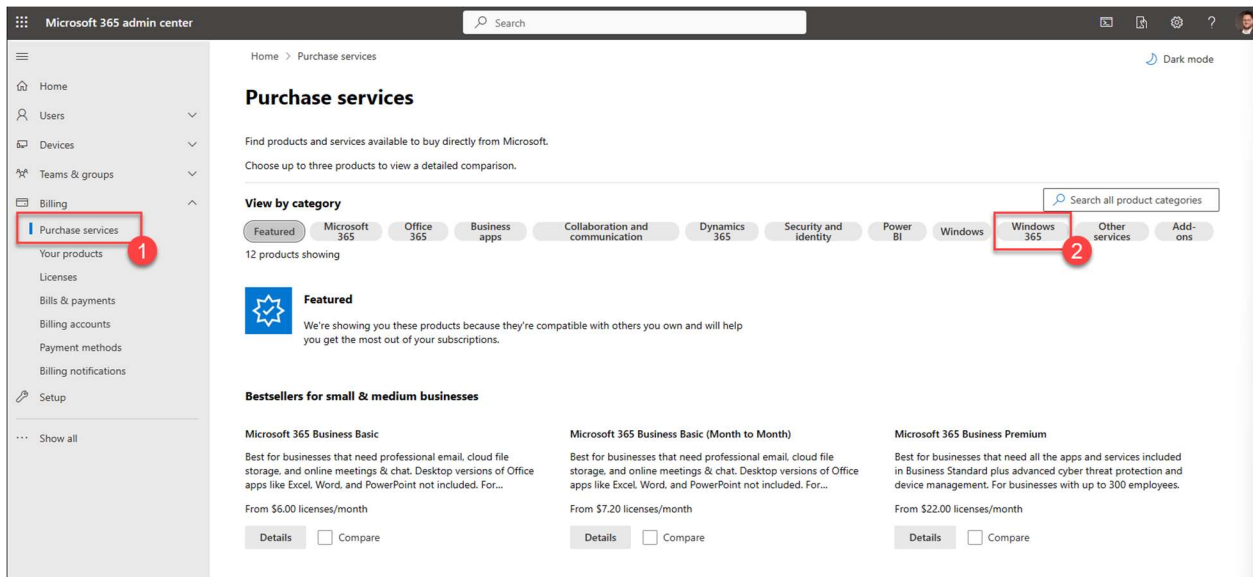
Open the Microsoft 365 admin center and navigate to **Billing > Purchase service**. Click **Windows 365**.

Under Windows 365 Enterprise, click **Details**
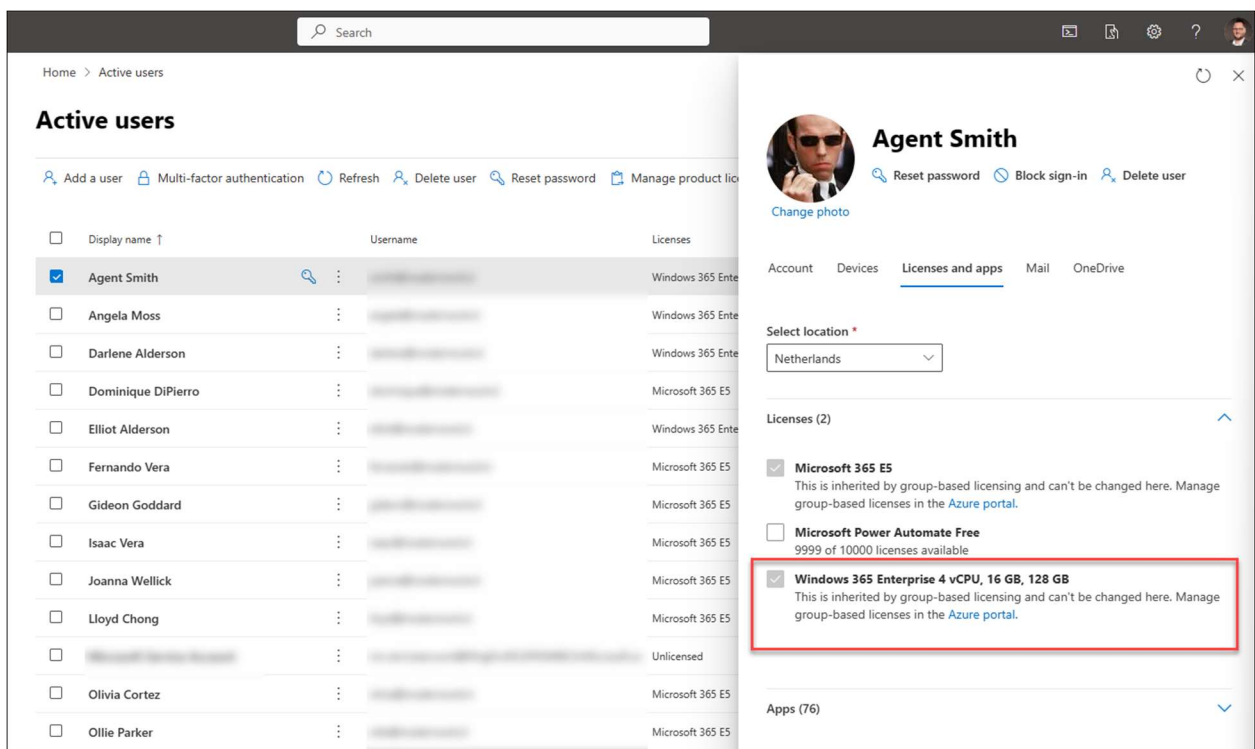
If you don't have Windows 365 licenses yet and to want to try it, you can activate a free trial license. In the **Select a plan** pull down menu you have the option to **Try for free** so you can start with Windows 365 directly.
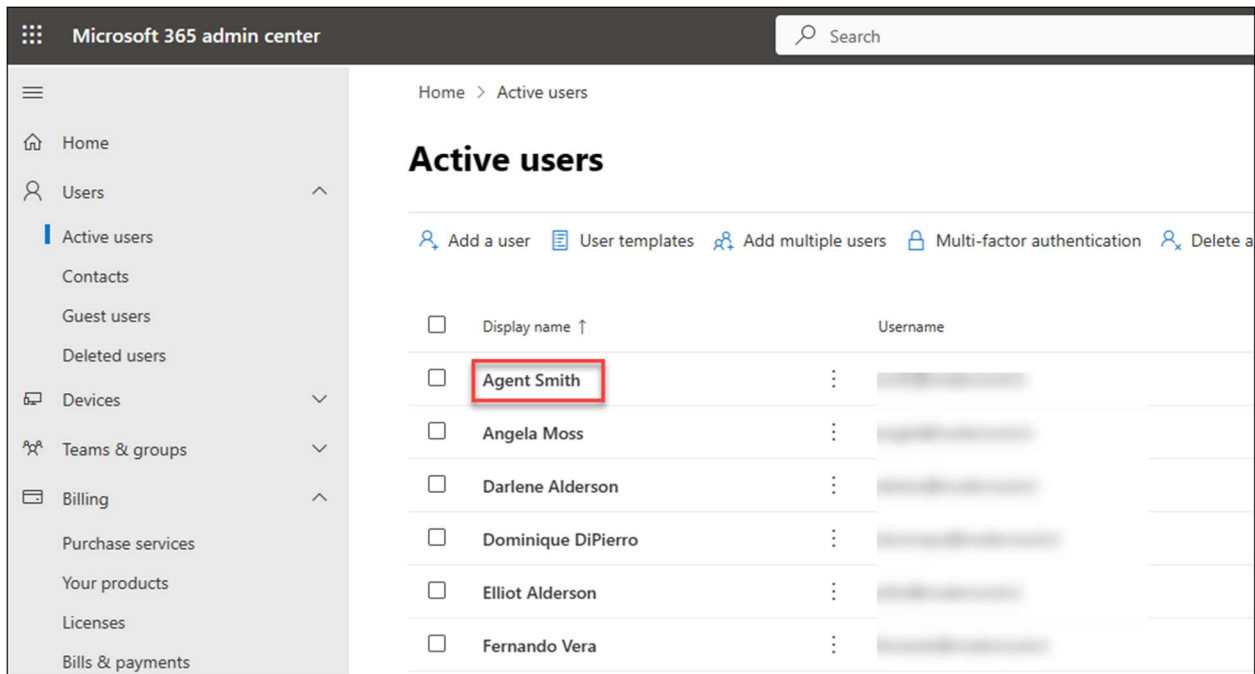
To assign a license to a user, navigate to **Users > Active users** and click on the user to want to assign a Windows 365 license.


Select the **Licenses and apps** page and assign the **Windows 365 Enterprise** license.

As an alternative you can also assign licenses based on group membership in Azure AD.

