LAB 2: Identity management

Contents

Introduction to LAB 2

In this LAB, you will register a public domain and then add it in Office 365. Then you will create (and delete) users and groups using various methods. Finally, you will enable and configure multi-factor authentication and conditional access policy in order to harden the security of the accounts in your tenant.

Exercise 1: Add a domain to Office/Microsoft 365

Register a public domain name

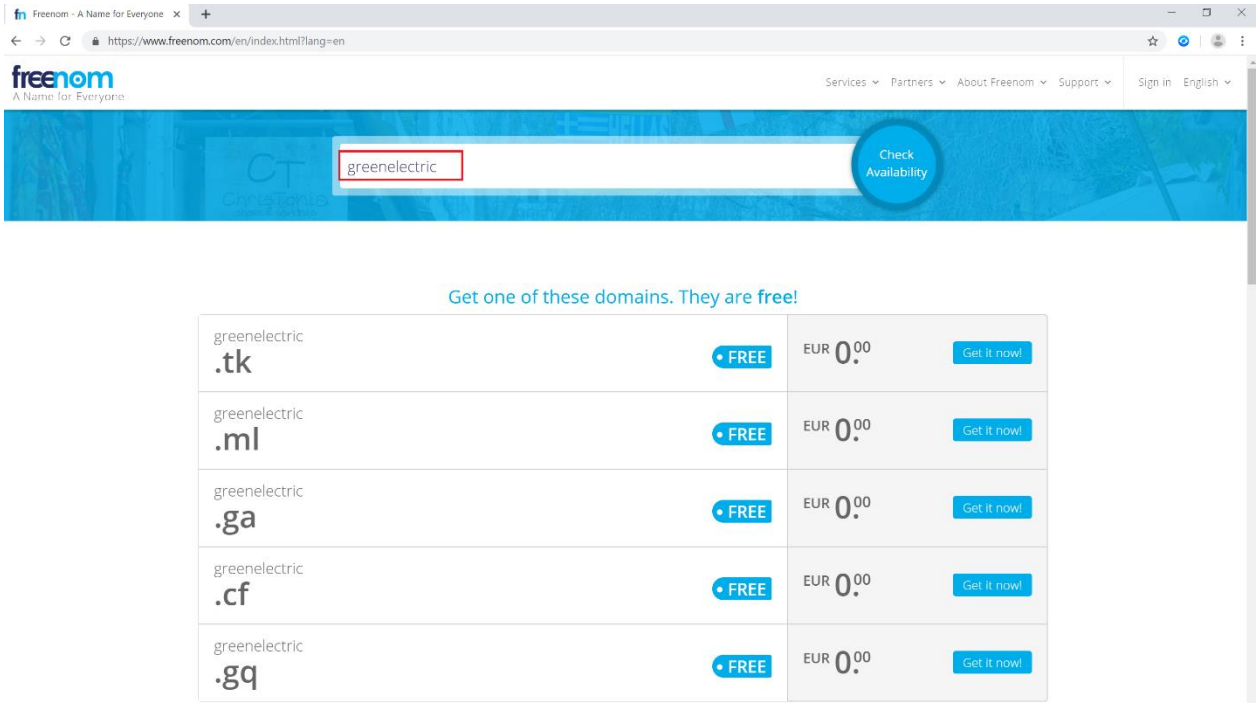
Remember that when you created your tenant, the associated default domain was in the format of **something.onmicrosoft.com**. This means that the users that you create later are in the format of **user@something.onmicrosoft.com**. In most situations, this doesn't look very pretty for the domain owners and they want to have their own, custom domain added in Office/Microsoft 365. For example, if

you add the domain **mydomain.com** in your tenant, the users that you create later can be in the format of **user@mydomain.com**.

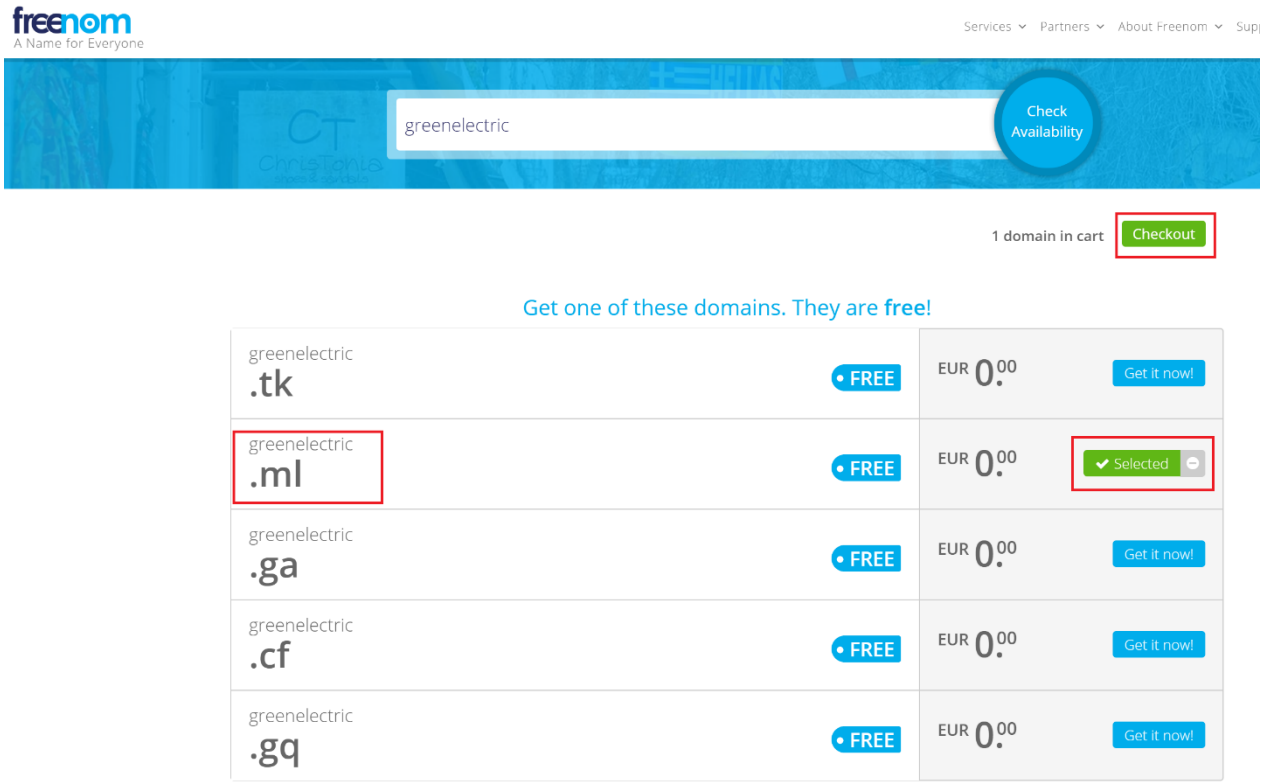
That is why we first want to register our own domain. The options to choose from "domain register" company/portal are a lot, so you can select the best one according to your preferences and the price, of course. There are also free domain providers, which gives you, in most of the cases, either a third level domain (like **mydomain.something.com**) or a second level domain with not very popular suffixes, like **mydomain.ga**, **mydomain.ml**, **mydomain.tk**, **mydomain.cf**, etc.

The instructions below will describe how to register and use a domain using **Freenom** – one of the free domain registers. Please note that there is no guarantee that it will work smooth and clear (since it is free) every time and for everyone. You can use any other service (free or paid) to register a domain.

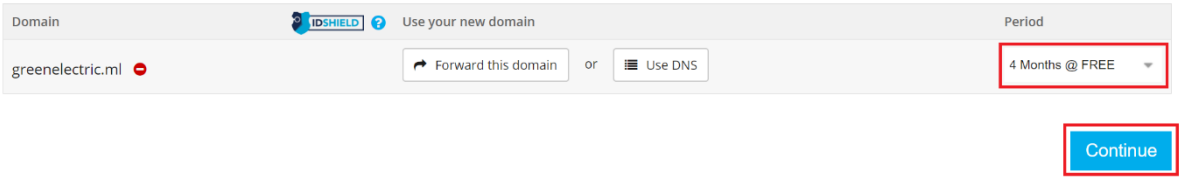
1. Go to https://www.freenom.com/
2. In the center of the page enter something which is similar to your desired domain name and click Check Availability to see the list of suggestions. In this example, we enter the word "greenelectric". After clicking on Check Availability, the result is:



3. As you can see, we have been offered with 5 options for free domains containing our keyword **greenelectric**. We will choose one of those, **greenelectric.ml**, and will click on Get it Now! Button and then go to Checkout



4. On the next step, we select the Period for this domain and click on Continue. Several months is OK but choose whatever you prefer.



Note: Due to the free of charge services and the huge number of registered domains every day, the **Freenom** service may periodically check if this domain is really used and may cancel it if not. Again, there are no guarantees, but if you want your free domain to last during the entire period, you need to point it to a

web service (so in the above example, when you type **greenelectric.com** and **www.greenelectric.com** in the browser, it goes to a web page, whatever it is in this page). This lab guide does not provided instructions on how to point your domain to a web service, since there are many options and it is out of scope. The bottom line is that you can leave your domain like this, but just be prepared that it can be cancelled – this is not a big issue, since you can always register another domain or simply work with users in the original, default domain (**user@something.onmicrosoft.com**).

5. Next, put your email address for verification and account creation. Click on Verify my email address, go to your email and confirm the link.
6. The confirmation link from the email will open the Freenom's Review & Checkout page. Fill in your details and click Complete Order.

Description	Price
Domain Registration - greenelectric.ml	€0.00EUR
Subtotal:	€0.00EUR
Total Due Today:	**€0.00EUR**

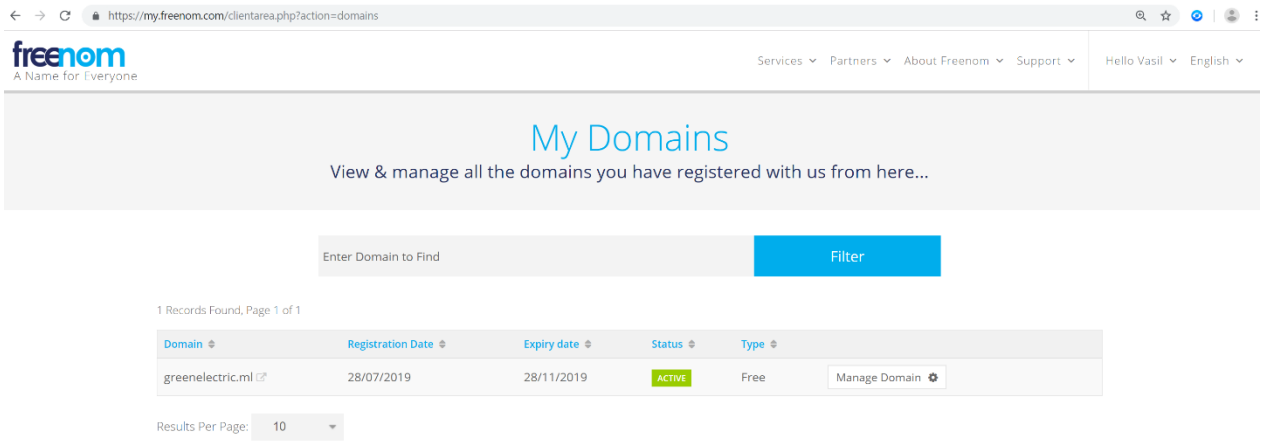
Your Details

First Name	Vasil
Last Name	Yordanov
Company Name	
Address 1	Sofia
Zip Code	1000
City	Sofia
Country	Bulgaria
State/Region	Sofia
Phone Number	+359
Email Address	@abv.bg Change
Password	••••••••••••
Confirm Password	••••••••••••

Tax may be charged depending upon the state and country selections you make. Click to recalculate after making your choices. Update

I have read and agree to the Terms & Conditions **Complete Order**

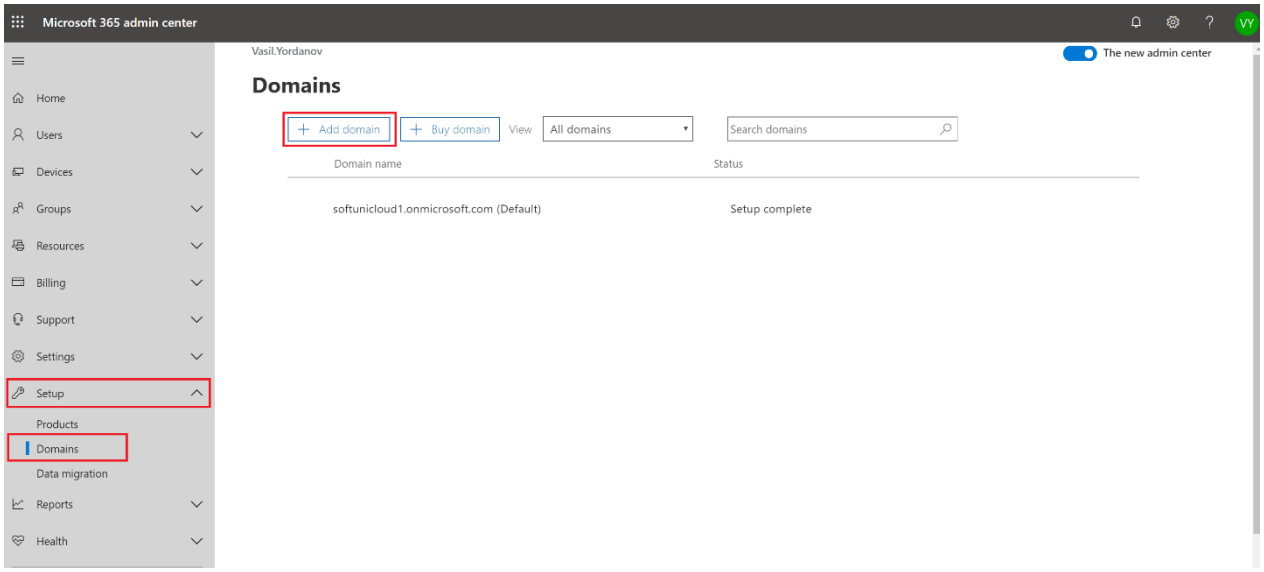
7. Congratulations! You now have a domain name. To see it, log in to https://freenom.com (if not already there) and navigate to Services -> My domains.



