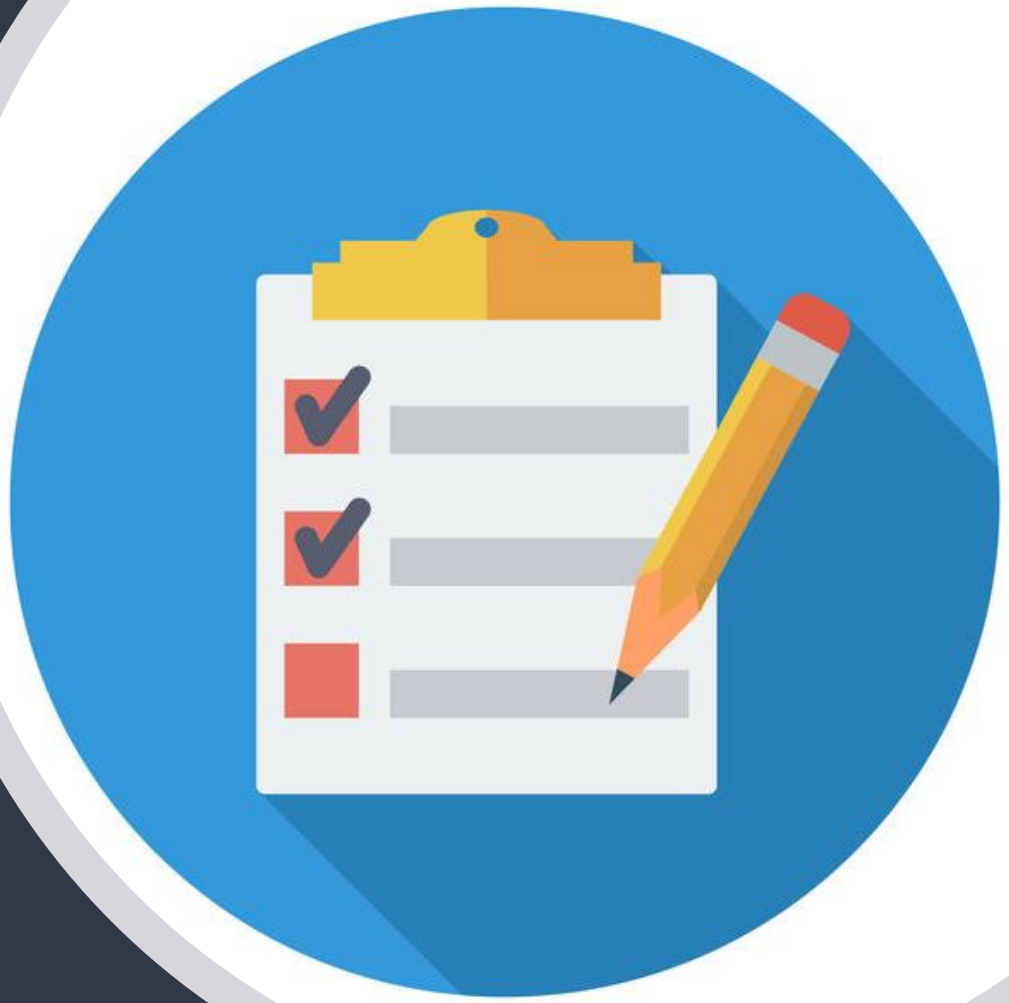
Setup Guide

Client Azure AD integration with CyberPilot platform

1. Prerequisites for using Azure AD integration with the CyberPilot platform

- A person with Admin access to your organizations Azure AD.
- This admin user must have at least Office 365 Premium P2 license to be able to create the application for the SSO.
- The rest of the staff members do not need a Premium P2 licenses to use SSO.
- All of the users must have an exchange account (email) to be able to login with SSO. A user must also have a name + surname, to be synced correctly to the platform.



2.a. Who will participate in the Awareness Training?

First thing to do is to figure out which users will participate in the Awareness Training. Most likely you will have to coordinate with the person in your organization that is responsible for the Awareness Training. He/she will know which users to onboard. Once you have a clear understanding of this you can start working with the group that will be synced to the Awareness Training. This can be done in two ways.