3 - Configure User settings

With user settings you can determine if a user needs to get local admin rights or not. You can also configure if you want to offer the user a point-in-time restore service where snapshots of the Cloud PC are created in the frequency you configure. User settings policies are published to Azure AD groups and you can create different User settings policies for different groups of users.
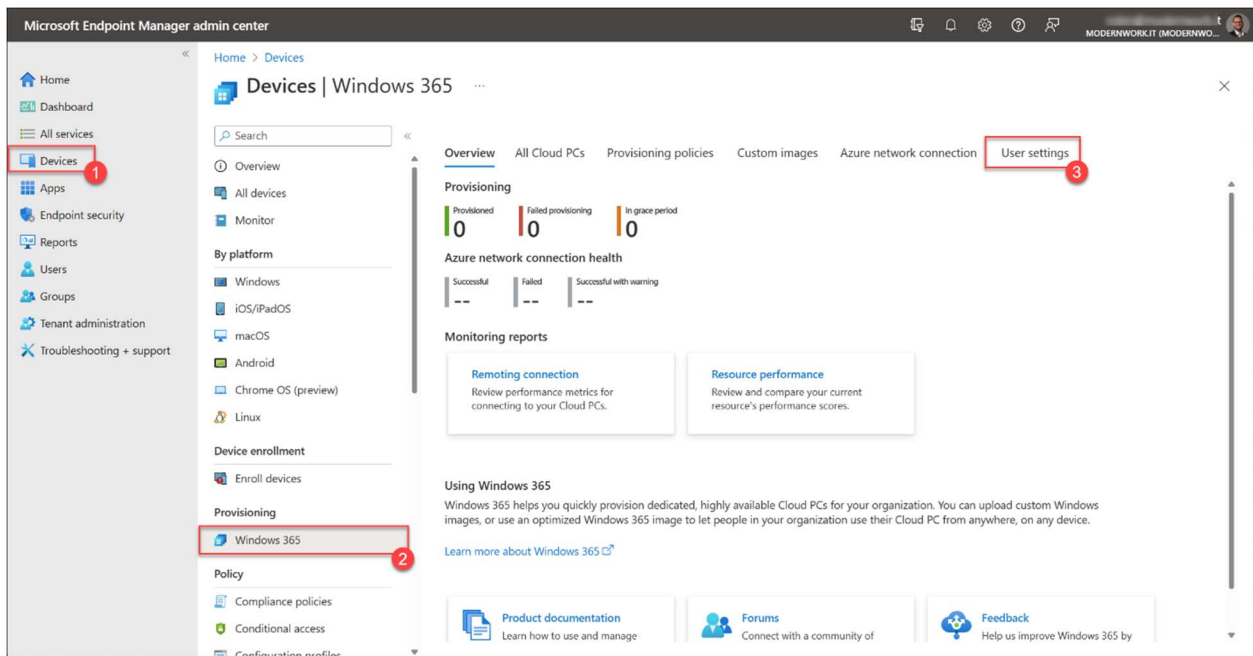
In the [Microsoft Intune admin center](), navigate to **Devices > Windows 365** and click **User settings**
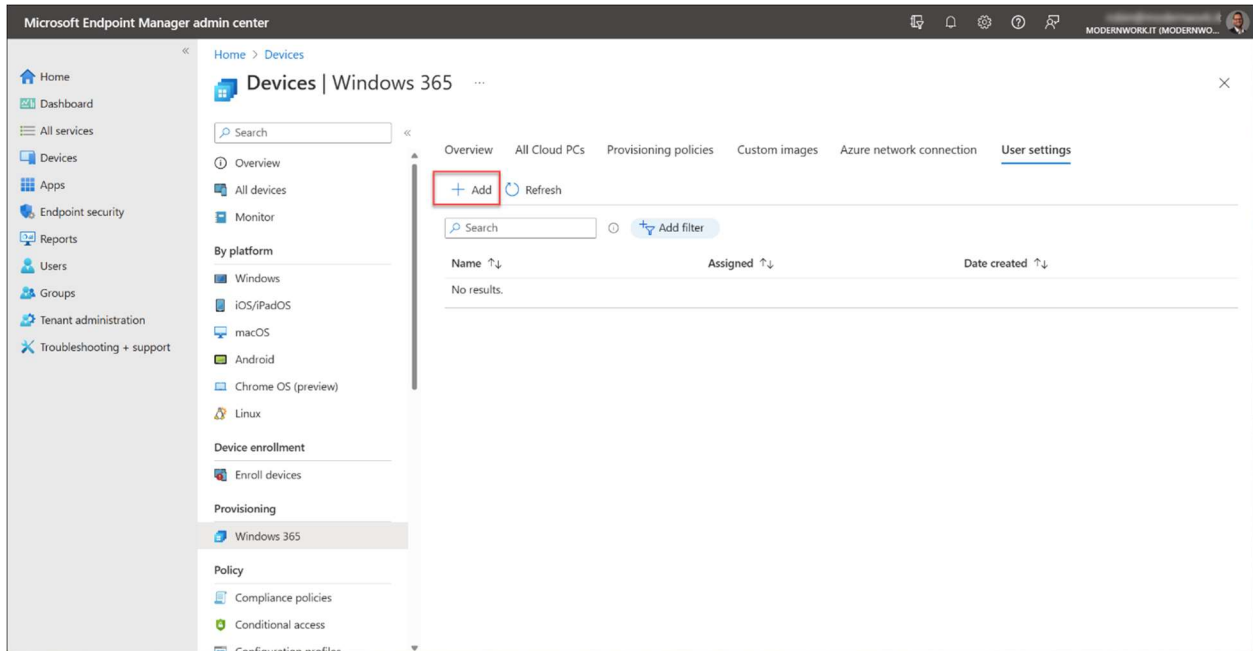
Click **+ Add**
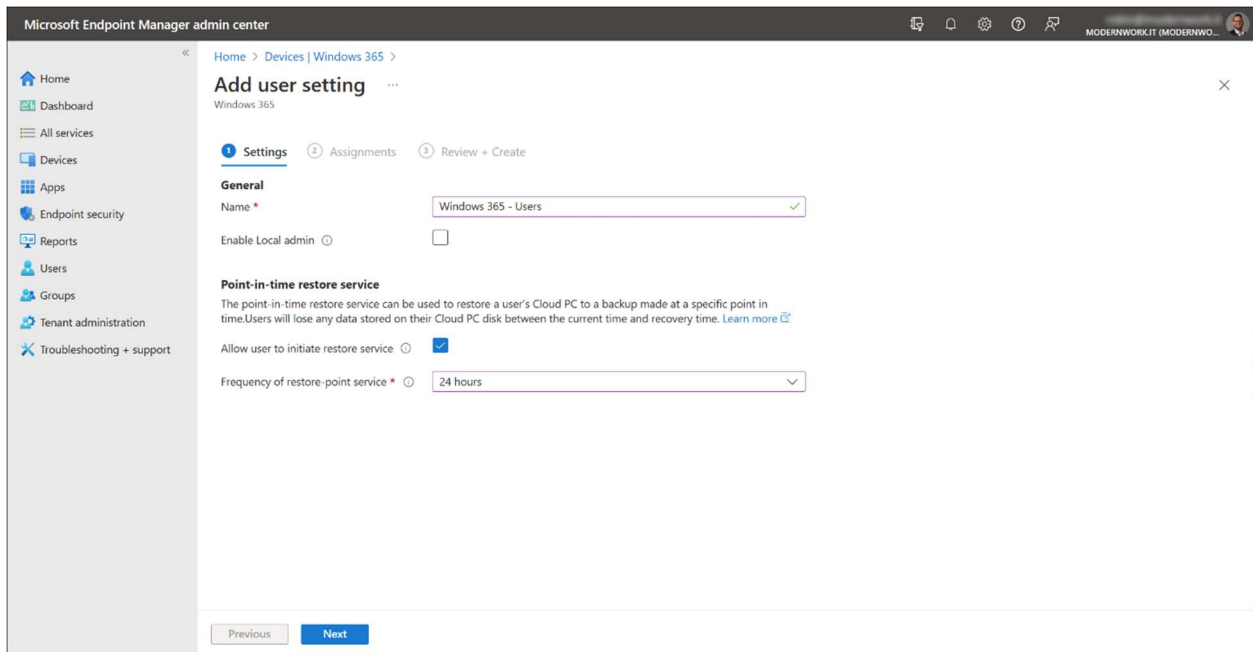
Give the policy a name and configure whether you want that users get local admin rights or not. For the point-in-time restore service a maximum of 10 snapshots will be created. So, the frequency of the restore-point determines how far you can go back with a restore.

Click **Next**
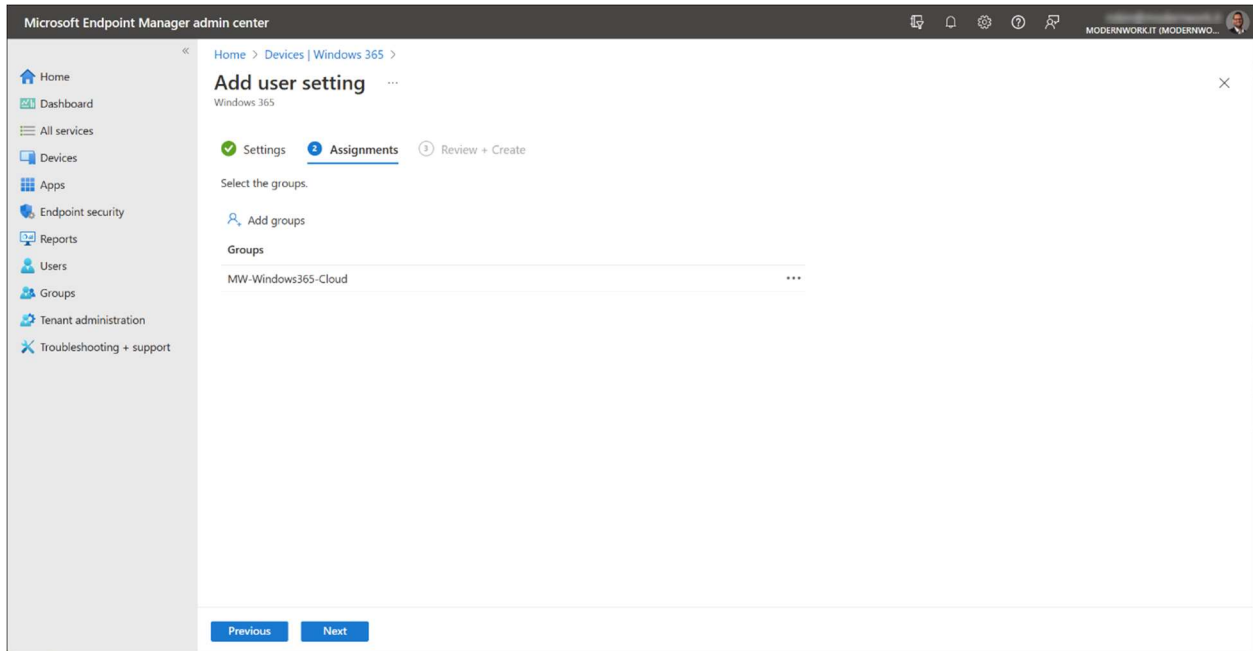
Select an Azure AD user group and click **Next**
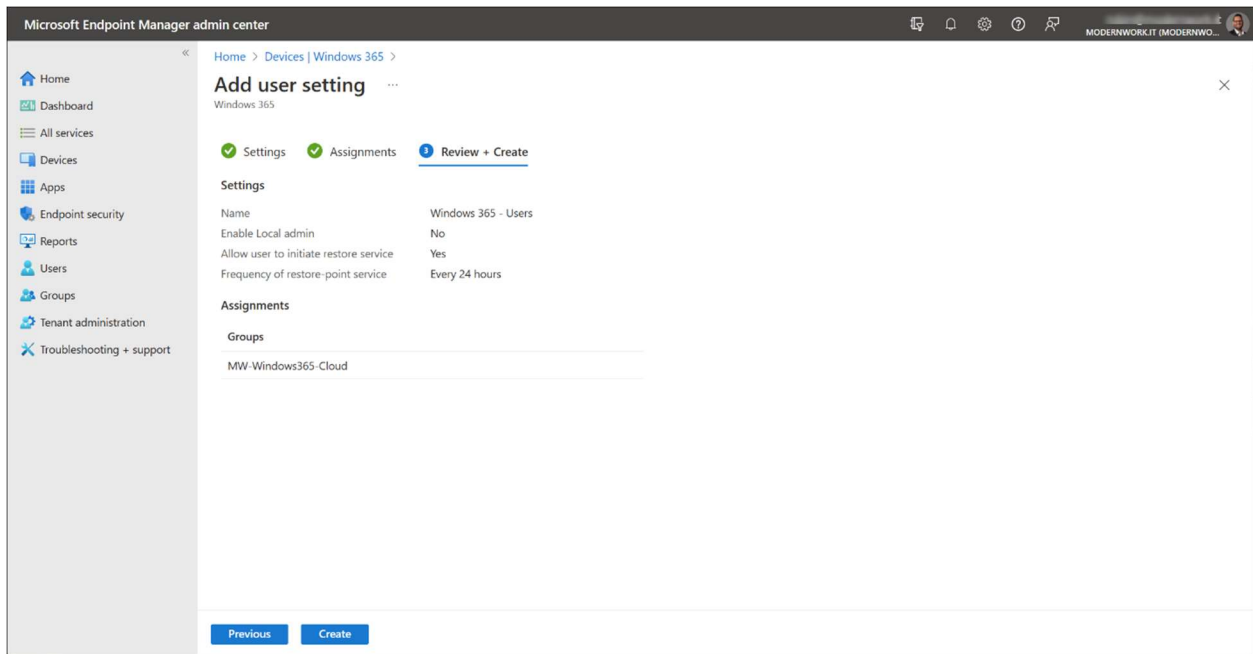
Click **Create**

4 - Create an Azure network connection (optional)

An Azure network connection can be created. This is required if you need a direct connection to your back-end environment without the need of a VPN solution. The

network needs to be already configured in Azure as a vNet. If this is not a requirement you can use the Microsoft hosted network.
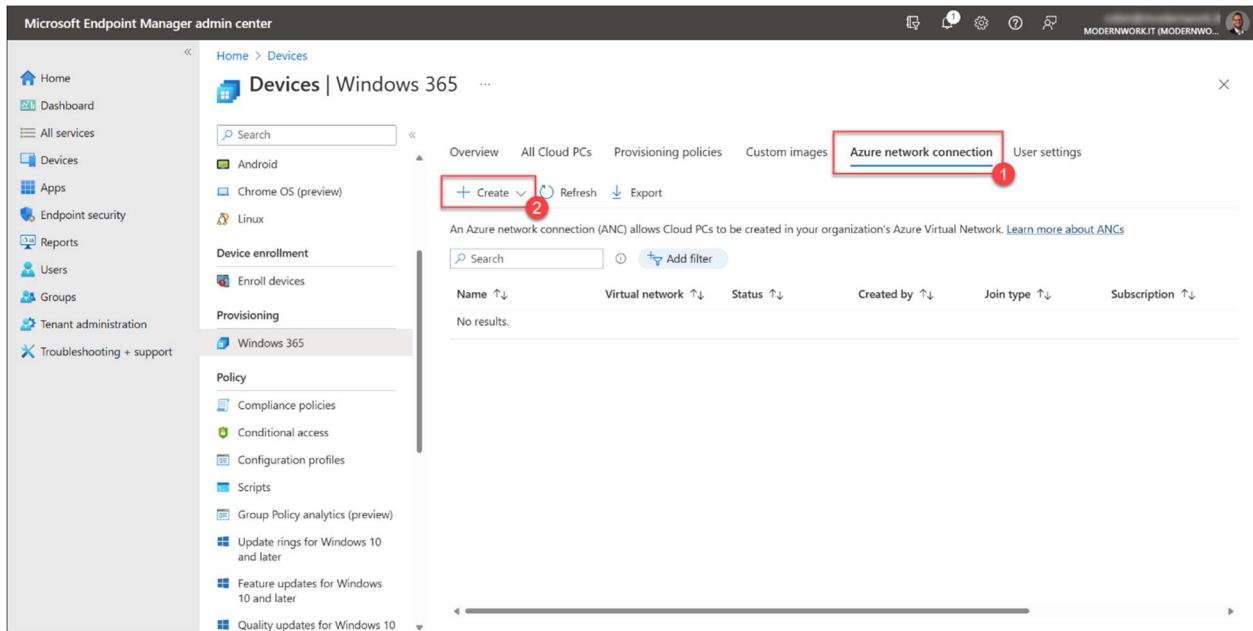
To make an Azure network connection, open the **Azure network connection** tab and click **+ Add** and choose one of the following options.