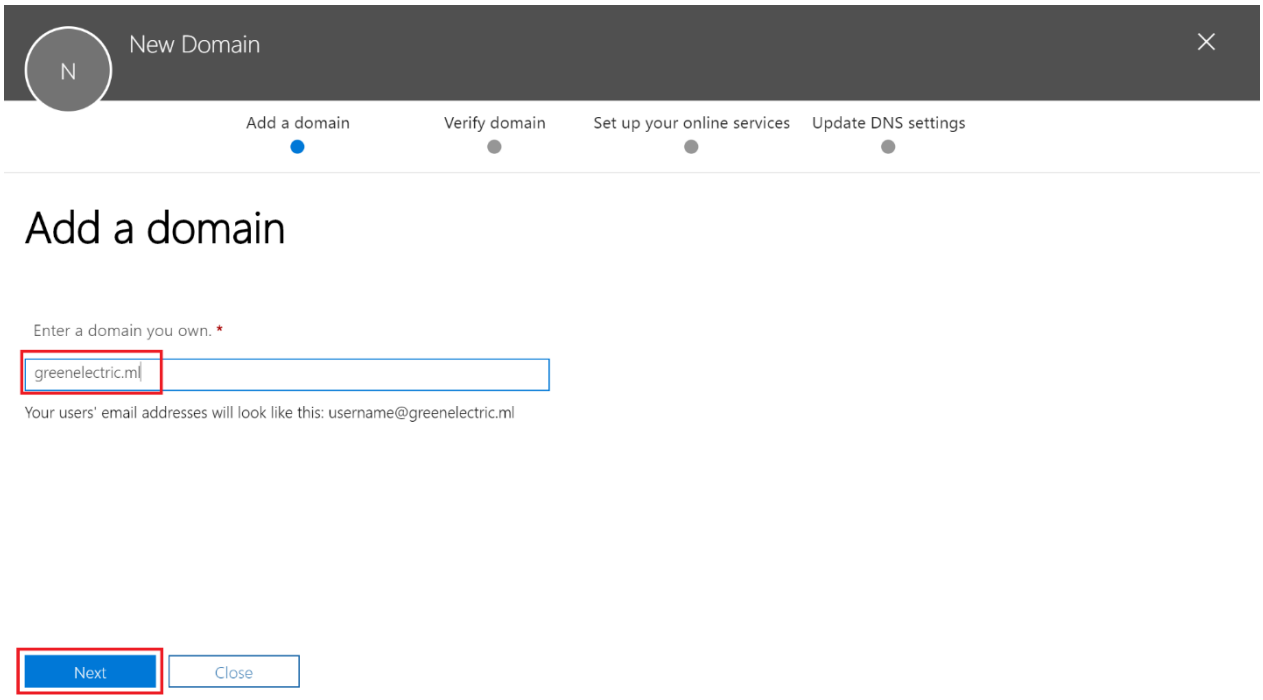
Verify and add the domain in the admin center

Now that you own a domain, you can verify it in Office/Microsoft 365 and add it in the admin center.

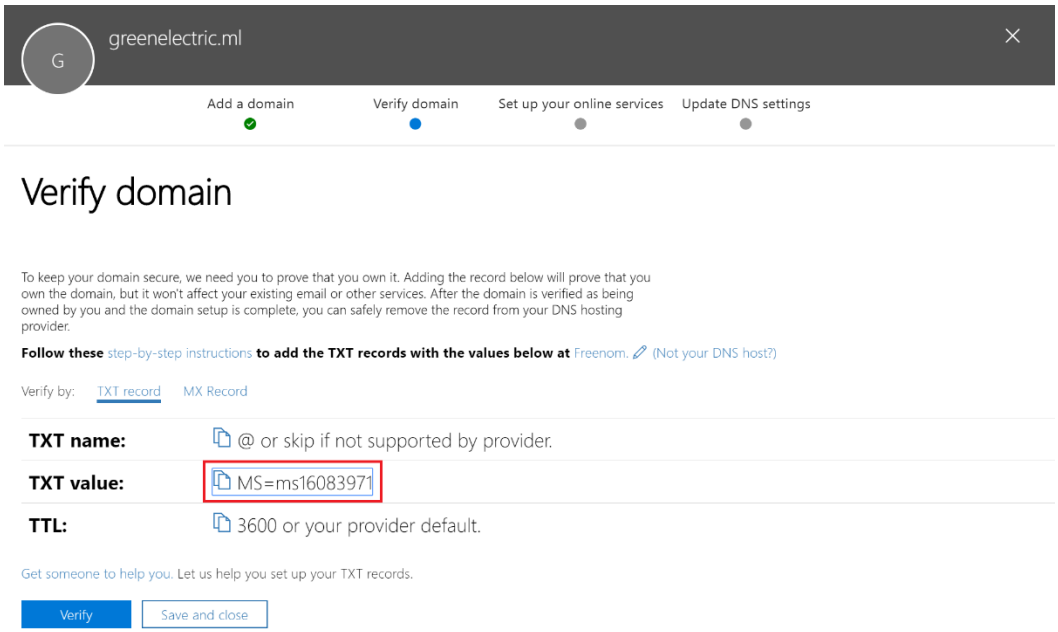
1. Go to https://portal.office.com and login with your global admin account
2. Go to Admin -> Setup -> Domains and click on Add domain



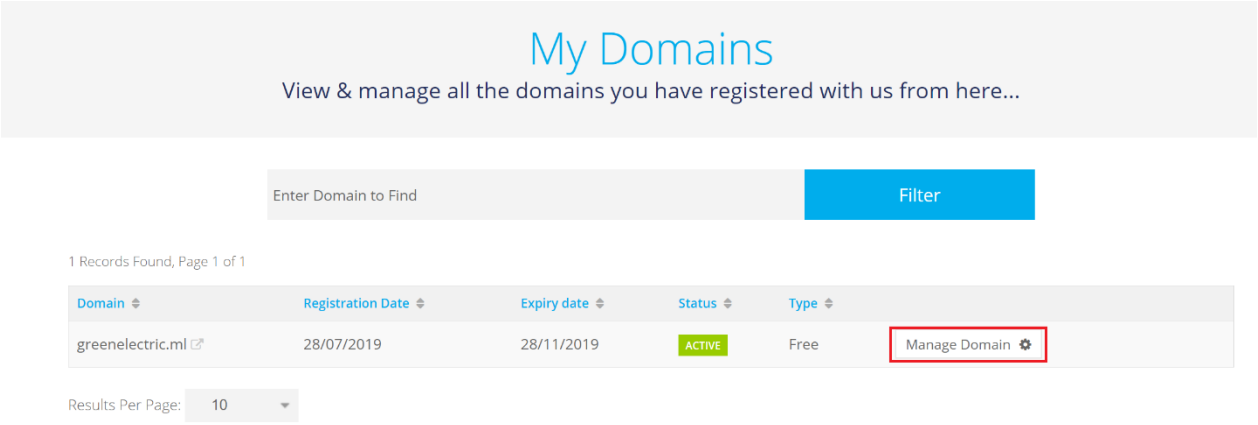
3. Enter your domain name and click Next



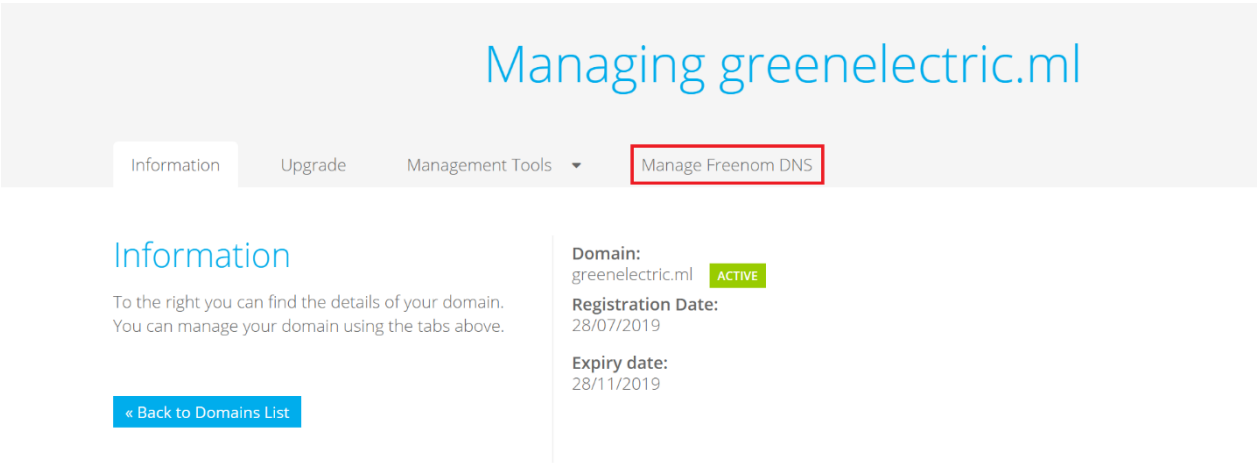
4. The next step is to verify your domain. Anyone can try to add anything in his/her tenant, that is why it is important to prove that you own it. There are several ways to do it, the recommended one is to verify it by a DNS TXT record. This is how it works: the admin portal generates a random text value and asks you to go into your domain register's DNS management and add this value as a TXT record there. When you do it, a script from the Office/Microsoft 365 admin center checks it – if it is there, this is a prove that you own the domain (because you can login to the management of this domain). So, as a first step, copy the TXT value



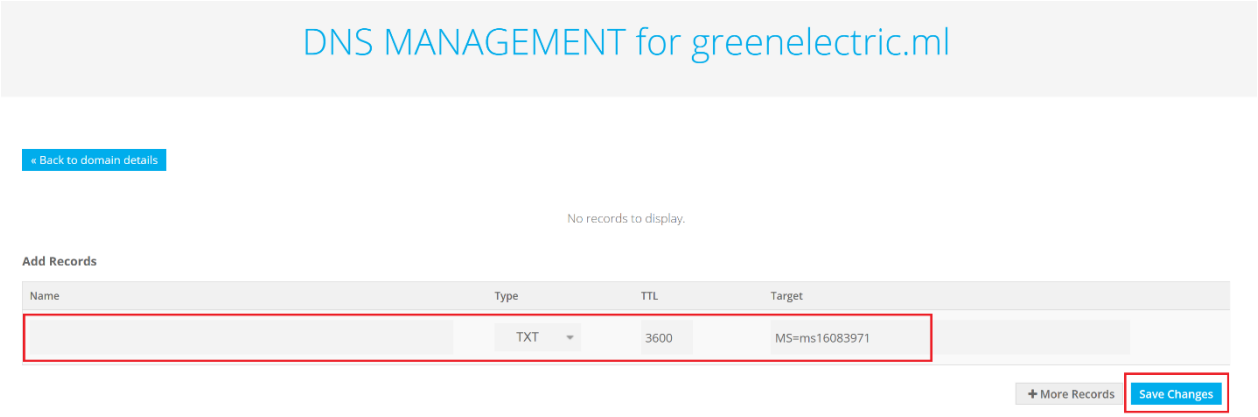
5. No go in your domain DNS settings and add this as a TXT record. In our example, we will go to https://freenom.com, sign in with our credentials and then go again to Services -> My Domains. From there, click on Manage Domain