Azure AD Join: If Azure AD Join only is sufficient.

Hybrid Azure AD Join: If an (local) AD domain join is also required. Be aware that additional Intune and Azure AD Connect configuration is required for Hybrid Azure AD Join.

In this case I will choose for Azure AD Join only.
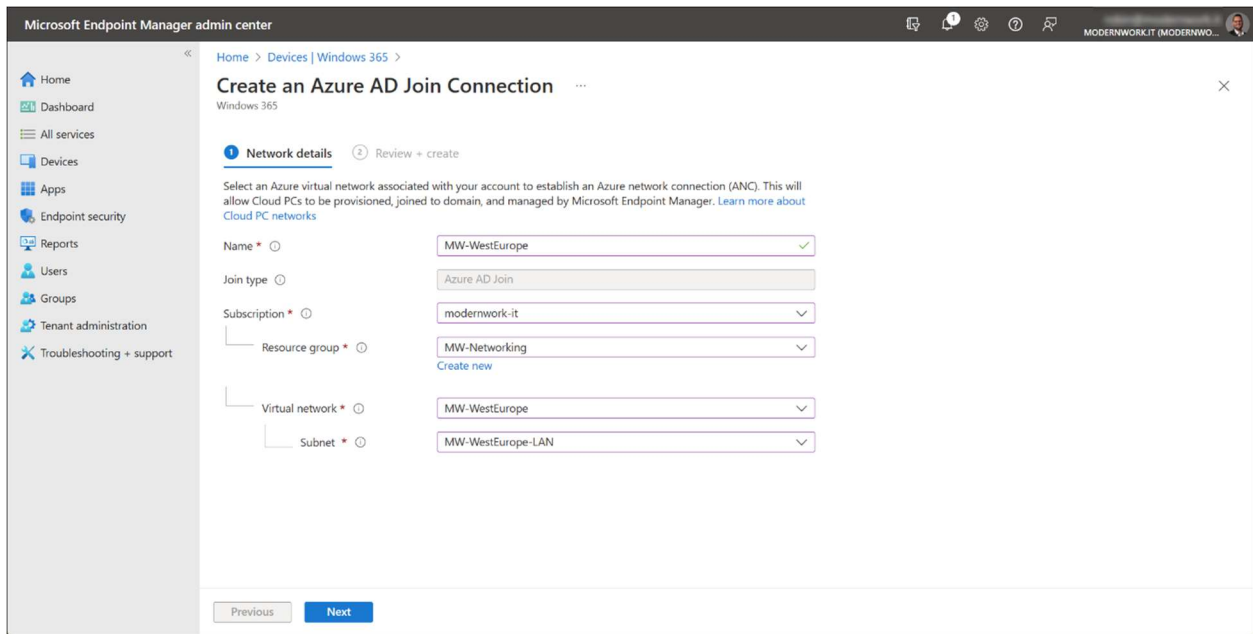
Give the Azure Network connection a **name**. Select your **subscription,** the **resource group** and **virtual network** including the **subnet**.

Click **Next**
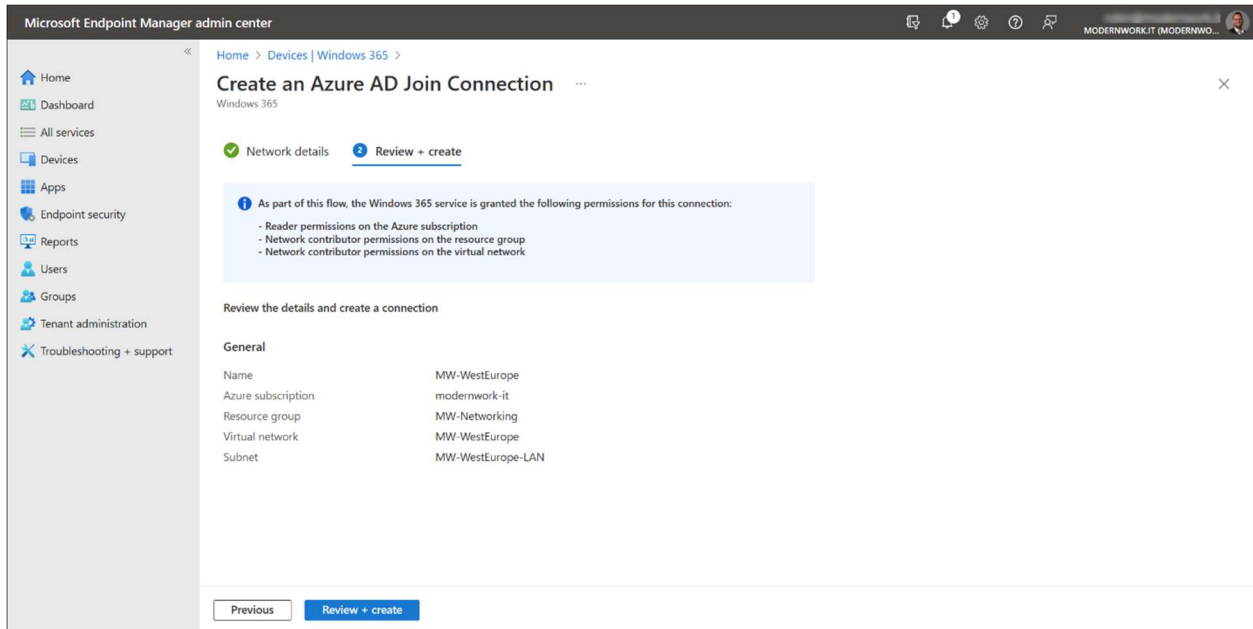
Click **Review + create**
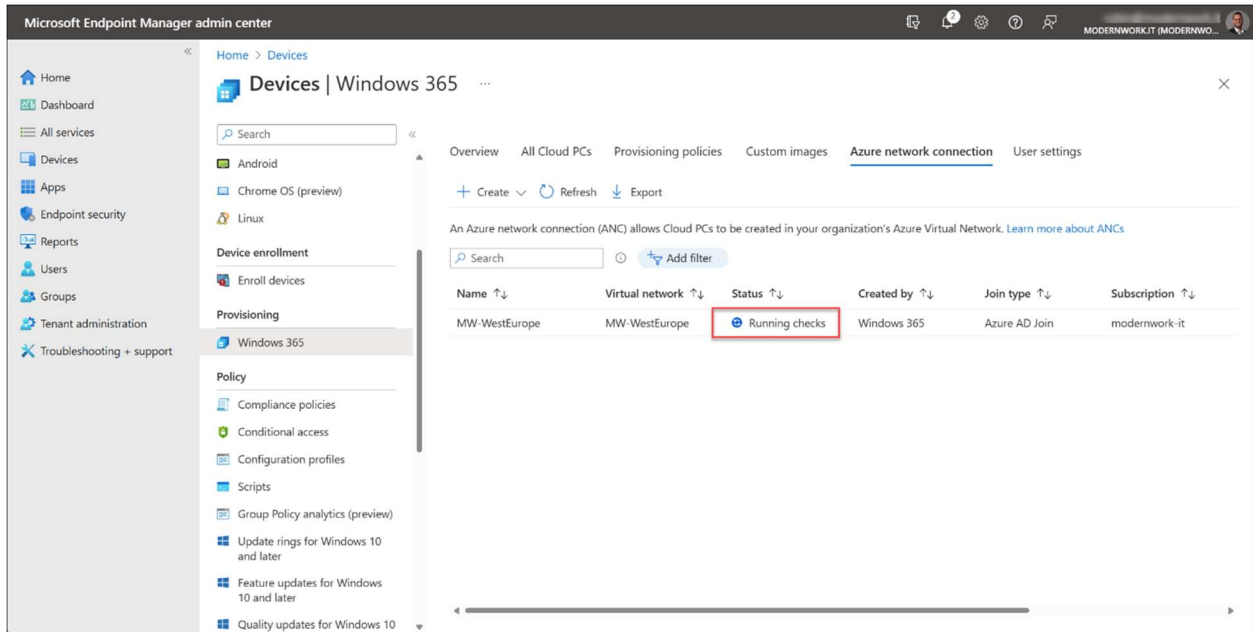
This will start the creation of the Azure network connection within the Microsoft Intune admin center.
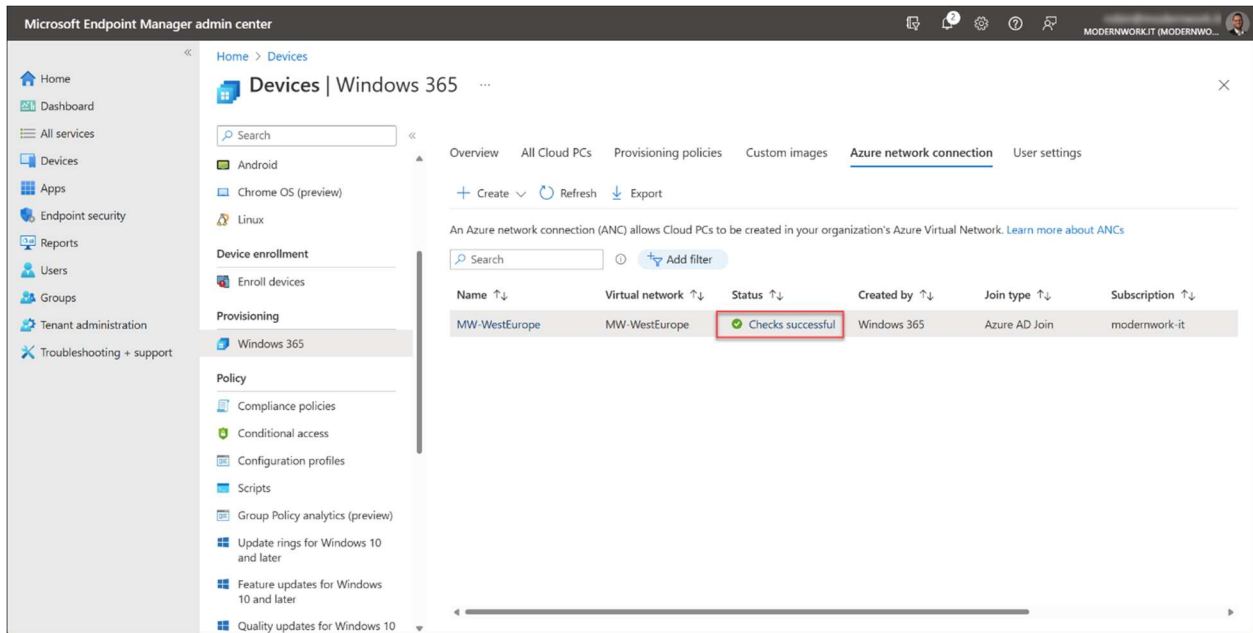
After a few minutes the Azure network connection is created and a "checks successful" status will be displayed (if everything is configured correctly). You can click on the status to get more info.
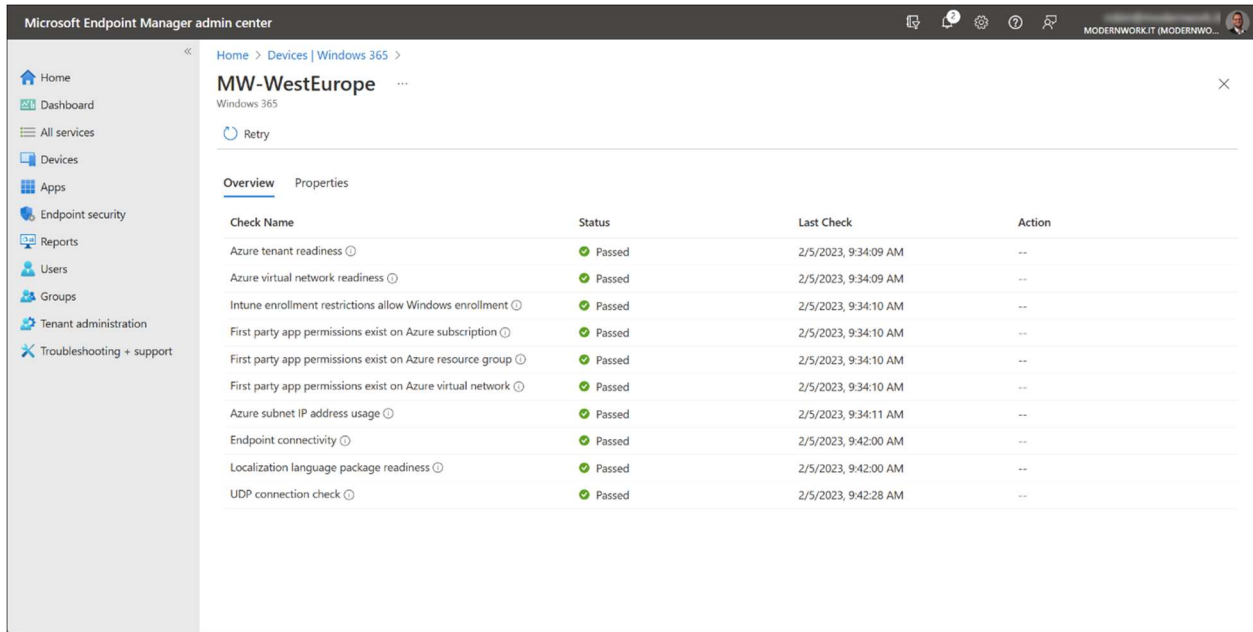
If there is a warning or error you can find more information here.