6. Click on Manage Freenom DNS



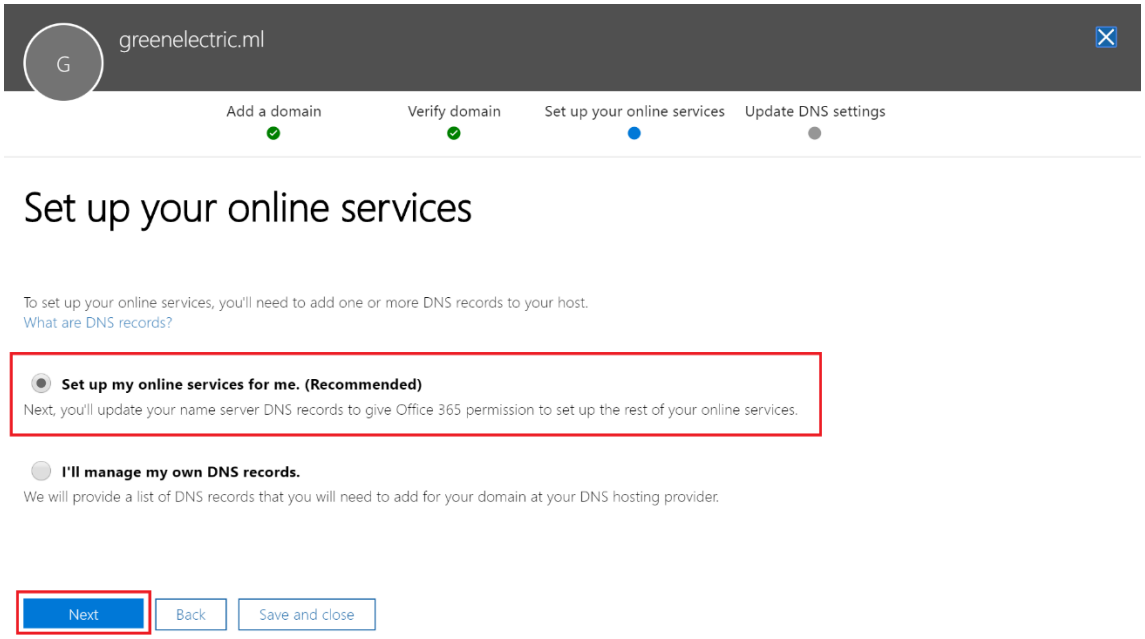
7. Add the TXT record. Leave the Name field empty (the correct syntax for this may for the different domain registers – for example it can be a dot, a star, or simply empty, like here). Change the Type to **TXT**, make sure that the TTL is **3600** (this is in seconds) and in the Target field paste the value that you have previously copied (in step 4) from the Office/Microsoft 365 admin portal. Click on Save Changes



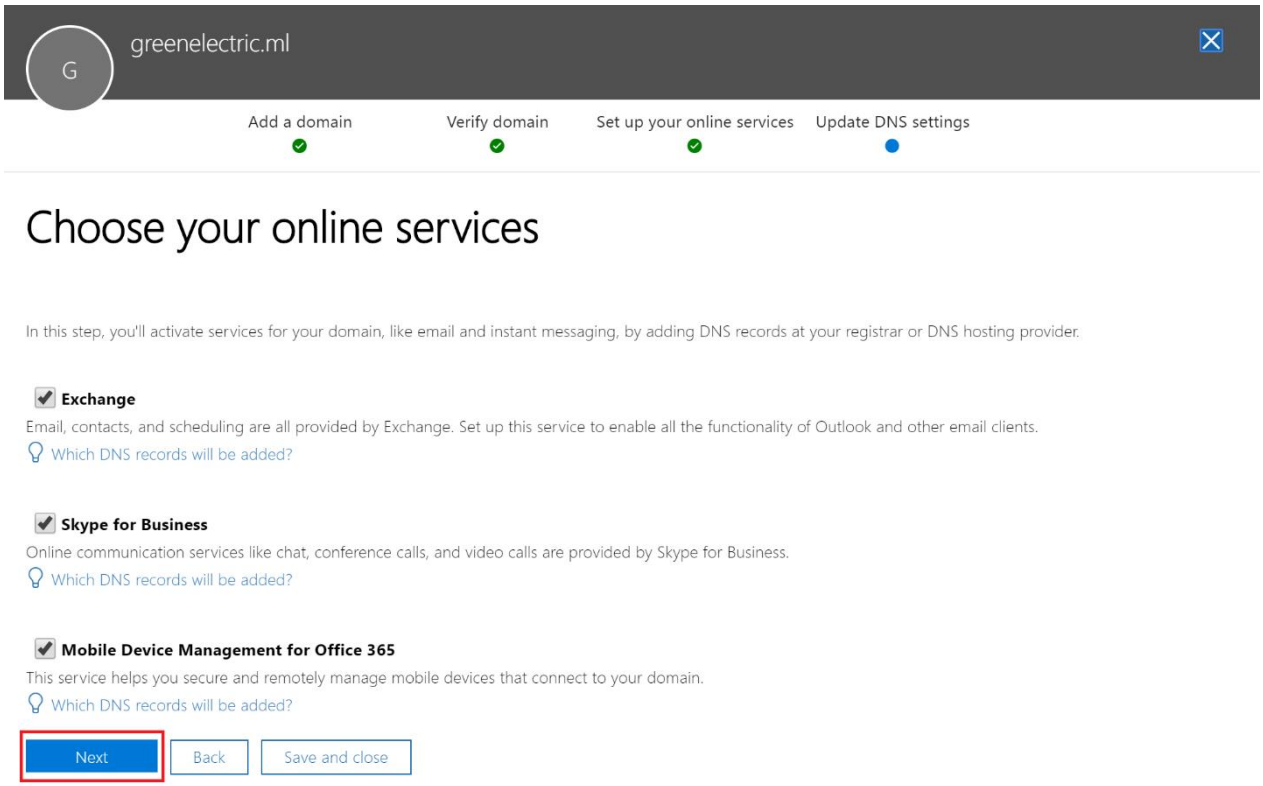
8. You should see a Record added successfully message. Wait several minutes (let's say 5) and go back to the admin portal. Click Verify. If the verification is not successful, simply wait another 5-10 minutes, then click Verify again.
9. Now you have two options. Either you transfer the DNS management from your domain register (Freenom) to Office 365, or you leave it there. One reason why the first option is recommended is because if you transfer the DNS to Office 365, all the required DNS records for the offered services will be automatically added in the DNS zone. Otherwise, you have to add them

manually in your domain register's DNS management (and it can happen that some of them are not supported). We will use the recommended option.

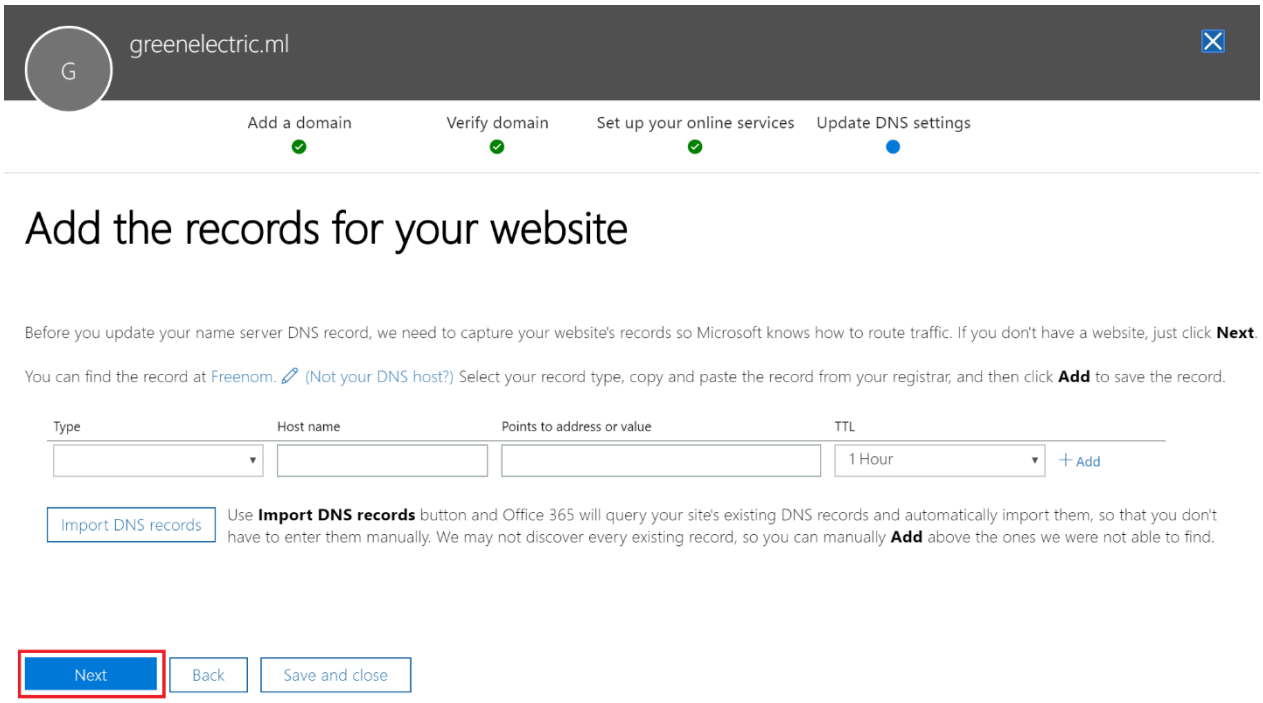
Select Set up my online services for me. (Recommended) and click Next.



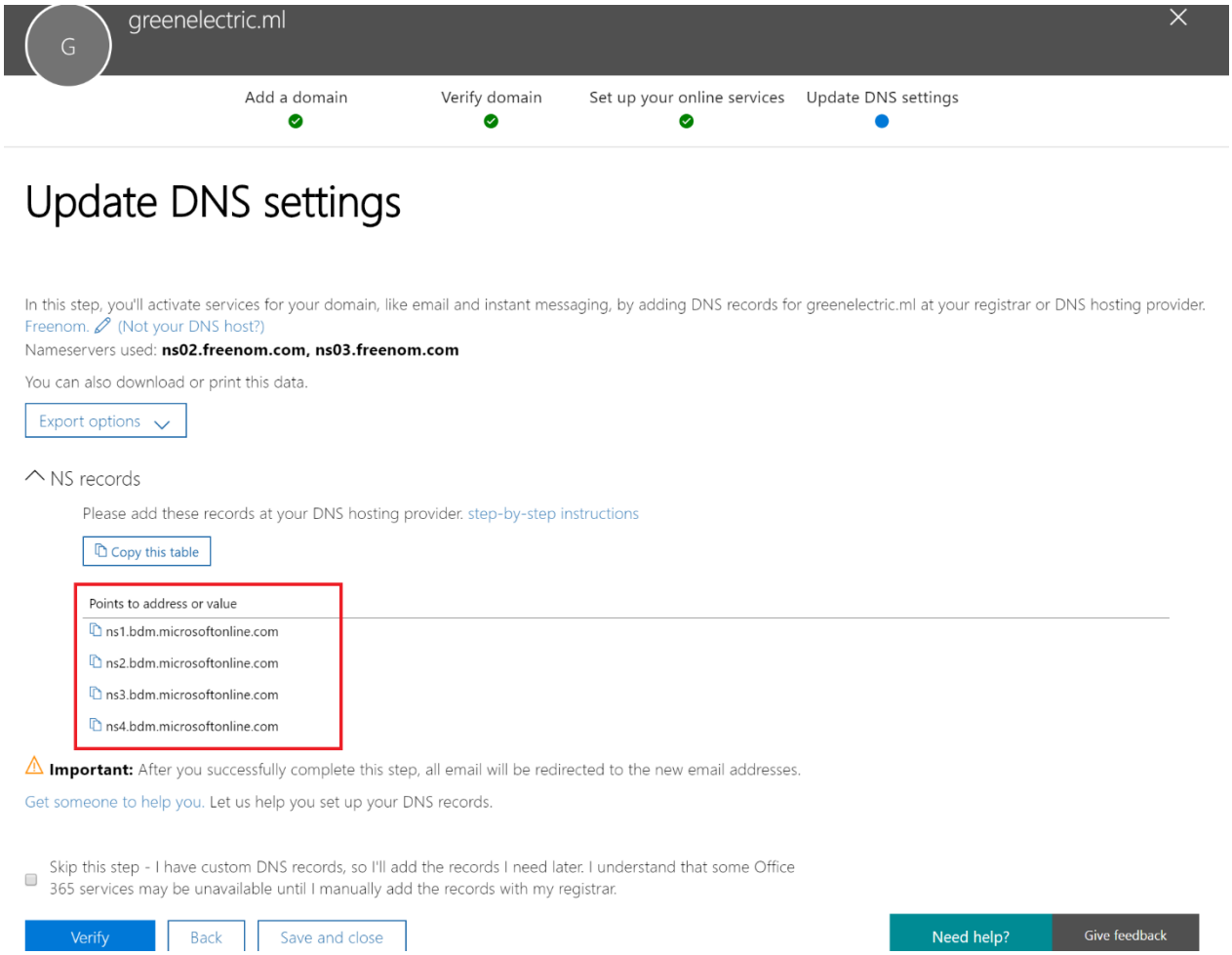
10. Leave the default selection of all services and click Next