5 - Create a Custom image (optional)

It is possible to create custom images for deploying the Cloud PCs. However, it is optional and personally I would try to avoid this because image management takes a lot of time and effort. With modern management it is recommended to start with a "clean as possible" installation of Windows 11 were all policies will be applied and all applications will be installed from Microsoft Intune. This gives you the most flexibility, just like with Windows Autopilot.

However, if there is an use case where custom images are useful you have the option to use it. To create a custom image, first a new Virtual Machine needs to be created in Azure. For the next steps go to the [Microsoft Azure Portal](#).
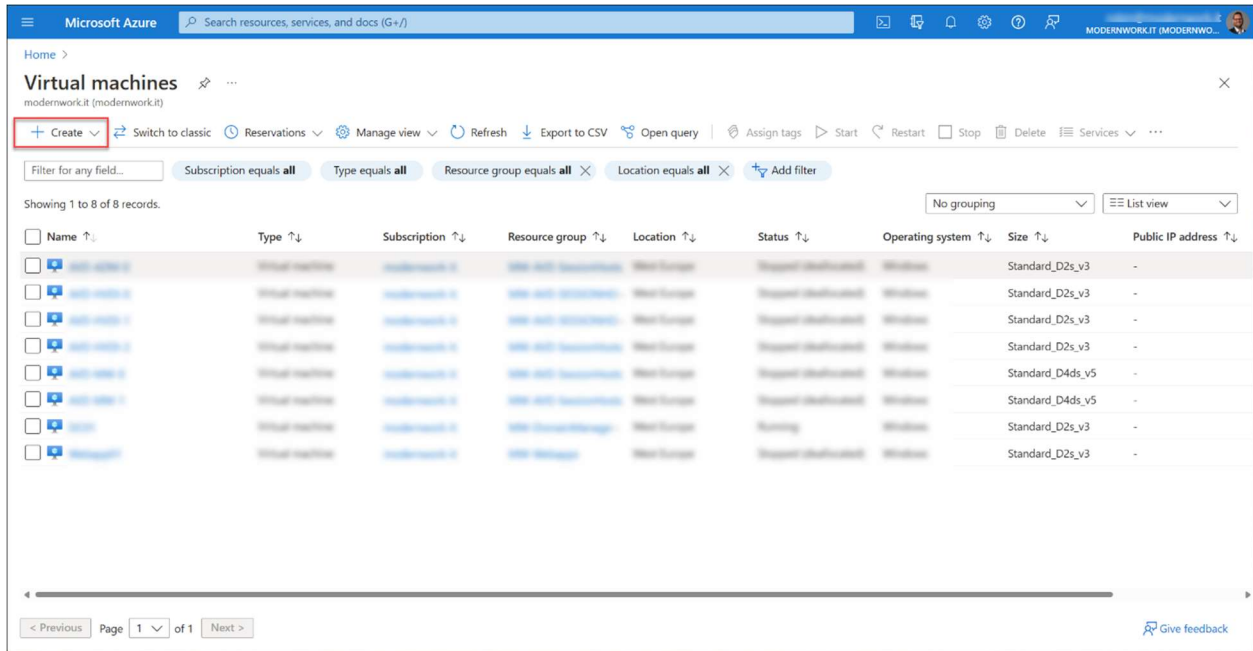
Open the **Virtual Machines** blade and click **+ Create**
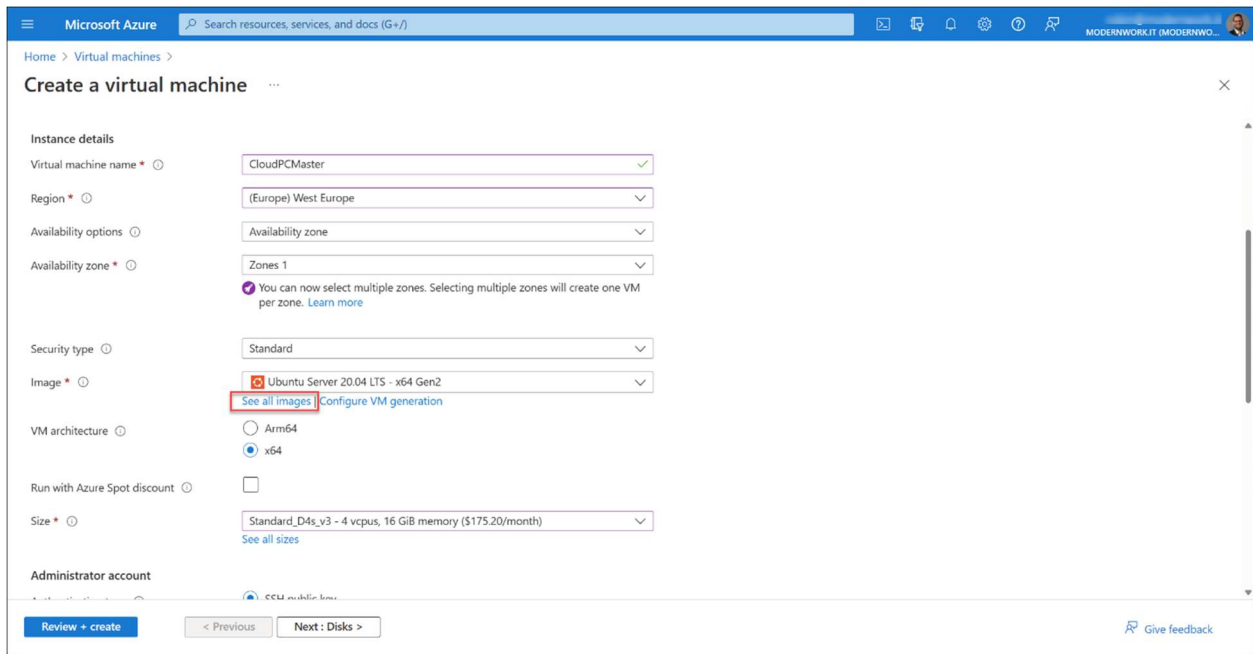
Give the virtual machine a **name**. And select the other required fields like **subscription** and **resource group**. Click **See all images**.

Search for **Windows 365** and click **Select** under **Windows 365 Cloud PC image template**.

Select the image of your choice. Windows 10 or 11, with of without the Microsoft 365 Apps and the build number.

Configure the rest of the settings of the virtual machine. I'm skipping these steps for now and let everything default. Click **Review + create**

Click **Create**.

When the virtual machine is deployed. Connect to it and make all required settings and install all required applications.
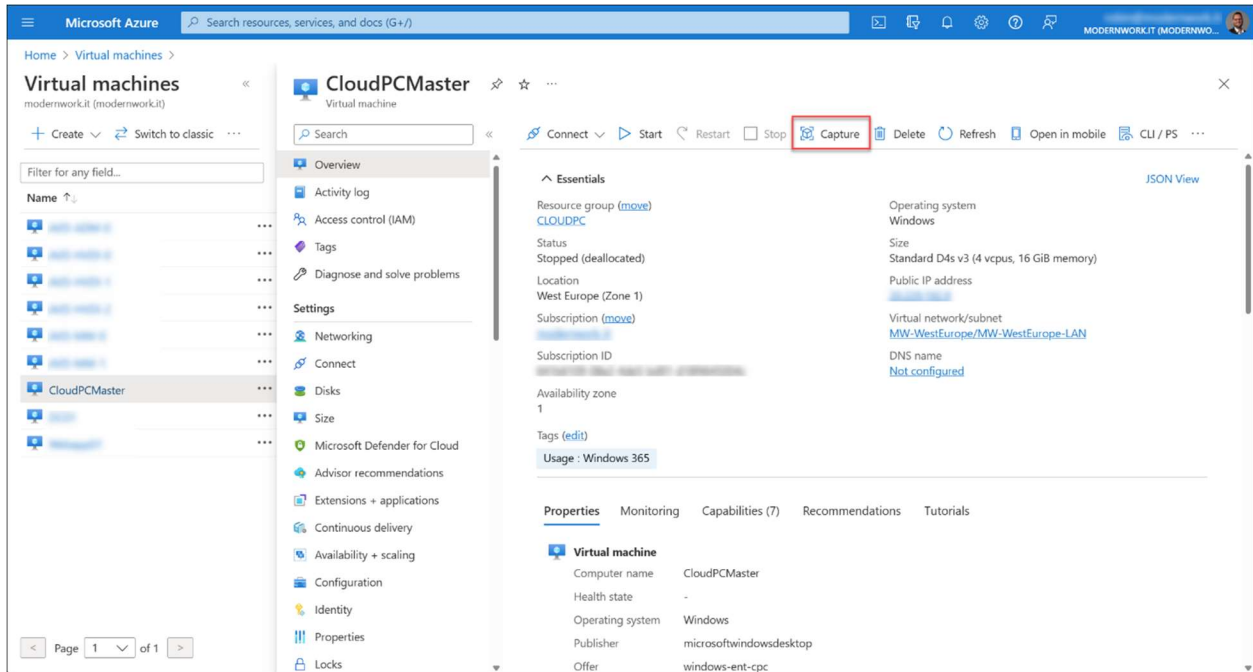
When ready, run **c:\Windows\System32\Sysprep\sysprep.exe**

Select **Enter System Out-of-Box-Experience (OOBE)** as **System Cleanup Action**. Make sure **Generalize** is selected. As **Shutdown Options**, select **Shutdown** and click **OK**.

Once the virtual machine has the **Stopped** status in Azure, deallocate the virtual machine.

Within the Microsoft Azure portal open the **Overview** page of the Virtual Machine and click **Capture**.
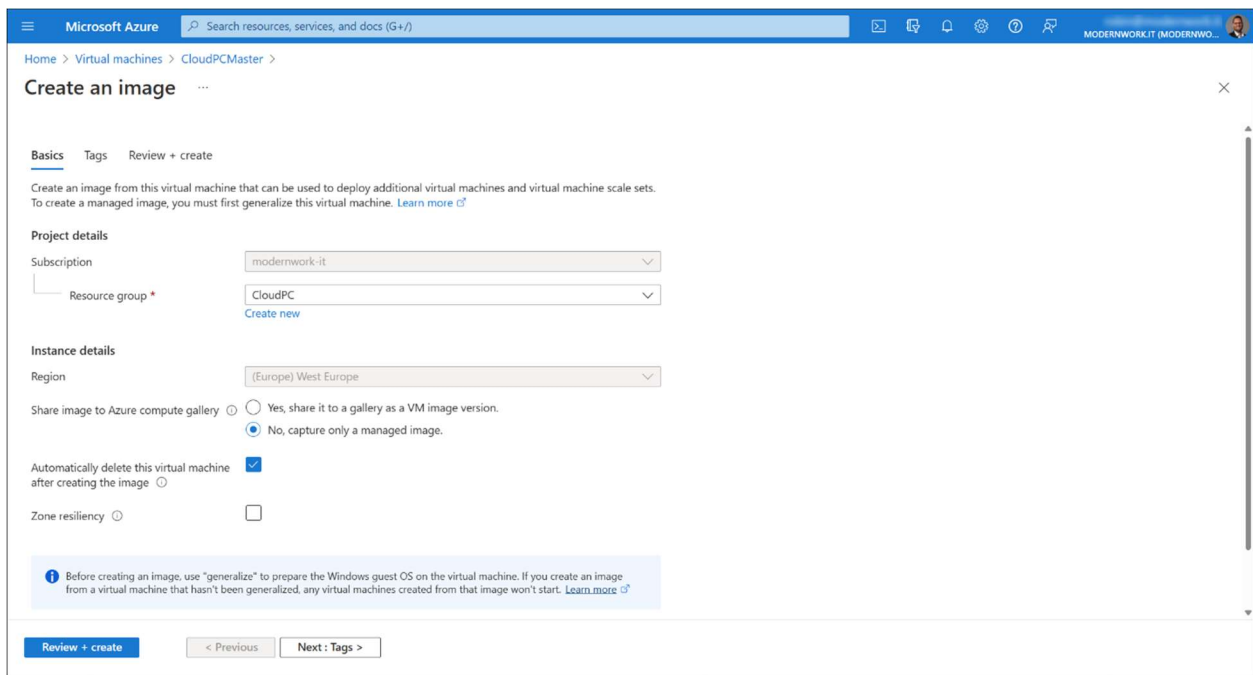
Select the Resource group for the VM capture. You can share this image to a gallery. However, this is not a requirement for Windows 365 Enterprise Cloud PC. For now, I will skip the gallery steps and just store the image in the Azure Resource Group.
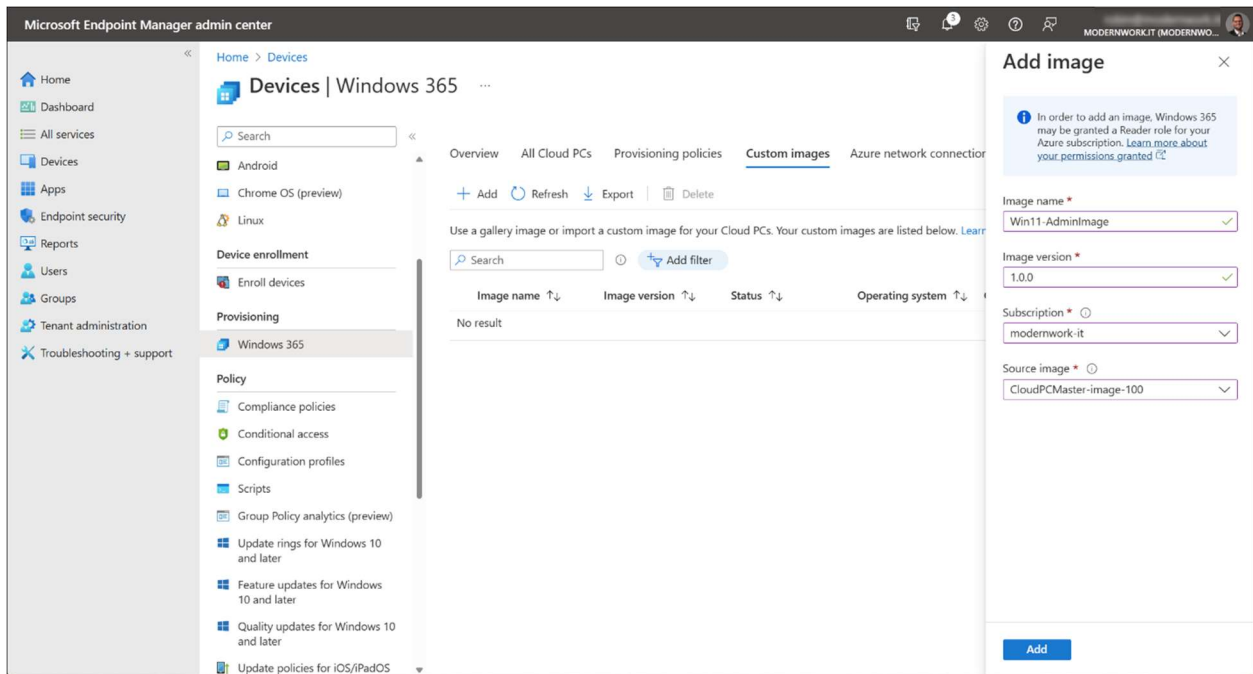
Select **Automatically delete this virtual machine after creating the image** (you can't use the VM anyway since you run Sysprep). Give the image a **Name** and click **Review + Create**.
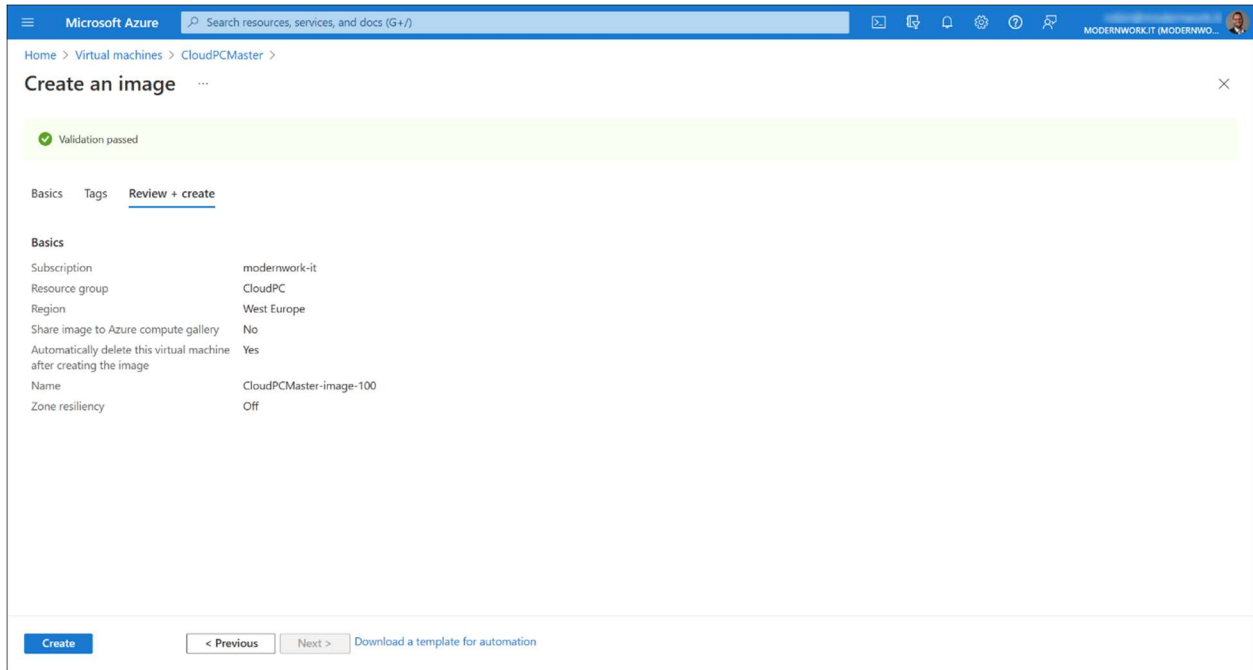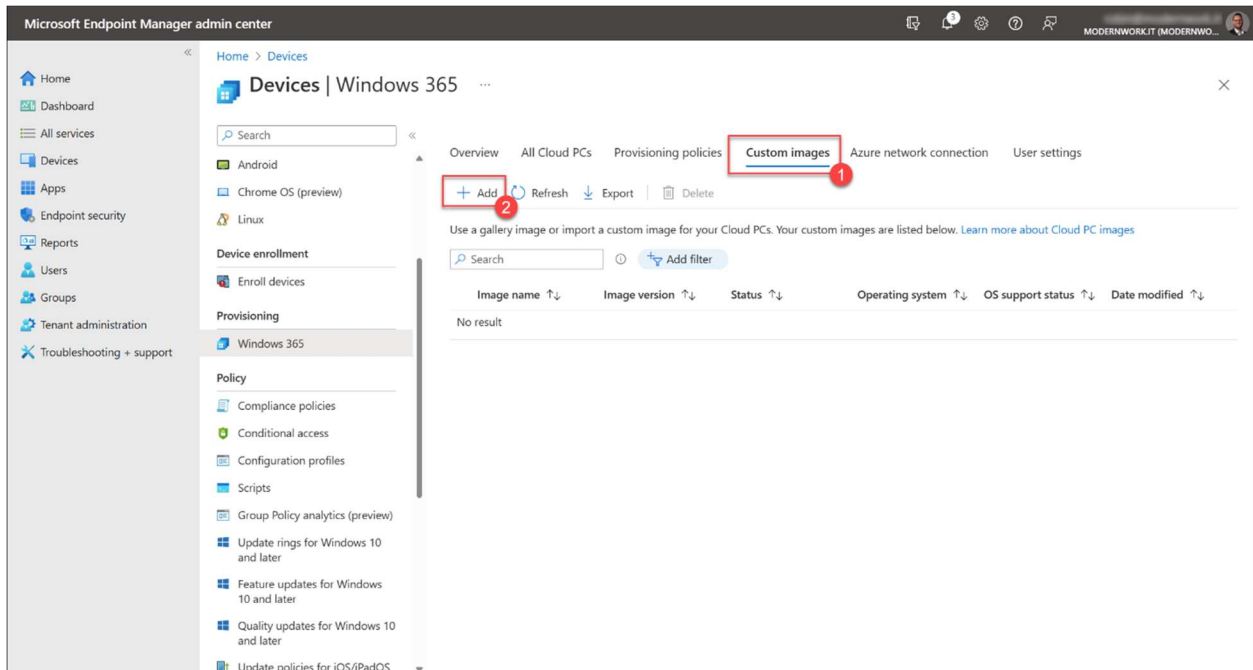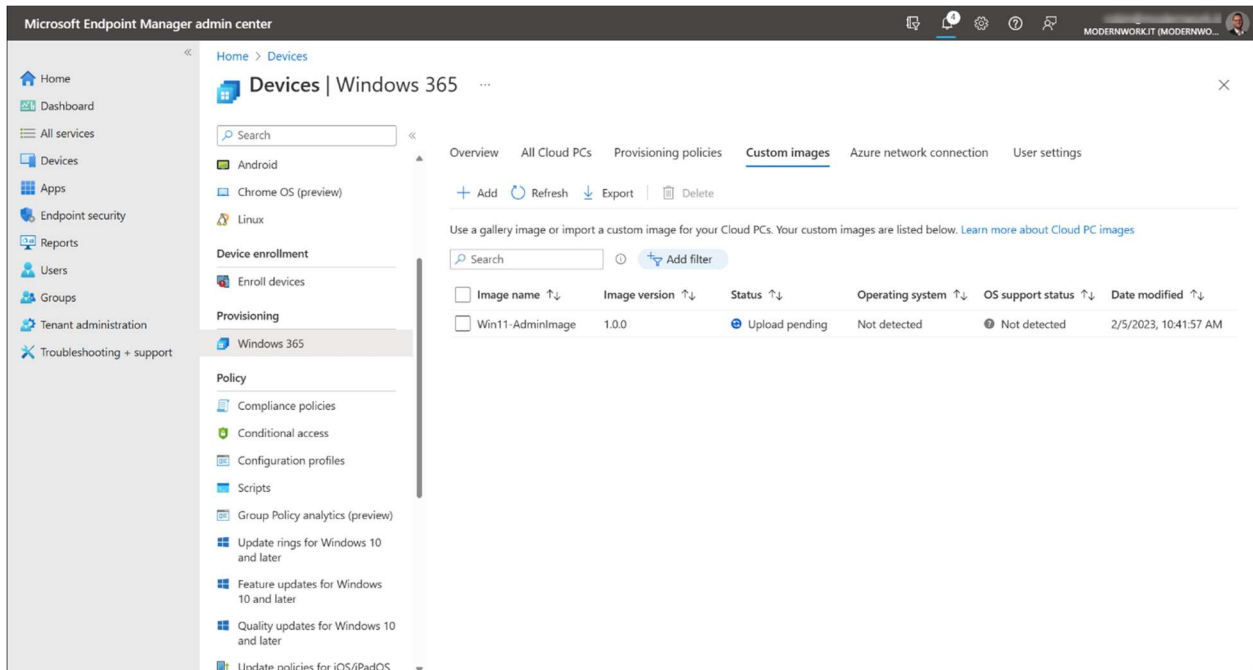