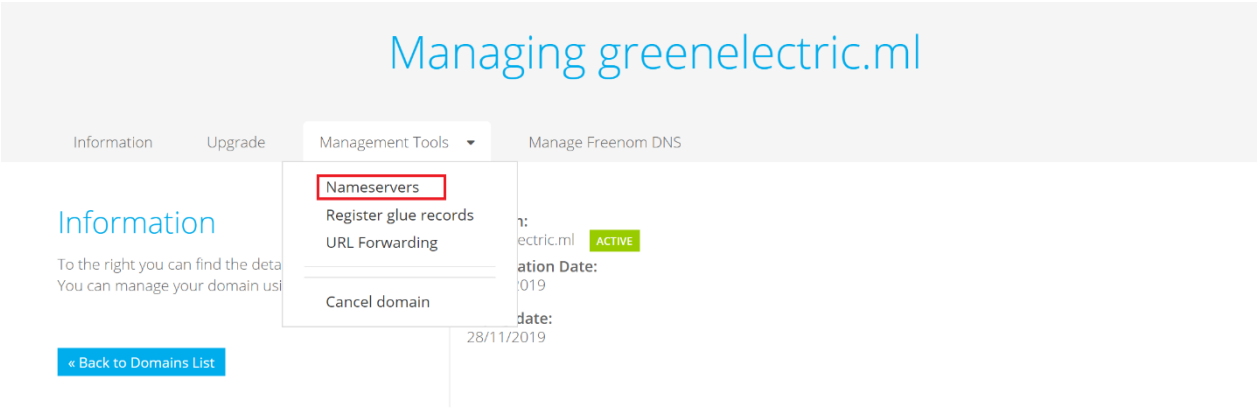
11. Now you have a chance to put some custom DNS records. For example, if you have a web site and since you are moving the DNS management, you need to add those records. Don't worry, even if you have something to enter here, you can also do it at any time later. In this case, we have nothing to add, so simply click <u>Next</u>



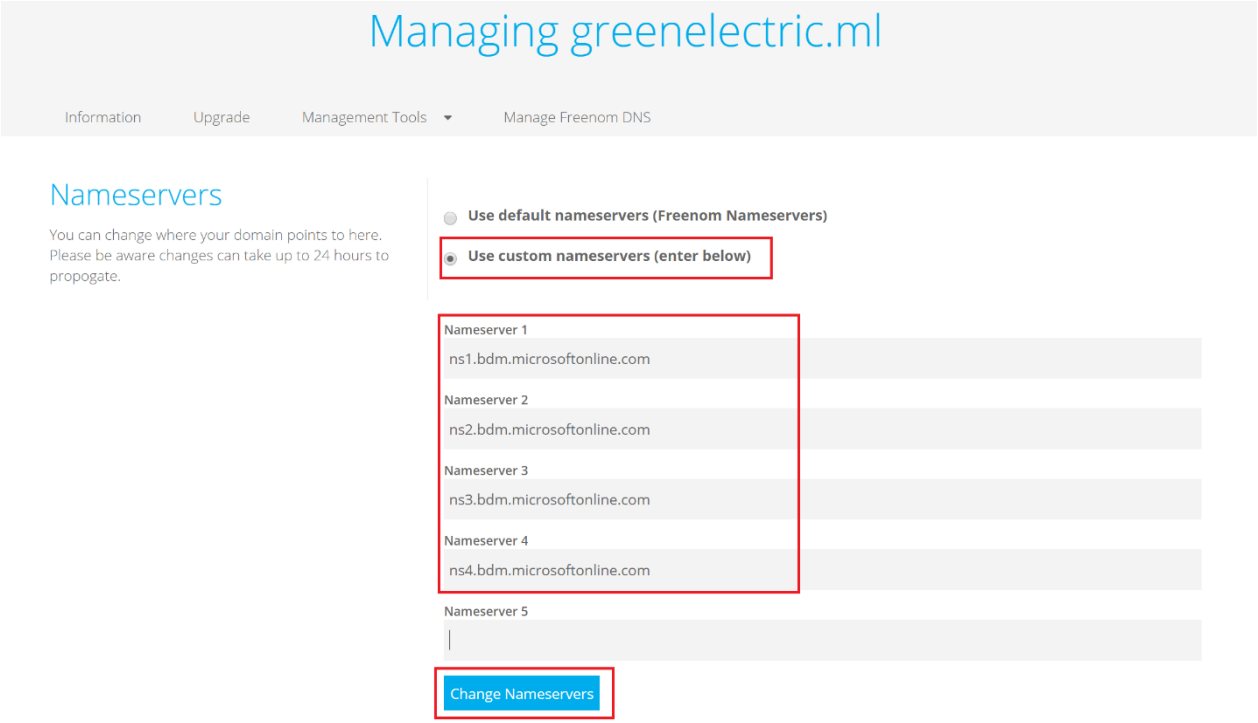
12. Remember, we have requested to transfer the DNS management to Office 365. In the DNS language, this means that you have to change the Name Server records (NS) to point to Office 365. Take a note of the four NS records (or copy them). They are: **ns1.bdm.microsoftonline.com**, **ns2.bdm.microsoftonline.com**, **ns3.bdm.microsoftonline.com** and **ns4.bdm.microsoftonline.com**



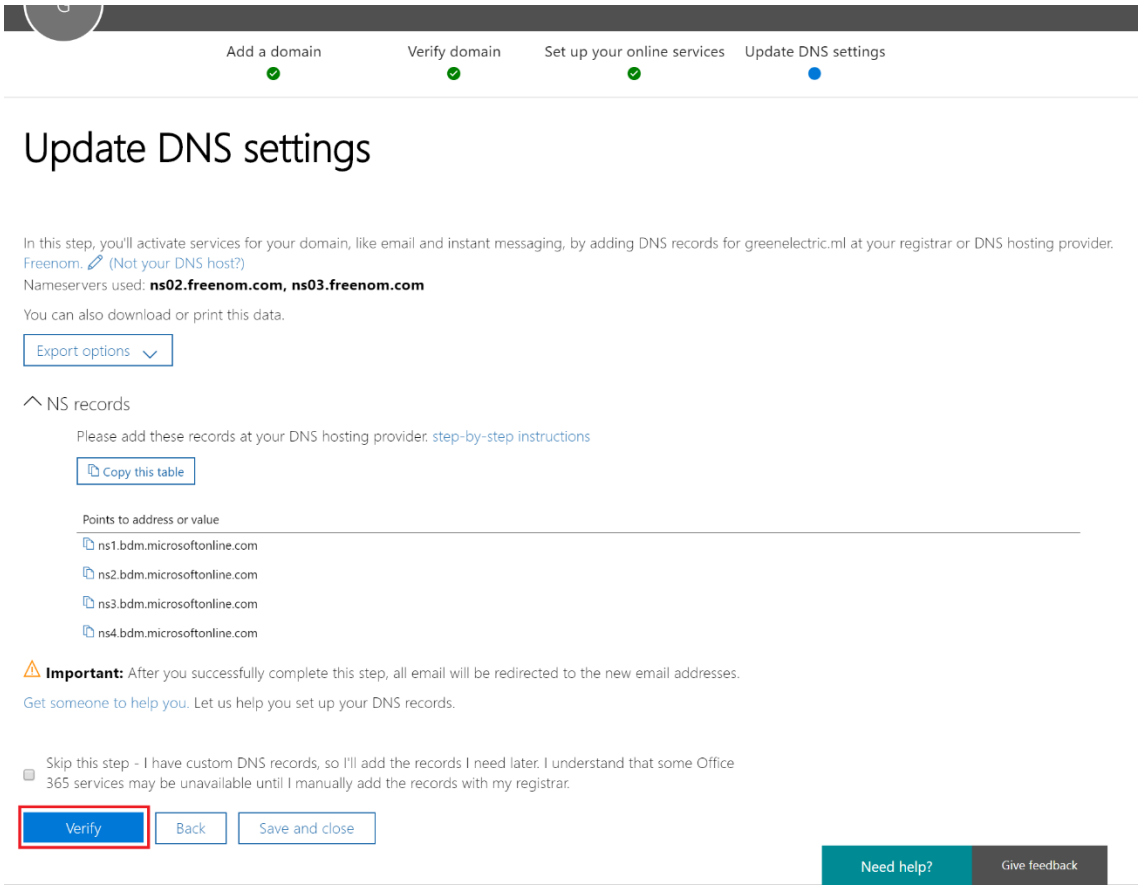
13. Go back to your domain register (Freenom) DNS settings and change the NS servers. To do this, go to Services -> My Domains -> Manage Domain -> Management Tools -> Nameservers



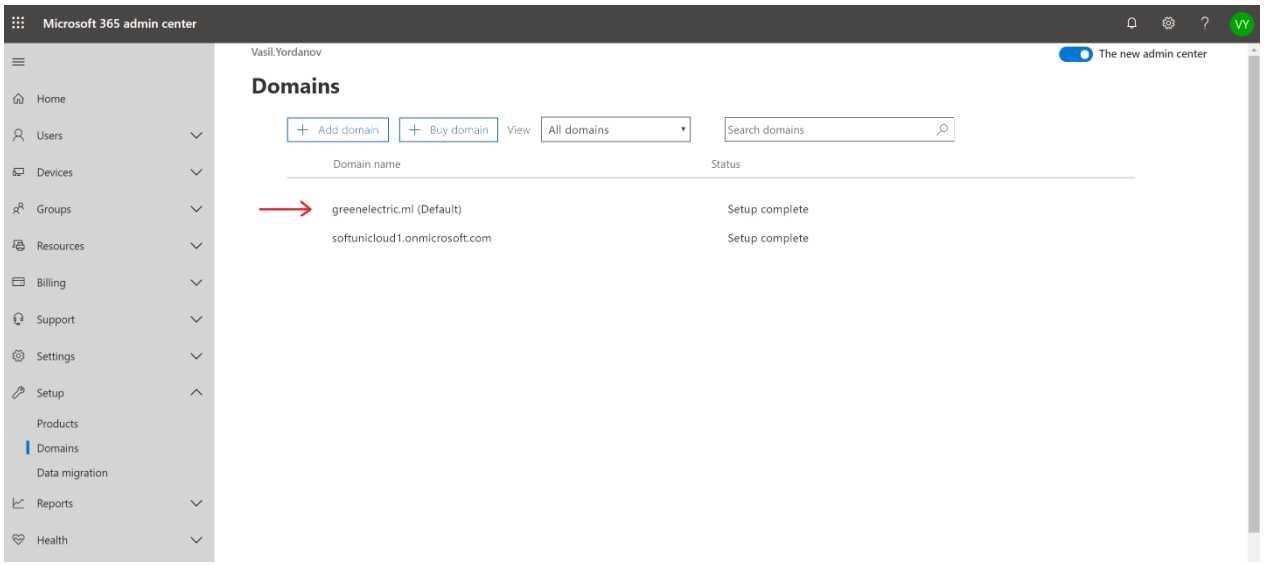
14. Change the selection to Use custom nameservers (enter below) and enter the four name servers that you have from the Office 365 portal. Click on Change Nameservers



15. Wait about 10-15 minutes. Then go back in the Office 365 domain add wizard and click Verify. If the verification is not successful, wait more (DNS needs some time to update its information across the other internet DNS servers) and then click Verify again