Click **Create**

Go back to the Microsoft Intune admin center, click **Custom images** and click **+ Add**.
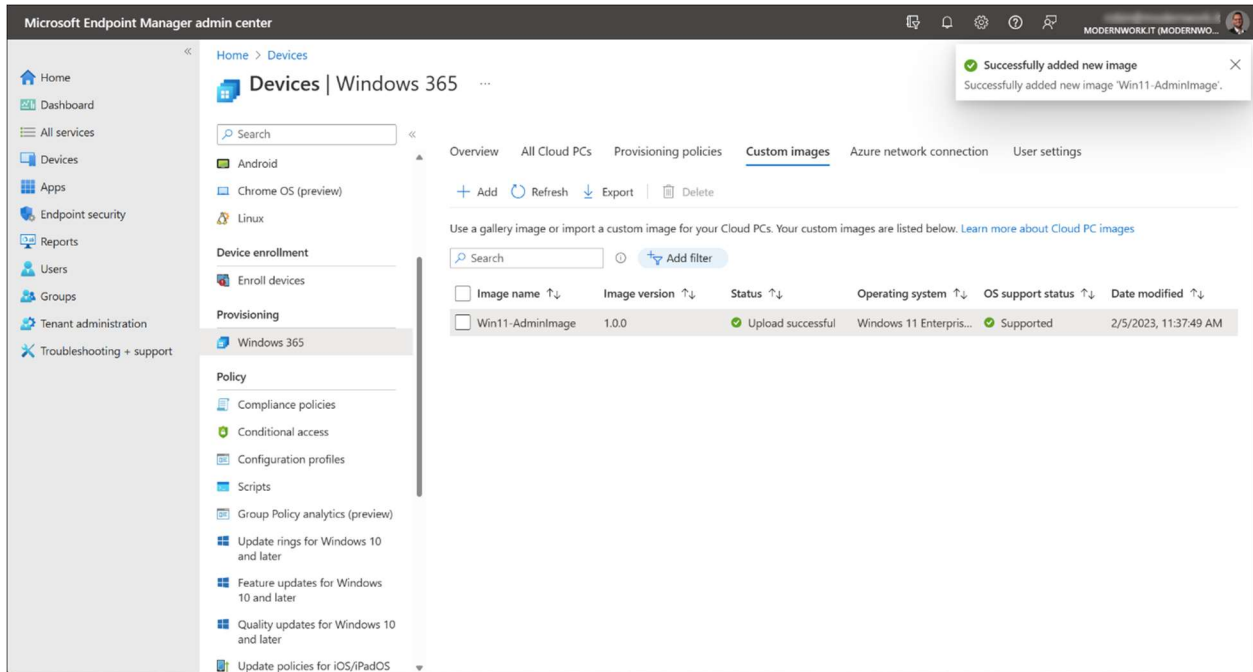
Give the image a **Name** and an **Image version**. This must be in the "x.x.x" format, so for example, 1.0.0.

Select the subscription. The just created image will be selectable in the pull down menu. Click **Add.**
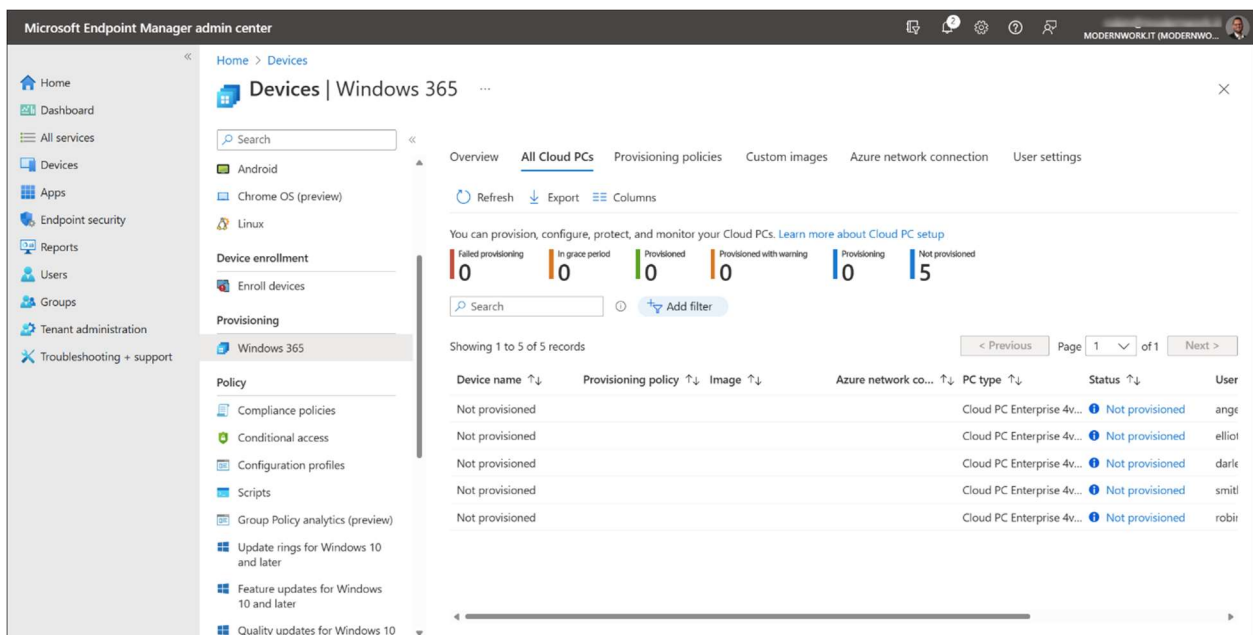

The upload will now start, this may take a moment.

After the upload is complete, the status will be changed to "Upload successful".

6 - Create a Provisioning Policy

A Provisioning Policy needs to be created to provision the Cloud PC with an image of choice. You can create multiple Provisioning policies and assign them to different Azure AD security groups.

As you can see in the screenshot above, no provisioning policies have been created and assigned. The Cloud PCs all have the status "Not provisioned".
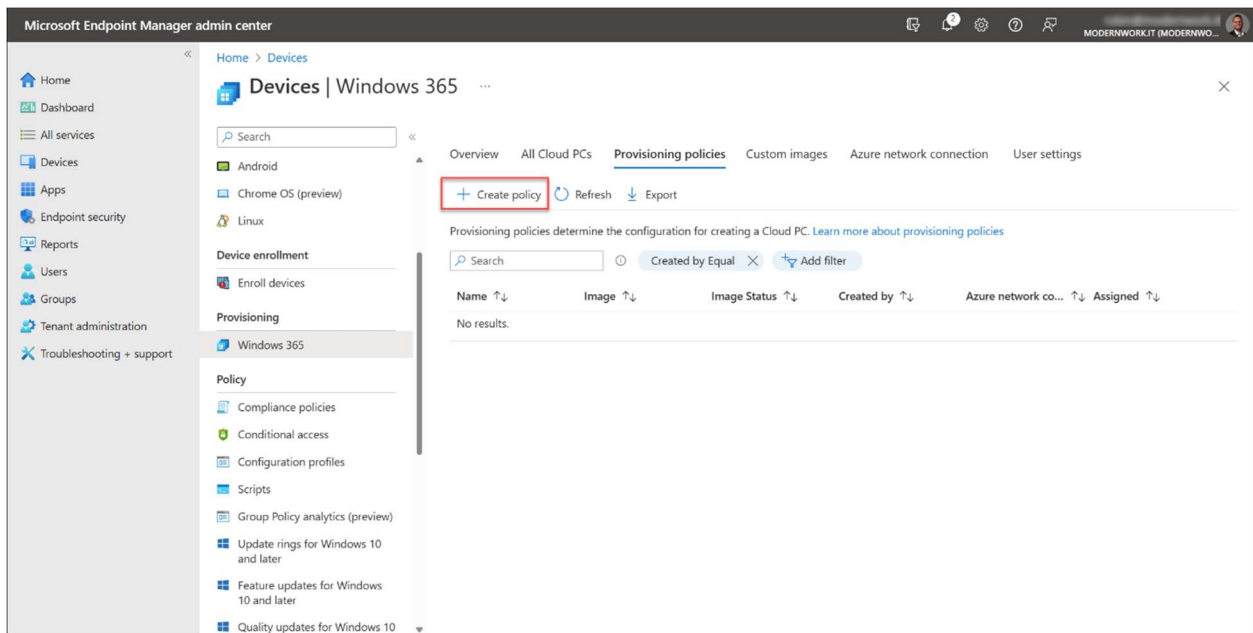

Open the **Provisioning policies** tab and click **+ Create policy**
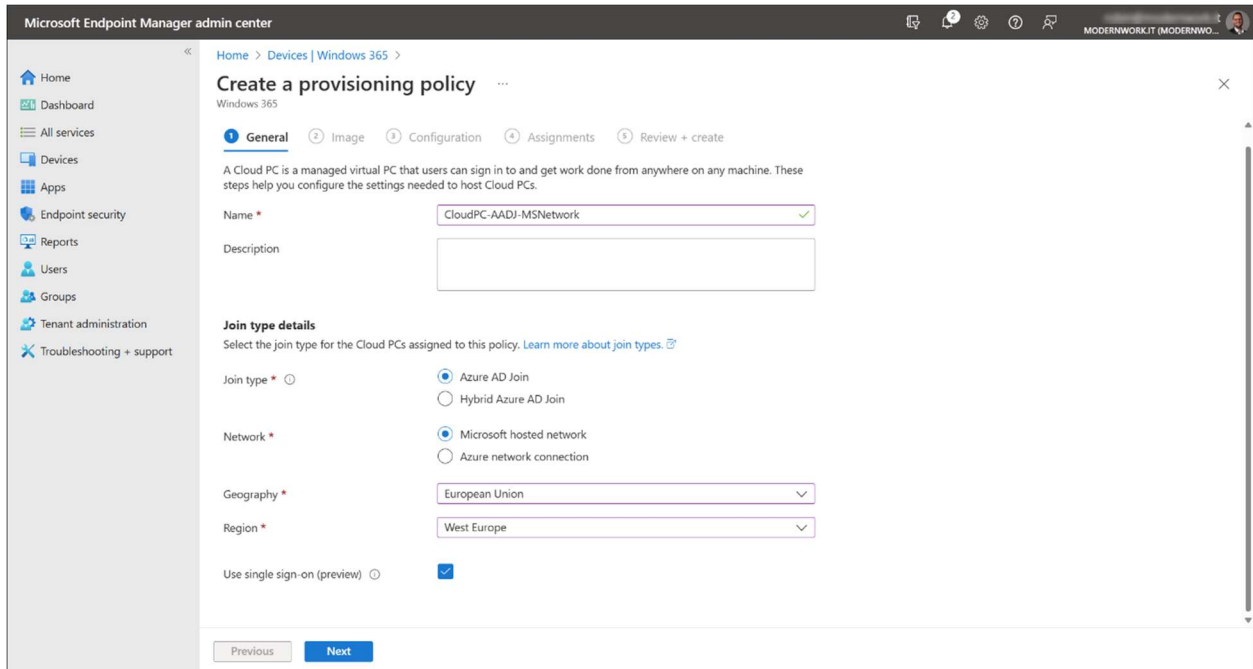
Give the policy a **Name** and select the **Join type**. Azure AD Join or Hybrid Azure AD Join. For **Network**, select the **Microsoft hosted network**, or an existing **Azure network**

connection (see previous steps). When you select the **Microsoft hosted network**, make a selection of the **Geography** and **Region**.

Select **Use single sign-on** and click **Next**
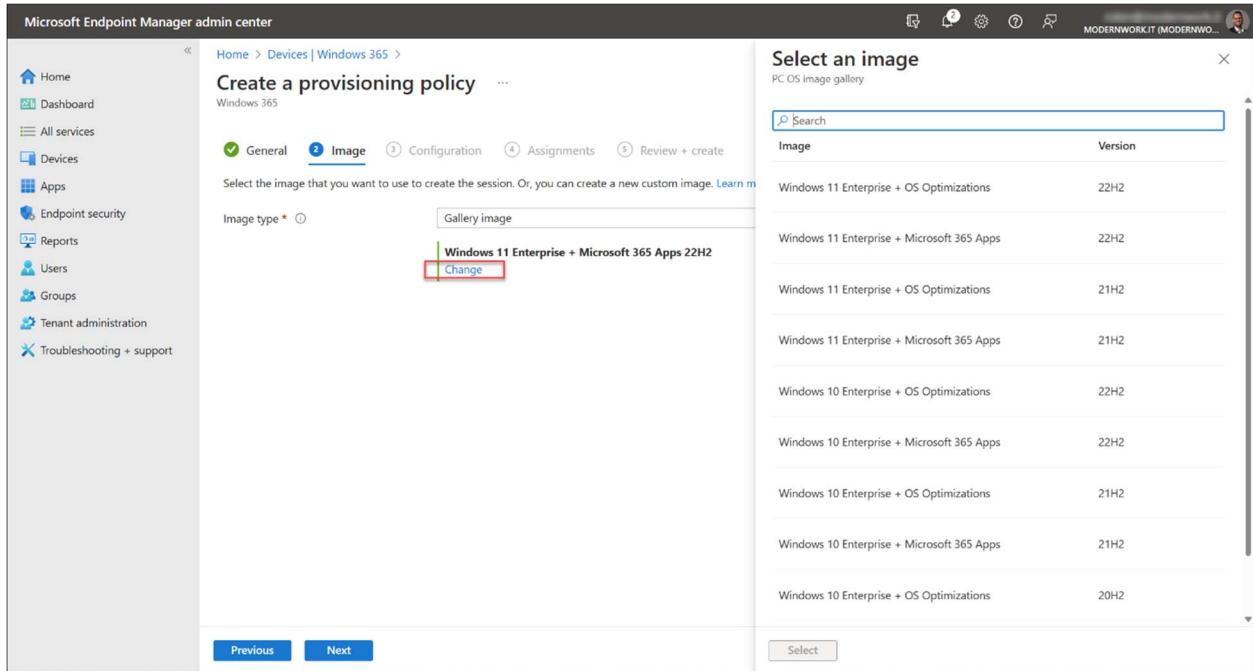
Select an image from the Gallery image or a custom image. When you choose **Gallery image** you have the choice for Windows 10 or 11, with or without the Microsoft 365 apps and the version/build.
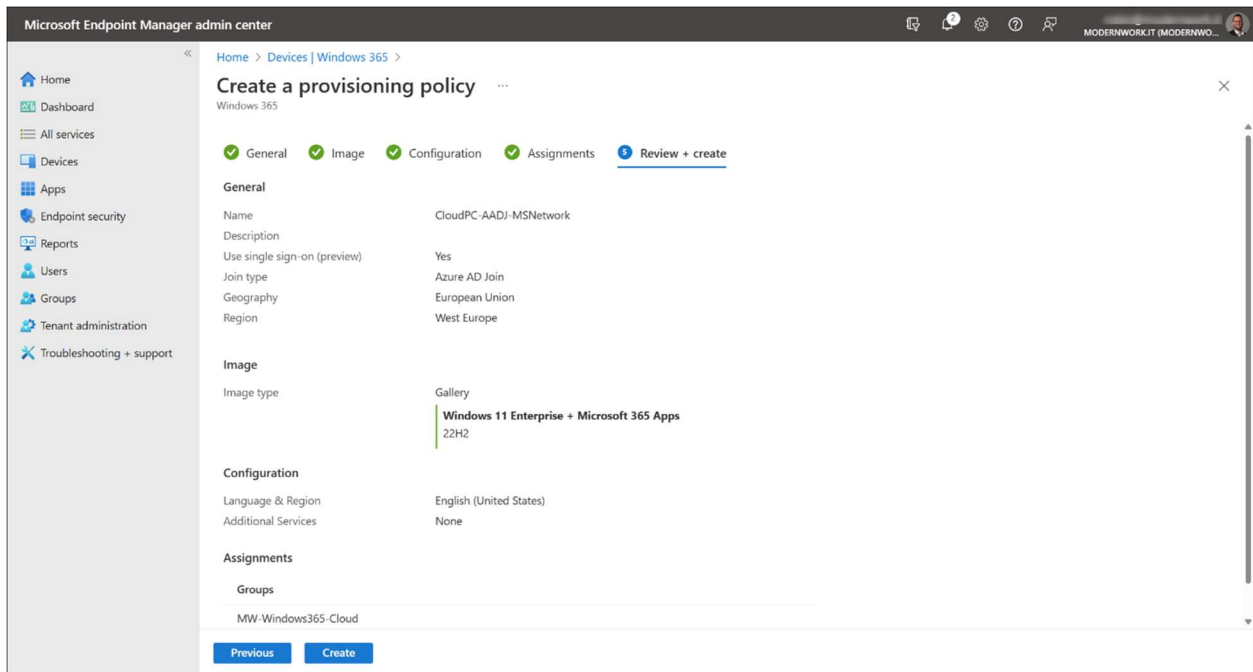
Select the image of choice and click **Next**
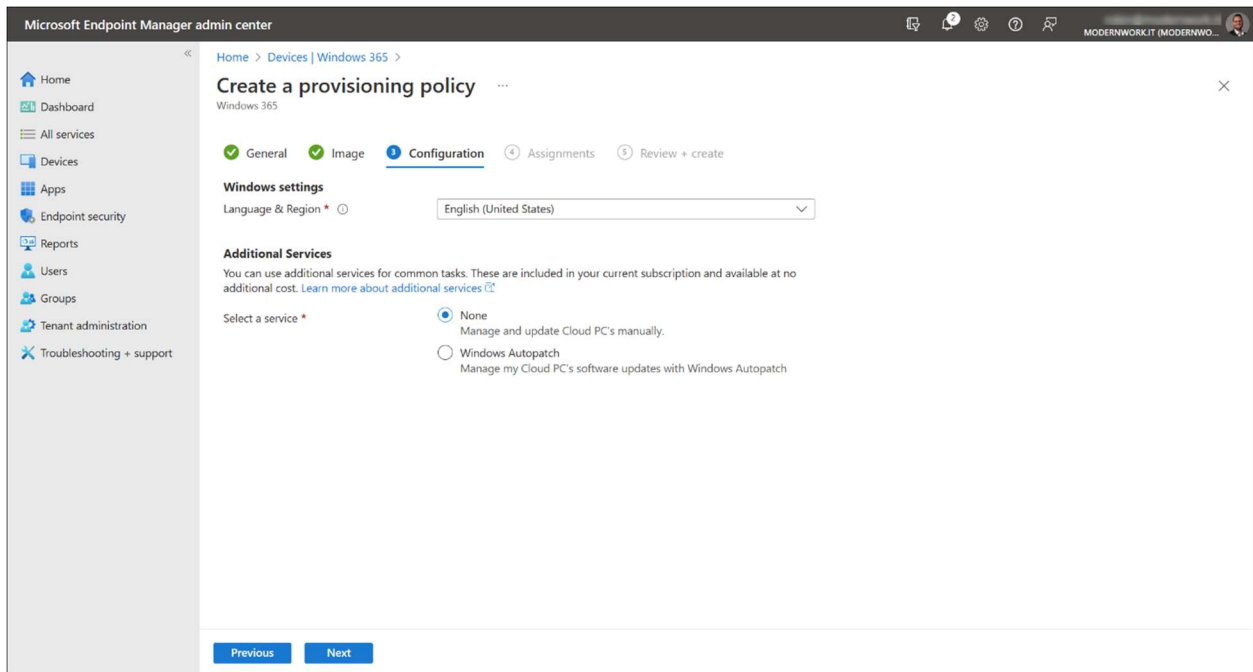
Select the **Language & Region** of your choice and the way you want to update the Cloud PC. This can be manually (via Windows update policies in Microsoft Intune) or via the [Autopatch service](#).
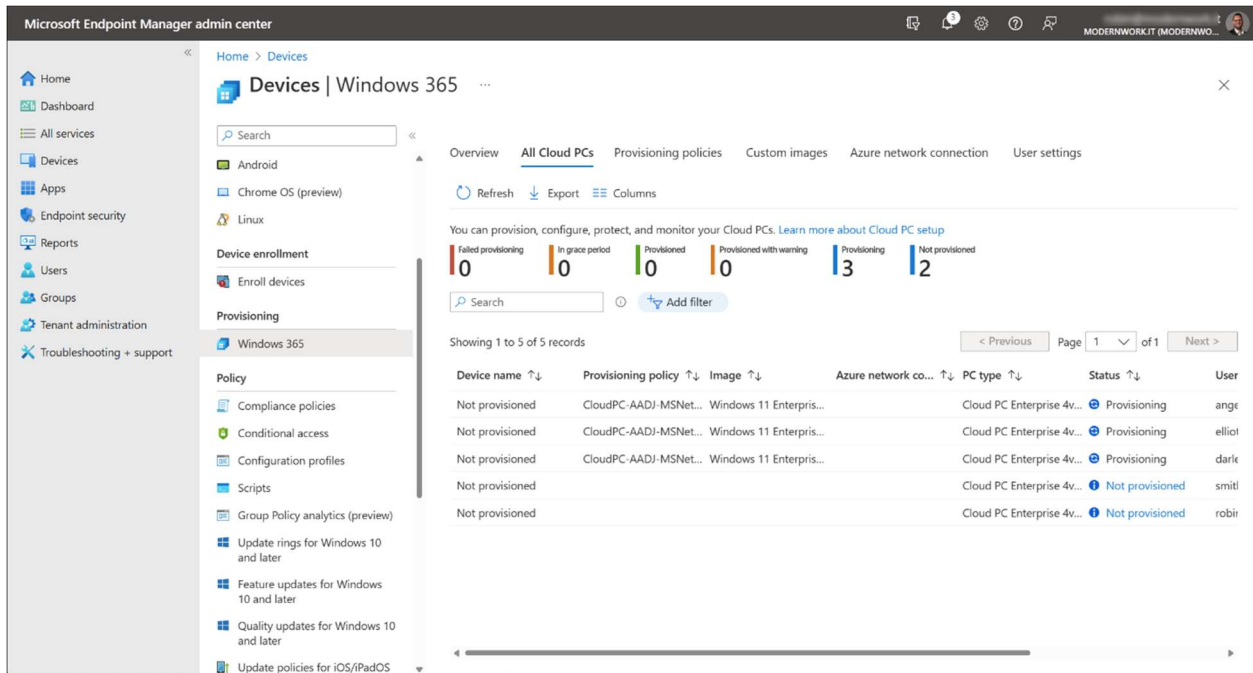
Click **Next**
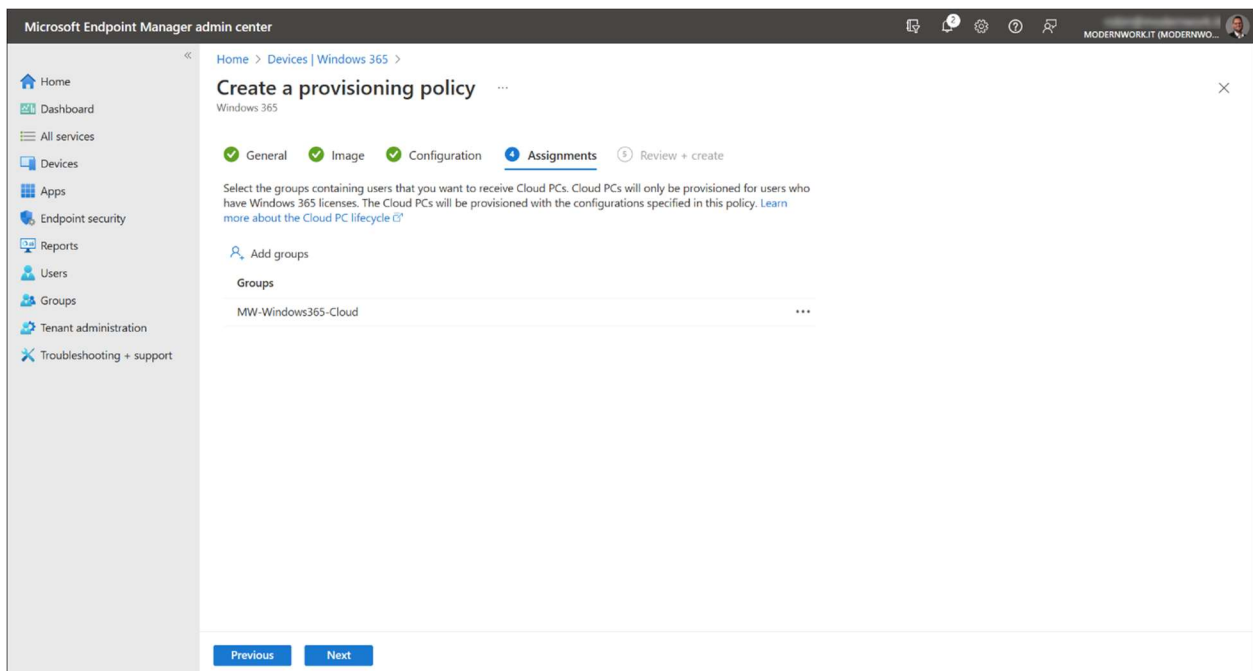
Select an Azure AD security group and click **Next**.