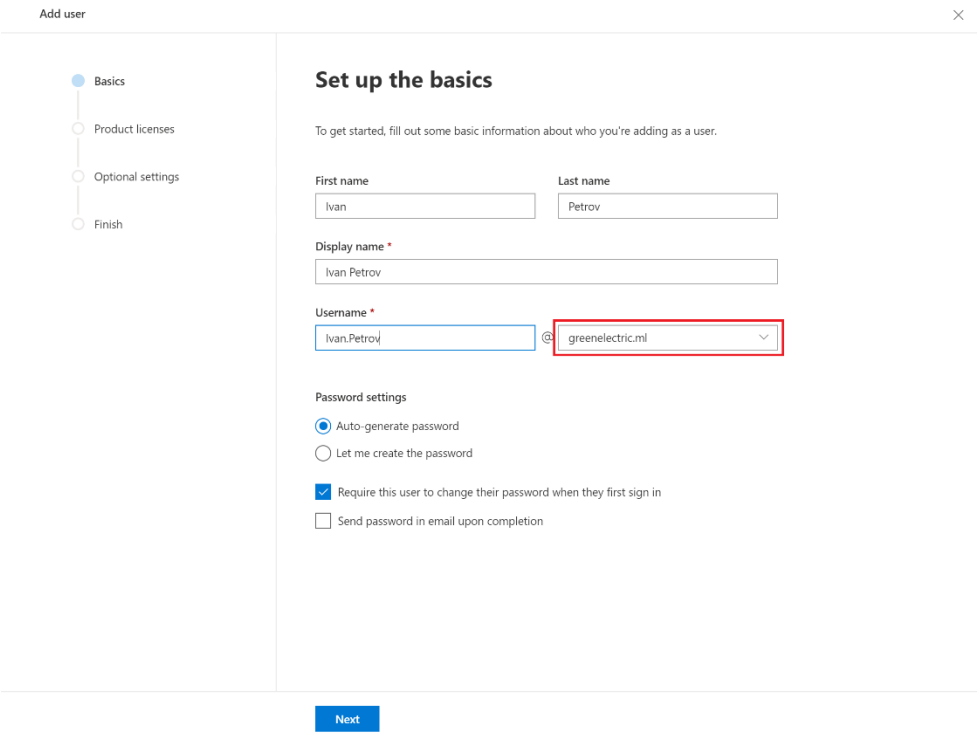
16. Read the Congratulations! Your domain and email addresses are all set up message and click Finish
17. Now you have your domain added in Office 365. To check it, go to Admin -> Setup -> Domains and you will see your domain in the list. It will also be set as a default domain



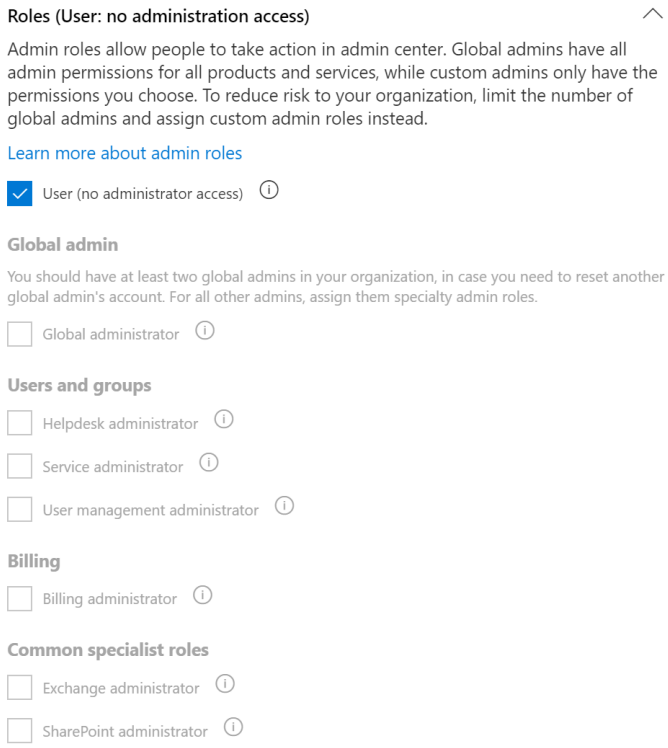
Exercise 2: Create users with the new domain suffix

From the admin center

1. Login to https://portal.office.com with your global admin account and go to Admin -> Users -> Active users. Click Add a user and fill in the required fields in the first screen of this wizard. Note that for the username, after the "@" sign, you can specify either your new domain (selected by default) or the initial domain **something.onmicrosoft.com**. Review the other settings and click Next



2. The next screen gives you an option to specify location, assign licenses and allow/deny particular apps. Select the Microsoft 365 E5 license, leave the default checkboxes for the apps and click Next
3. The next page is Optional settings. Here you can specify the user role. This is very important since it determines what will be the user's permissions. By default, the role is set to user, which means no administrative privileges. On the other side, you can uncheck this and instead check Global administrator. This is the role with the highest privileges for the tenant. There are also different administrative roles which give different (and limited) privileges, for example Billing administrator (can manage subscriptions and licenses), User management administrator (can manage and reset passwords for non-administrative users, manage support tickets, etc.) and other custom admin roles.
   You can also update the profile information for the user in this page.
   Leave the default User role and click Next

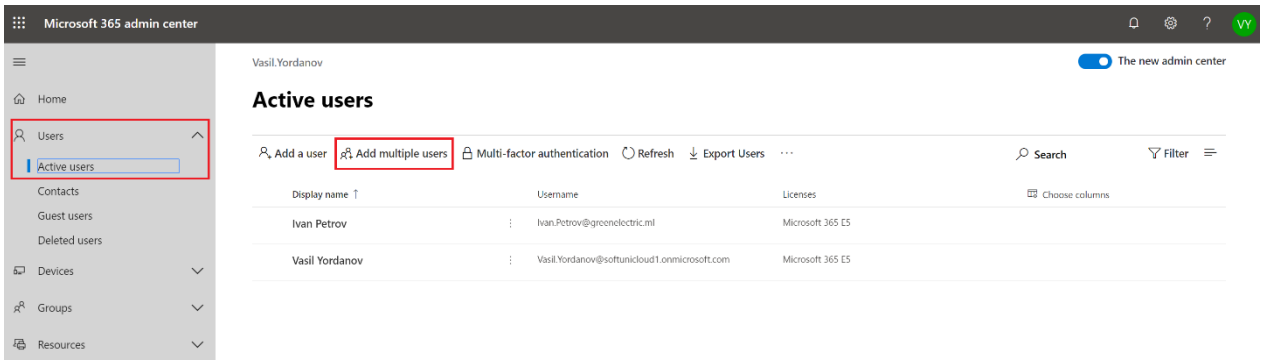


4. Review your settings and click Finish adding
5. You have now your first user associated with your domain. Remember that initially you were able only to add users in the format of **user@something.onmicrosoft.com** and after you have added your domain, now you can add users in the format of **user@mydomain.com**

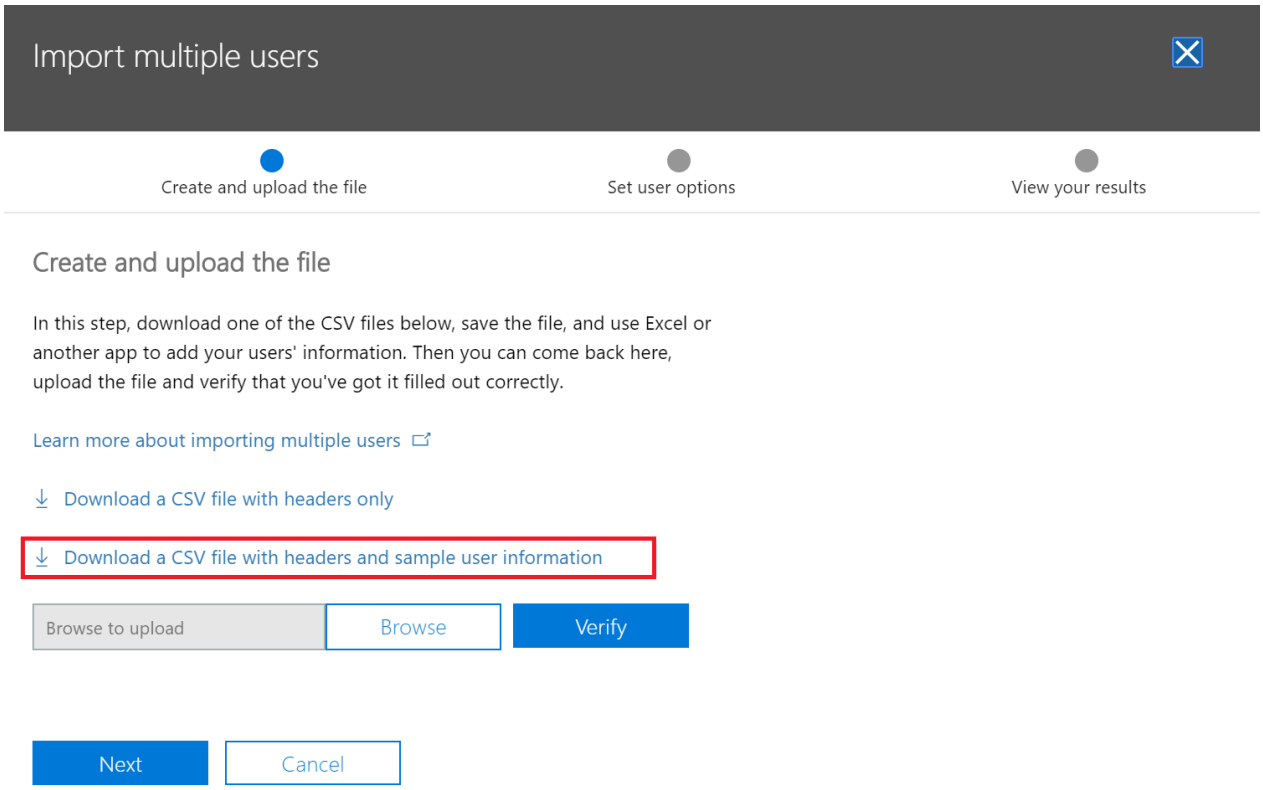
From a CSV file

There are different options to create users, so they show up in the admin center. Instead of creating them one by one, you can upload a file and then upload it.

1. Go to Admin -> Users -> Active users and click Add multiple users



2. Download one of the sample CSV files. In the example below, we have downloaded the one with headers and some example users



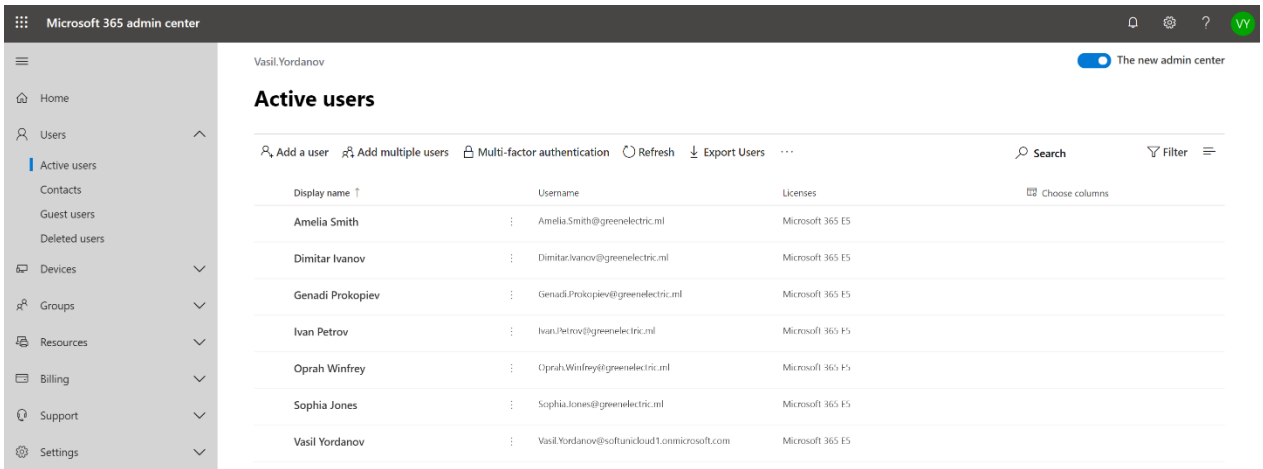
3. Delete the example users (leave only the first row) and then add your own users. You can fill in only the User Name, First Name, Last Name and Display Name columns, but it is up to you to type some information in the others, too

Note: In the User Name column, it is important to type the usernames containing your previously added domain(s). For example, if you type

user@mydomain.com there and you do not have **mydomain.com** verified and added in Office 365, you will receive an error.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
1	User Name	First Name	Last Name	Display Name	Job Title	Department	Office Number	Office Phone	Mobile Phone	Fax	Address	City	State or Province	ZIP or Postal Code	Country or Region	
2	Amelia.Smith@greenelectric.ml	Amelia	Smith	Amelia Smith												
3	Dimitar.Ivanov@greenelectric.ml	Dimitar	Ivanov	Dimitar Ivanov												
4	Sophia.Jones@greenelectric.ml	Sophia	Jones	Sophia Jones												
5	Genadi.Prokopiev@greenelectric.ml	Genadi	Prokopiev	Genadi Prokopiev												
6	Oprah.Winfrey@greenelectric.ml	Oprah	Winfrey	Oprah Winfrey												
7																
8																

4. Browse for your file, upload it and click Verify. When you receive the Your file looks good. Click or tap Next message, click Next
5. Leave the Sign-in status to Allowed, assign Microsoft 365 E5 licenses and click Next
6. Remove the Email the results files to these people checkbox and click Close without sending
7. It may take 10-20 seconds for the web page to reflect the updates. Refresh the portal if needed and you will see your accounts created



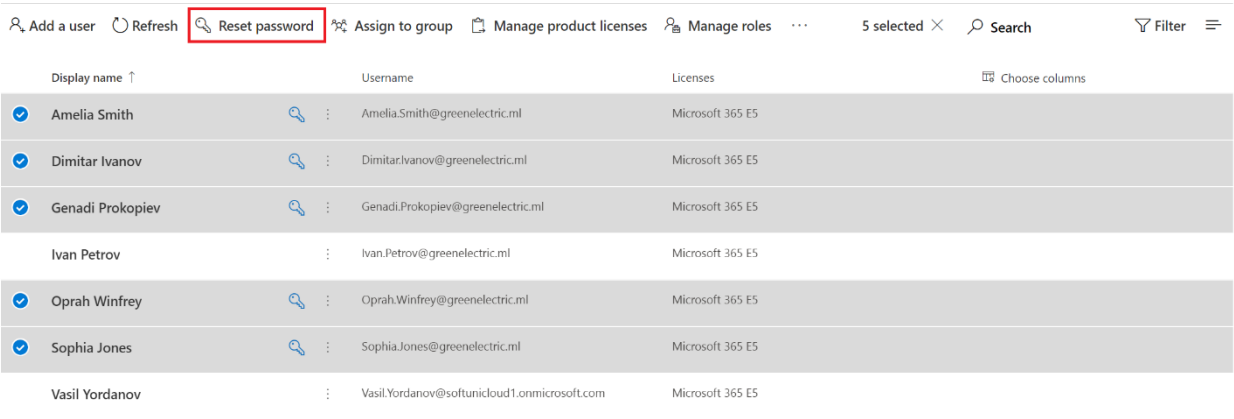
Note: From now on, you will decide which users you will create and use and how to assign passwords, licenses and roles. Regardless of what your decisions will be, there are several recommendations:

- Assign the Global administrator role to at least two users
- It is a best practice that the users which are global admins are in the initial domain (**user@something.onmicrosoft.com**) so they are not dependent on the other added domains (if they expire or something goes wrong with them)

- The global admins do not need to have licenses
  For example, if your name is **Amelia Smith** and you have to be a global admin, the recommendation is to have two accounts:
  - **Amelia.Smith@something.onmicrosoft.com** - global admin, no license
  - **Amelia.Smith@mydomain.com** - user role, licensed

  This way you can use the second account for your daily tasks (email, communication, etc.) and if you need to administer something in the portal, you can login with your global admin account.

8. Reset the passwords
   You can select the users that you have just added and (bulk) reset their passwords



PowerShell (Optional)

Talking about automating user accounts creation, we need to mention PowerShell. You can do almost anything with PowerShell in Office 365. We give no detailed instructions in this guide, but If you want, you can follow the procedures here to create user accounts in Office 365 with PowerShell.

In a nutshell, you need to have PowerShell (included in all supported Windows versions), to install a special module and to connect to your tenant. Then, you can

use cmdlets (pronounced “commandlets”) to manage users. For example, the cmdlet to create user account is:

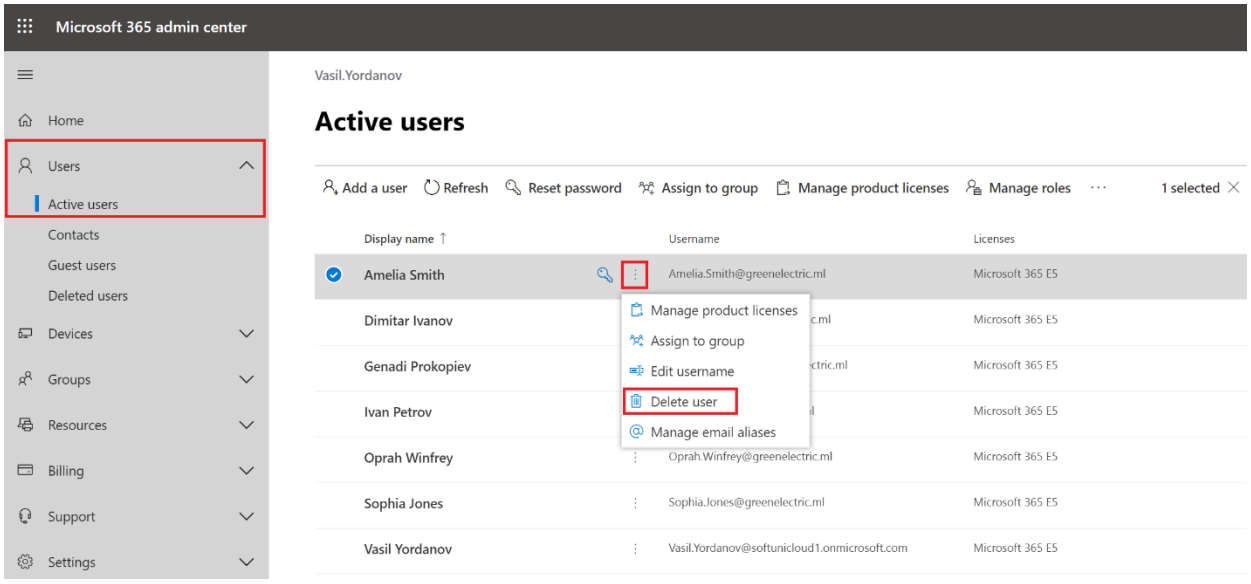
New-MsolUser -DisplayName <display name> -FirstName <first name> -LastName <last name> -UserPrincipalName <sign-in name> -UsageLocation <ISO 3166-1 alpha-2 country code> -LicenseAssignment <licensing plan name> [-Password <Password>]

Exercise 3: Delete and restore users

When you delete a user account from Office 365, it goes to a recycle bin (called Deleted users in the portal) and stays there for 30 days. During this period, you can restore the user and its associated mailbox and OneDrive content. After these 30 days, the user account and its corresponding data is permanently deleted and cannot be recovered. More detailed information can be find here and here.

From the admin center

1. To delete a user, go to Admin -> Users -> Active users, click on the vertical dots next to the username and click Delete user. Leave the default selections and confirm the deletion



2. To check the deleted user account, navigate to Admin -> Users -> Deleted users. To restore it, click on the account name and click Restore. You need to decide how you want to create/generate the user's password and if the user will need to change it during the first logon. After this, you may need to reassign the user license(s).

Note: When you delete a user account, the corresponding license(s), if any, will be released and can be reused by another user. Also, if you restore the user within the 30-day period and reassign the license(s), the user's mailbox and OneDrive content will also be restored.

Via PowerShell (optional)

The detailed steps to delete user account with PowerShell are described here.

After you have connected with PowerShell to your tenant (and in this example here we use the "Connect with the Microsoft Azure Active Directory Module for Windows PowerShell" option), you can delete users in different ways. For example, you can delete a user account by specifying its UPN:

```
Remove-MsolUser -UserPrincipalName Amelia.Smith@greenelectric.ml
```

Alternatively, you can restore this user from PowerShell again (within the 30-days period):

```
Restore-MsolUser -UserPrincipalName Amelia.Smith@greenelectric.ml
```

Permanently delete (PowerShell only, optional)

You may want to permanently delete a user account. This means that it cannot be restored, which is also valid for the associated user data – mailbox and OneDrive.

To permanently delete a user account, first delete it normally either via the web interface or with the PowerShell command below:

```
Remove-MsolUser -UserPrincipalName Amelia.Smith@greenelectric.ml
```

After this, delete it from the recycle bin:

```
Remove-MsolUser -UserPrincipalName Amelia.Smith@greenelectric.ml -RemoveFromRecycleBin
```

Check that this user account is permanently deleted.

You will need user some accounts for the rest of this and the other labs, so now you will create one more account – it can be with the same name/UPN as the deleted one.

Manually create a user account (and assign a license).

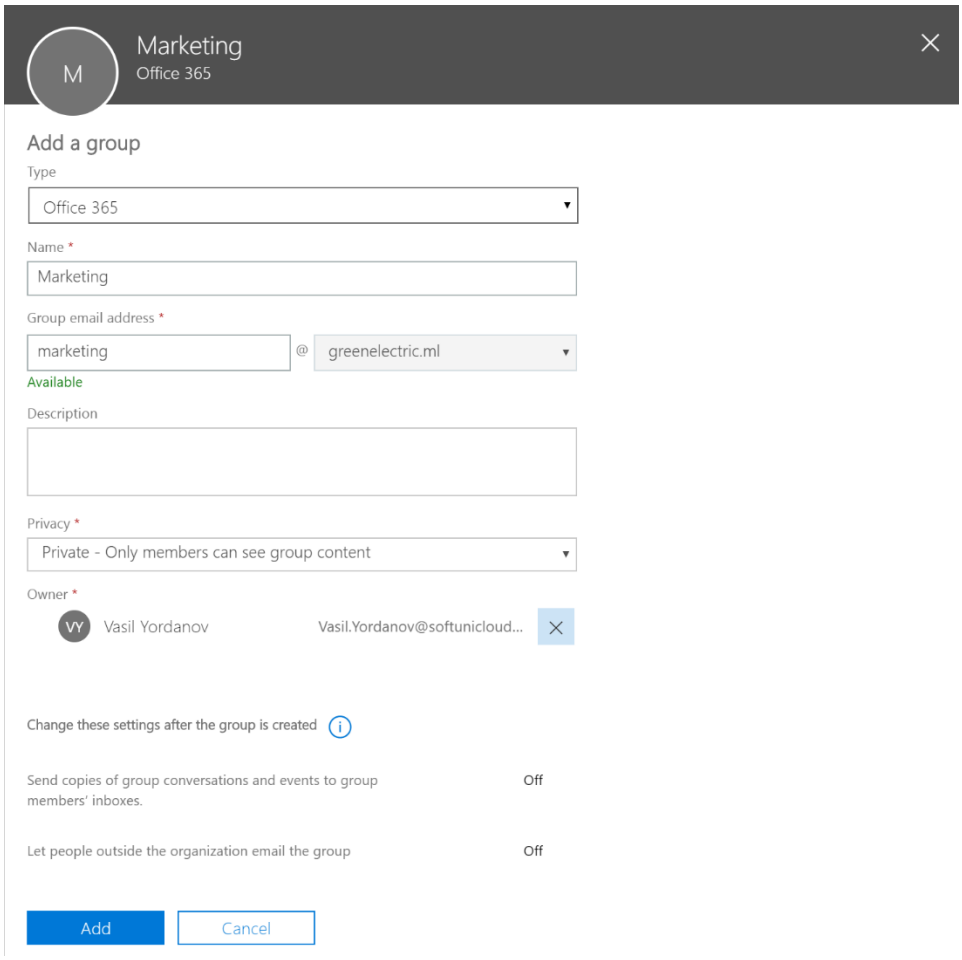
Note: Even if you create a user with the same name/UPN after the permanent delete, it is considered as another, brand new user account and it will have a new (empty) mailbox and OneDrive.

Exercise 4: Manage groups

You know that there are different type of groups in Office/Microsoft 365 and they have different purposes (Office 365, Distribution list, Mail-enabled security, Security). We prefer to use groups rather than individual user accounts, because when we give permissions, we do it based on groups. And once the permissions are configured, we simply add or remove members of the groups.