Click **Create**

After the provisioning policy is created, Cloud PCs of assigned users will be provisioned. After the provisioning is finished, the status will be changed to "Provisioned" and the Cloud PC is ready to use.

7 - Connect to the Windows 365 Cloud PC

Let's connect to the Windows 365 Cloud PC. You can use different clients for this, depending on the operating system you are using on the (local) client. First, lets use the web client. Navigate to https://windows365.microsoft.com/
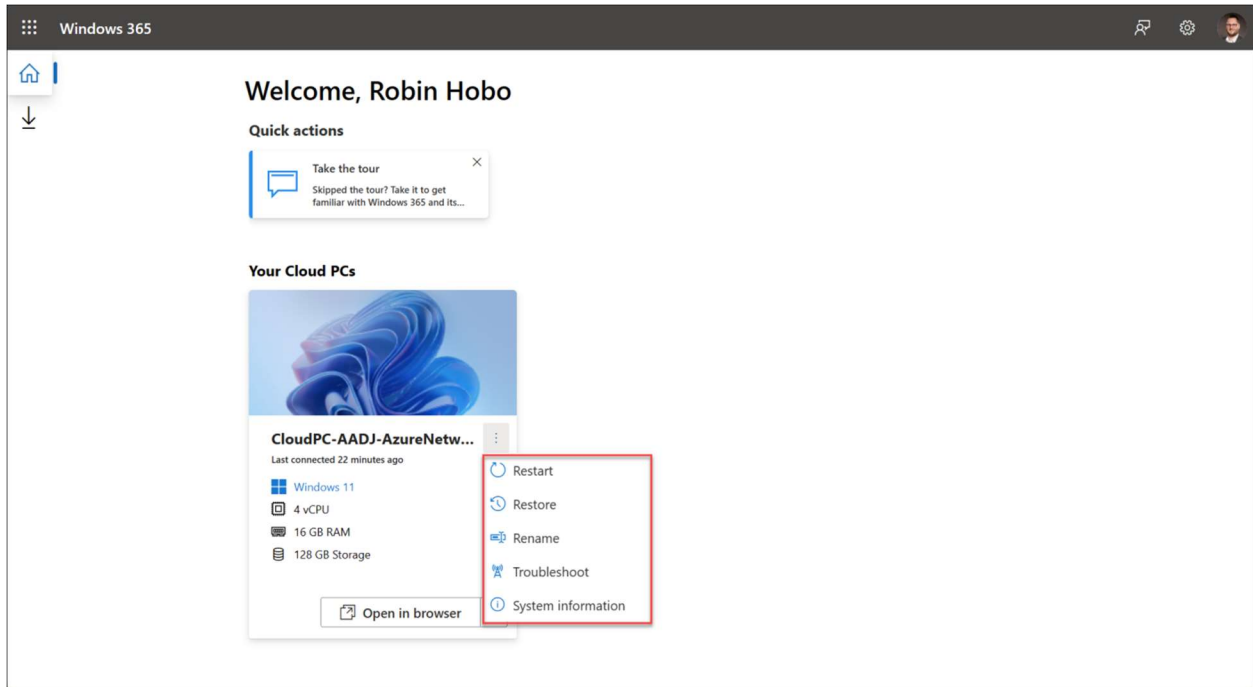
After signing in, you will see your Cloud PC. There are options for the user to restart, restore the Cloud PC and some other options from this web interface.
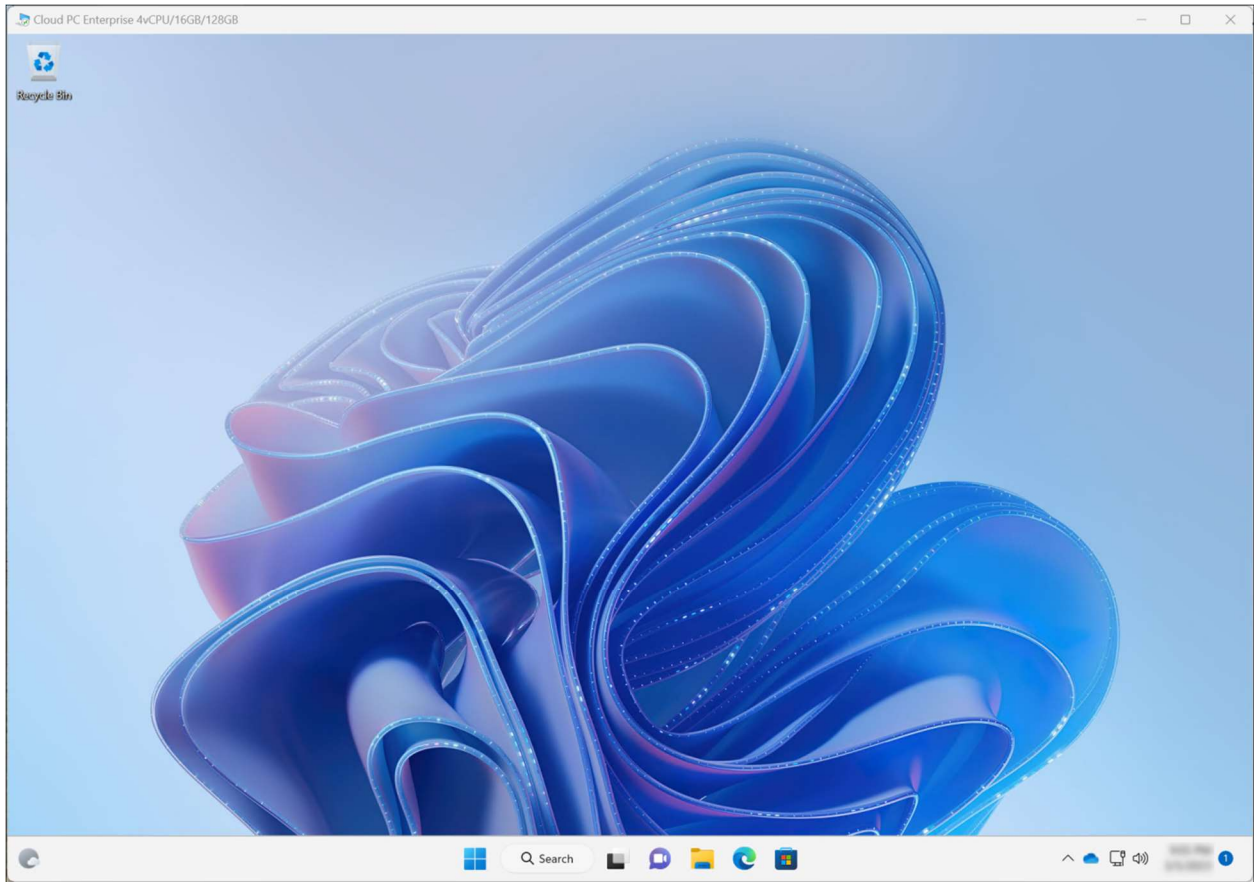
When opening the **Remote Desktop Clients** page, you can find the download links and information to all other available clients.
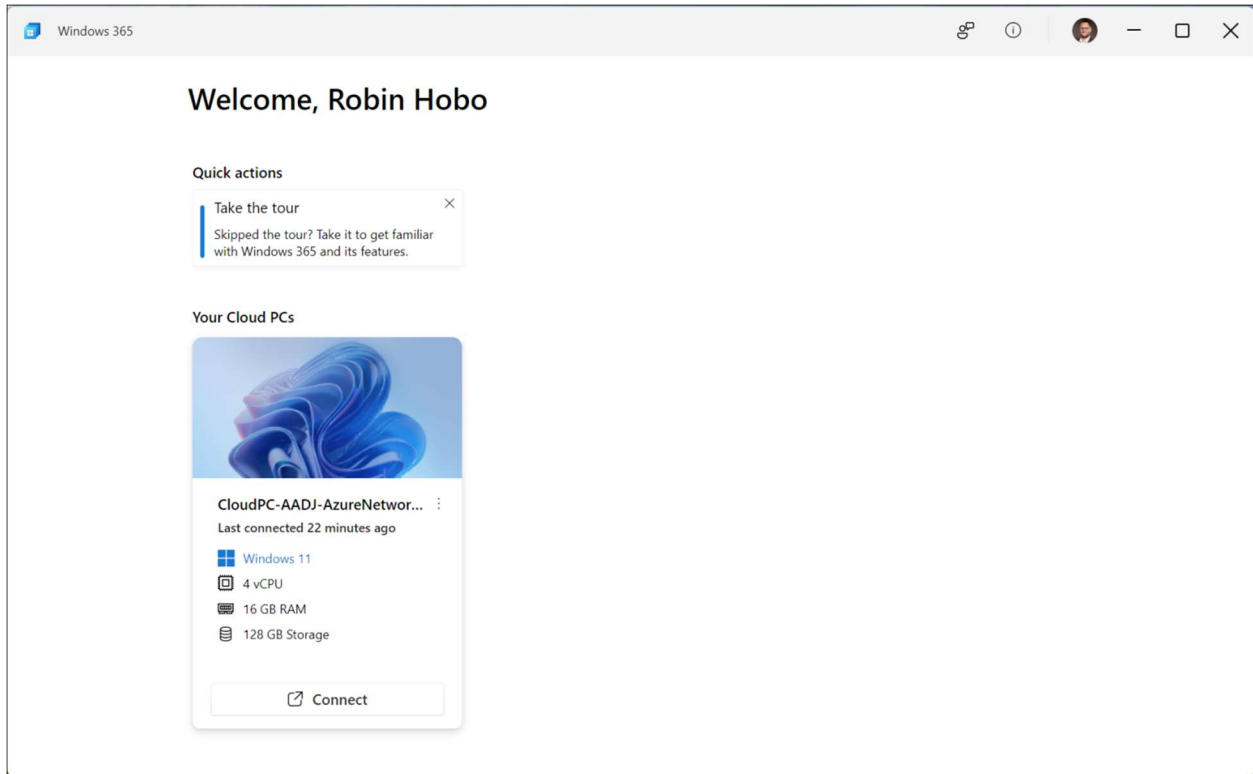
For example the new Windows 365 for Windows app you can download straight from the Windows store.

Click **Connect**

In a few second you have access to your Windows 365 Cloud PC.