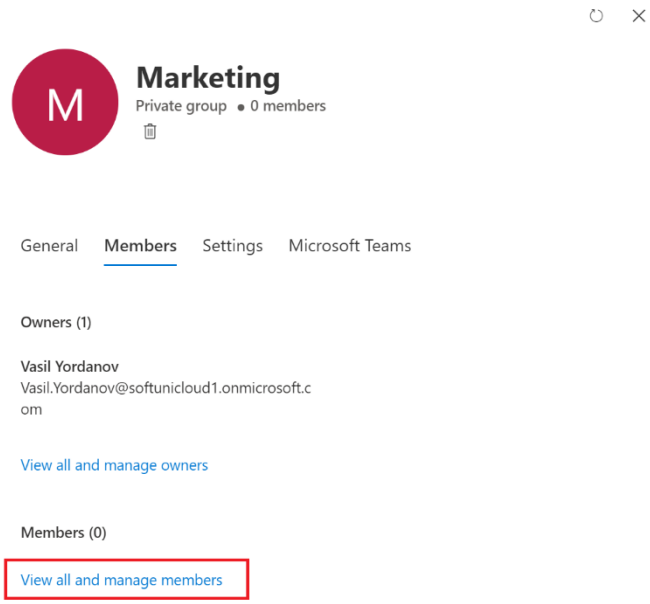
Create groups using the admin center

1. Navigate to Admin -> Groups -> Groups and click Add a group
2. Select Office 365 as a type, name it Marketing, select **marketing@yourdomain** as an email address, change it to Private, select owner and click Add

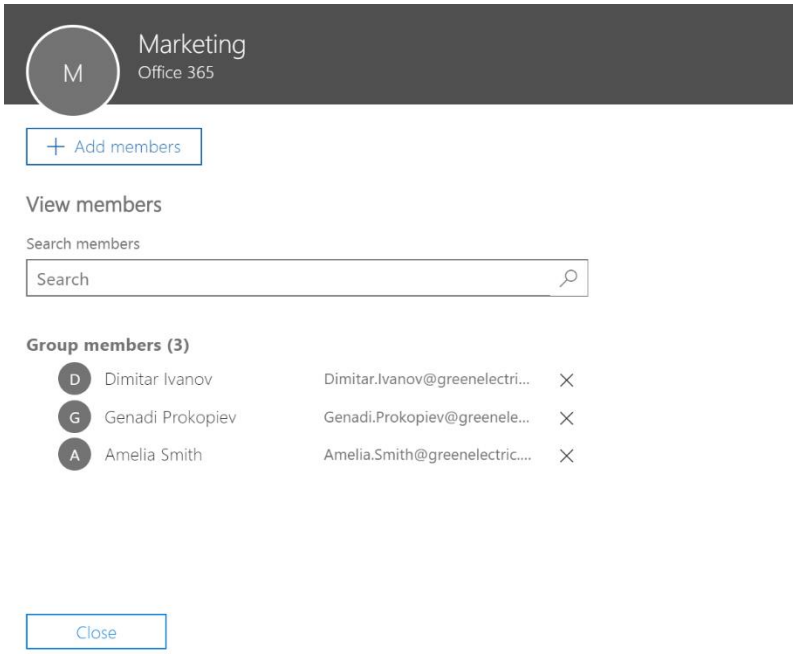


Add group members using the admin center

1. Go to Admin -> Groups -> Groups to see your newly created group (refresh the page if needed)
2. Click on your **Marketing** group and go to the Members tab. Click on View all and manage members



3. Add some of the users as members. In this example, we have added the first three users



4. Confirm if needed and close all opened windows

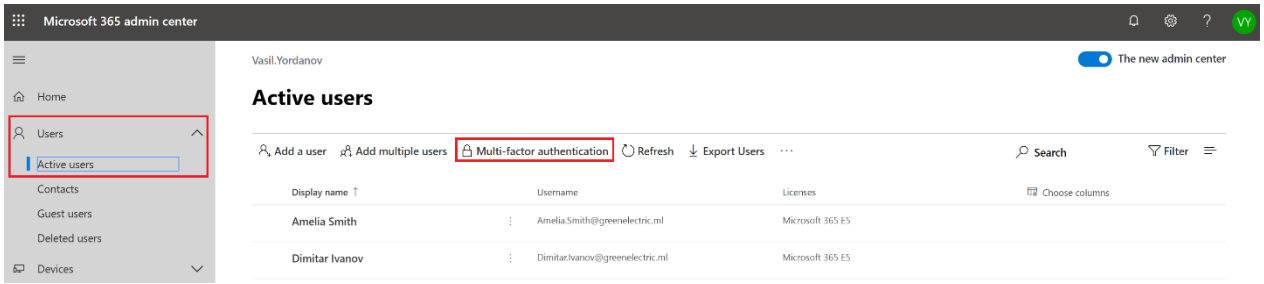
Using the same procedure, create one more Office 365 group and name it **Sales**. Add the another three users as members of the Sales group.

Exercise 5: Enable multi-factor authentication (MFA)

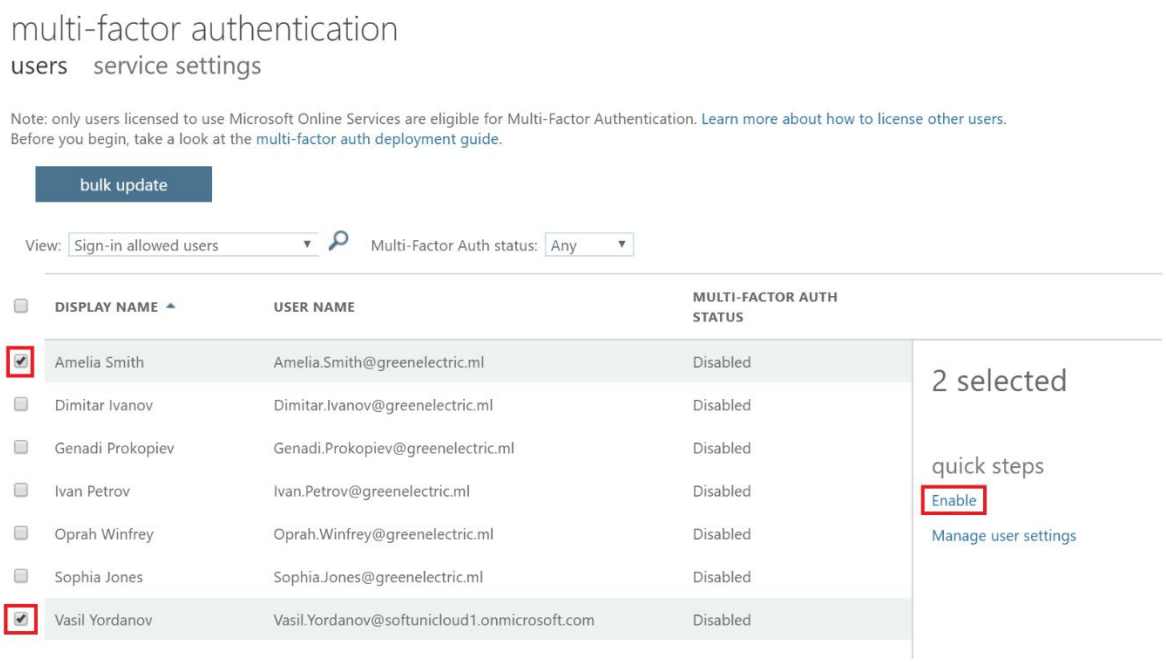
You know how important is to protect the identities and you also now that the passwords are not enough anymore. One very good step in this direction is to enable multi-factor authentication, or MFA.

Note: This is especially important for the global admins (and all other admin roles)

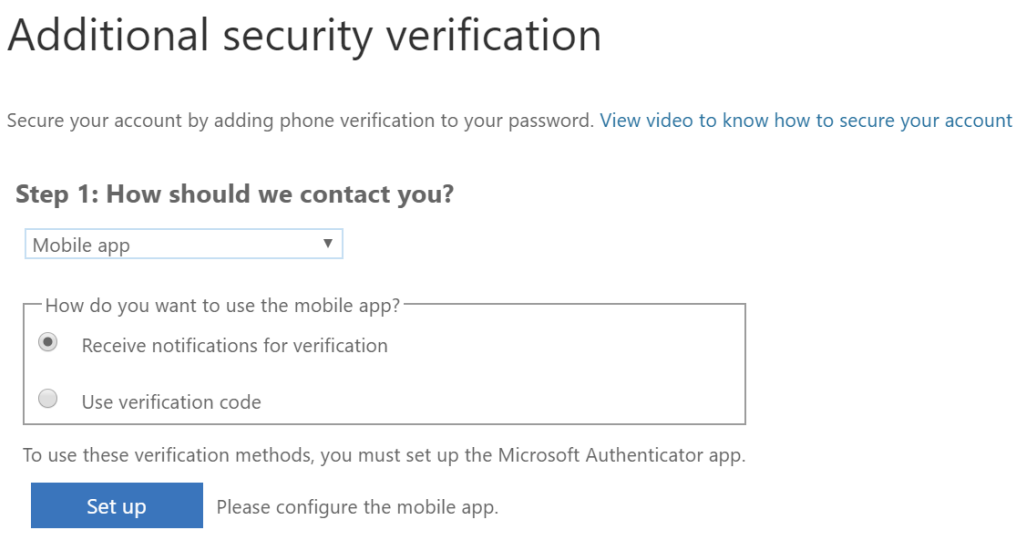
1. Navigate to Admin -> Users -> Active users and click on Multi-factor authentication



2. Select several users. For example, your global admin(s) and one more regular user and click Enable. Confirm when needed



3. The next time, a MFA enabled users logs in, a More information required window will popup and the user will need to add and configure the second authentication method. It is up to the user which option to select but generally the Mobile app option is considered more secure (and it is more convenient in most cases also)



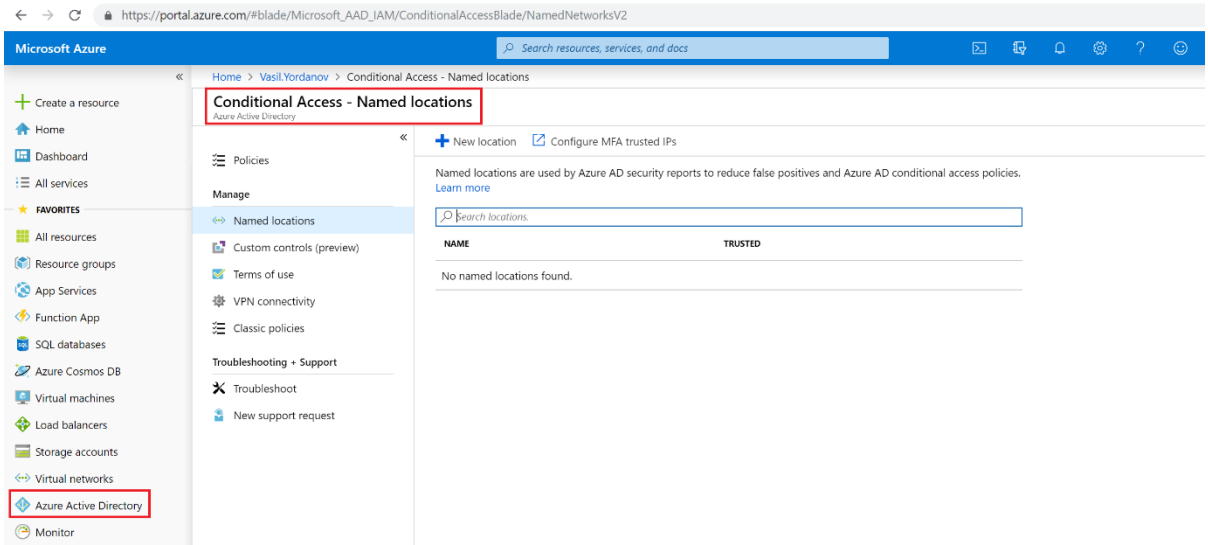
Using this option, the user need to install Microsoft authenticator app (iOS or Android) and to associate his/her account, following the instructions

Note: In some apps, like Outlook, Apple Mail, and Microsoft Office, you can't use a phone to secure your account. To use these apps, you'll need to create a new "app password" to use in place of your work or school account password. More information – here.

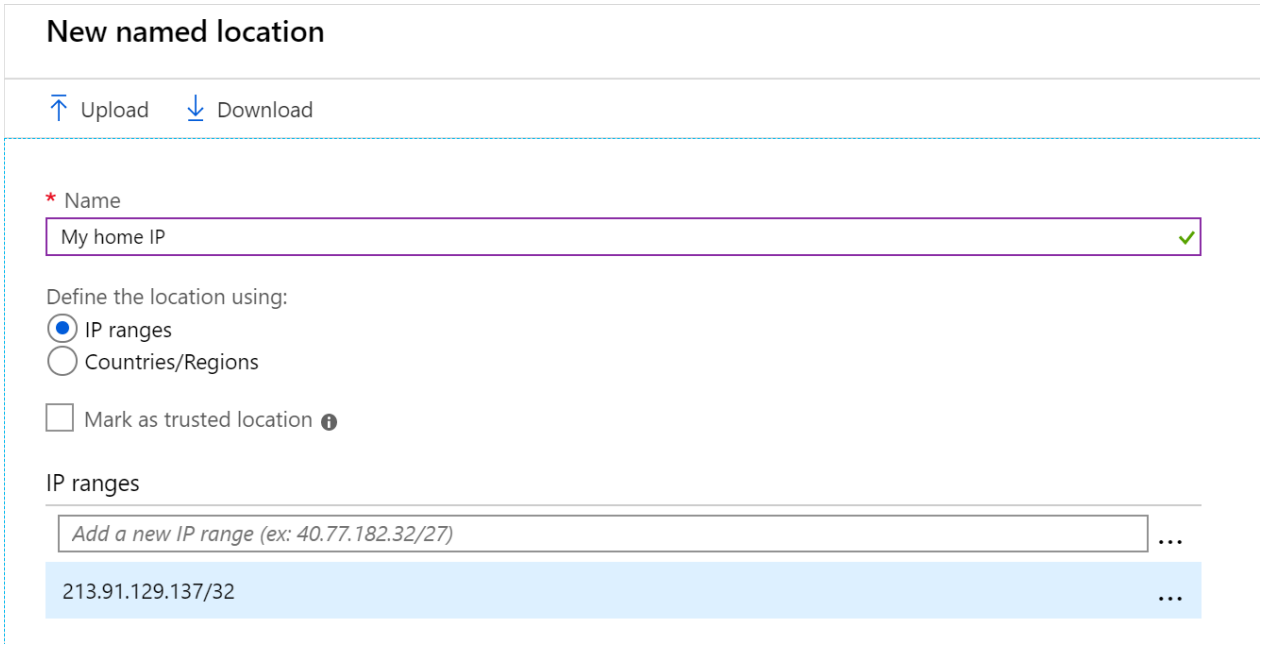
Exercise 6: Configure conditional access policy

By configuring Conditional Access policies, you can maintain control over how and where your company data is accessed, making your business more secure. You can define exact criteria for who can gain access and block those who don't meet the criteria. The criteria can be based on factors like the type of device, app and location

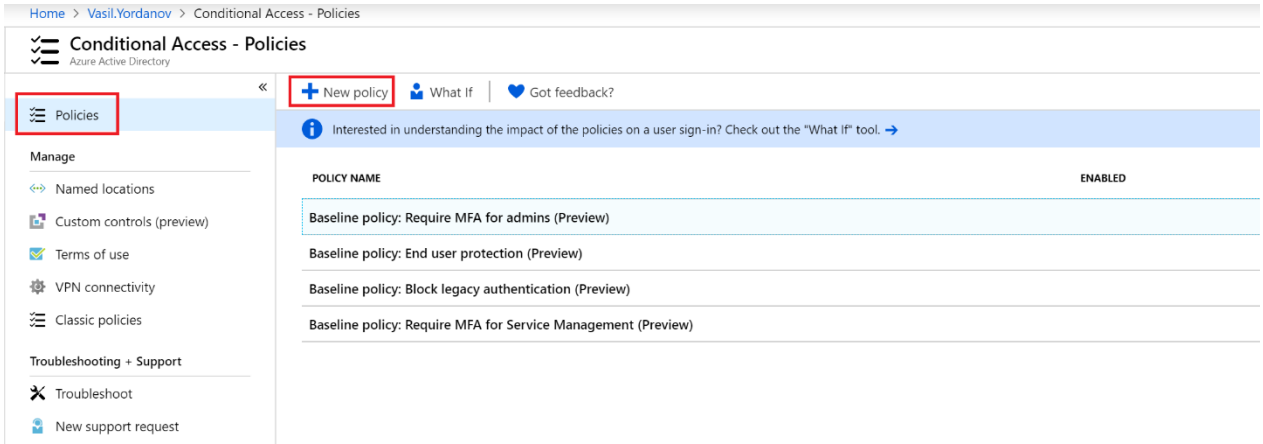
1. Navigate to https://portal.azure.com and authenticate with a global admin account (Remember – since you can login to Office/Microsoft 365, this means that you can also login to Azure)
2. Go to Azure Active Directory -> Conditional Access (or search directly for "Conditional Access" in the search bar) and click first on Named locations



3. Let's put your home IP address, for example, as a Named location. First, obtain your public IP address by navigating to (while you are connected to your home router) a public site like this: https://whatismyipaddress.com/. Now go back in the portal and fill in the New named location details. For Name, put something descriptive. For IP ranges, put the IP address that you have obtained and append **/32** after it. Finally, click Create at the bottom

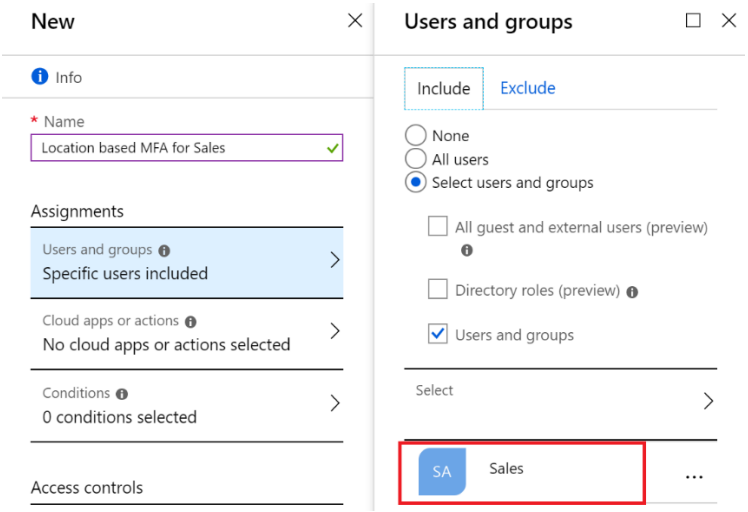


4. While still there, go to Policies -> New policy

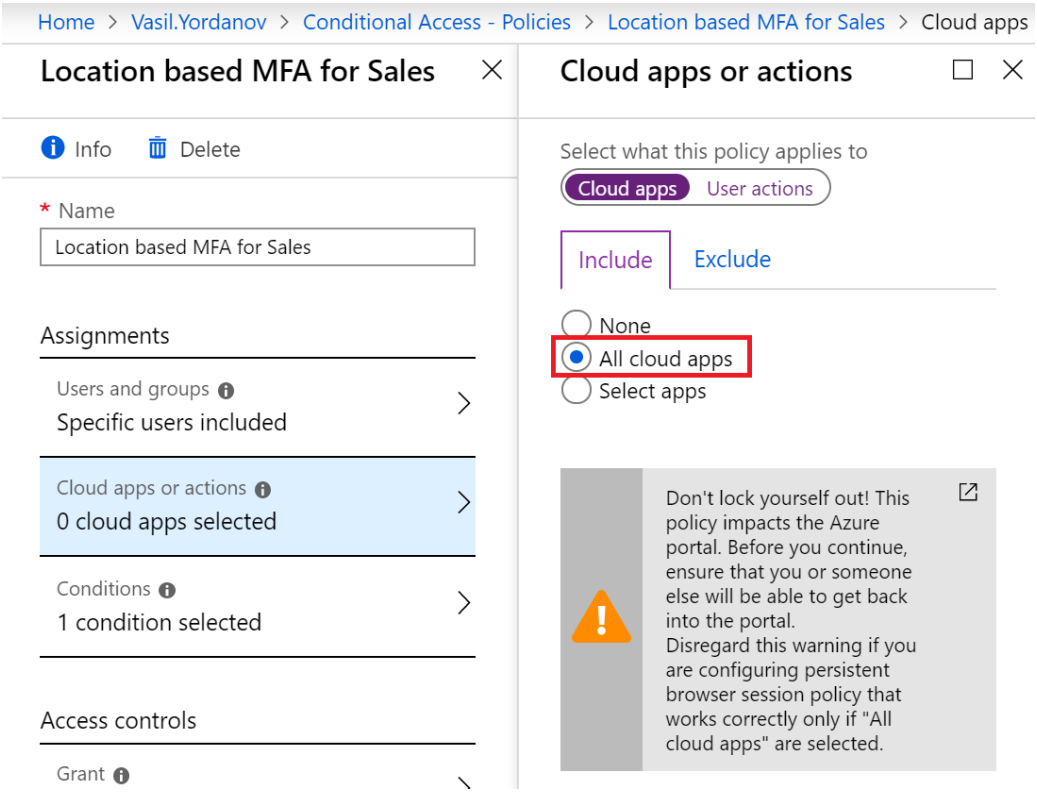


5. Configure the following in your new policy:

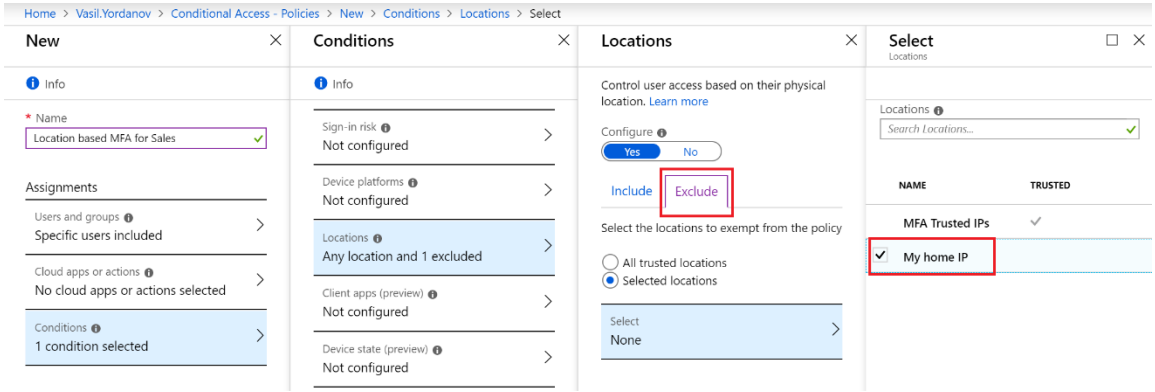
- **Name** – put a descriptive name, such as “Location based MFA for Sales”
- **Assignments (Users and groups)** – include the Sales group



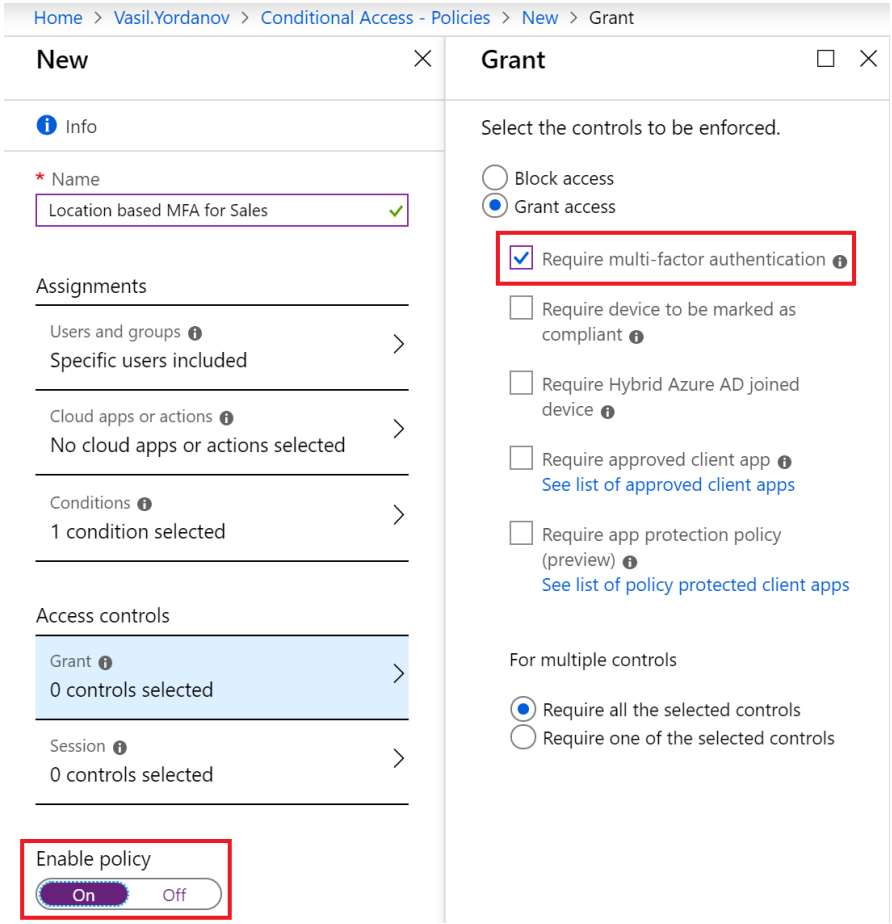
- **Assignments (Cloud apps or actions)** – select All loud apps



- **Assignments (Conditions)** – select the previously configured My home IP to be excluded (from the MFA)



- **Access controls (Grant)** – check the box next to Require multi-factor authentication. Finally, click on Enable policy and then Create



6. Test your conditional access policy
   What should be the result of this configuration?
   Answer: It will ask for MFA, but only if all of the conditions below are met:
   - The user is member of the Sales group

- The user tries to access any cloud app (or to login in the portal)
- The user is accessing the cloud app (or the portal) from a different than the specified location (based on the My home IP address)

In other words, if the user accesses the portal or an app from “home”, he/she will not be asked for MFA (second factor will not be required, only a password). If the user accesses the portal or an app outside “home”, second factor to authenticate will be required.

You have completed LAB 2.