1. By syncing with an exisiting group where all the relevant users are members. Note that only 1 group can be synced, so if the users are in different groups this will not work. See slide 4. on how to locate the object_id that CyberPilot needs to complete the setup.
2. **Create a new group for use with Awareness Training. This is recommended, since it will allow for a more specific and selective approach to which users will participate in the training.**

2.b. Create group in Azure AD

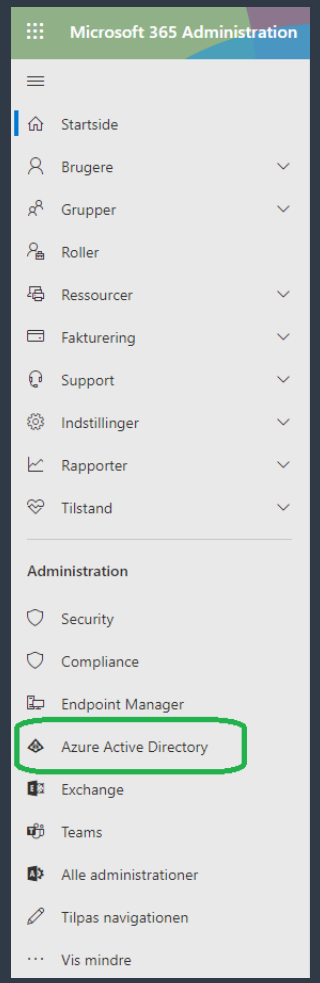
1. Go to your admin view in Azure AD.
2. Add group
3. Settings for the group

- Group type = Security
- Group name = fx "CyberPilot Awareness"
- Membership type = Dynamic user

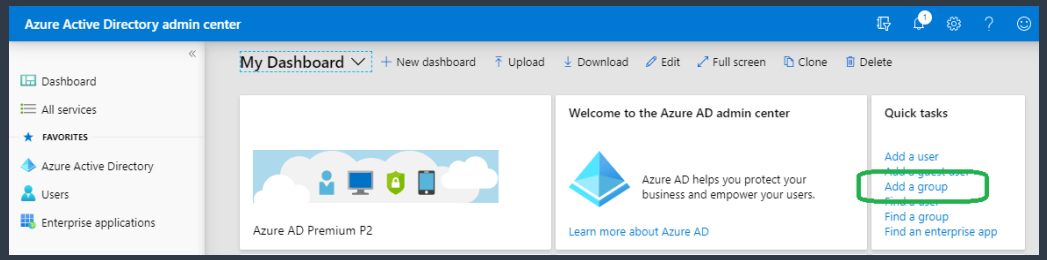
4. Click on add dynamic query.

NOTE: You can also choose to work with the Membership Type "Assigned" instead of "Dynamic". In that case you will need to manually assign each user. Azure AD does not currently support the option to nest groups by assigning existing groups to other groups. Unfortunately ☹

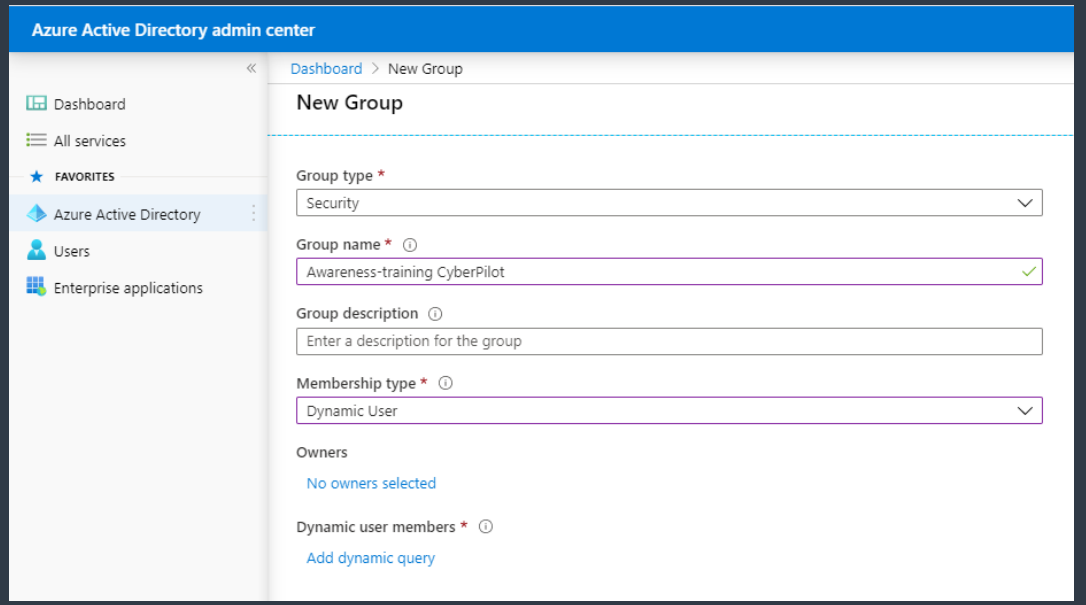
1.



2.



3.



3. Create group(s) in Azure AD

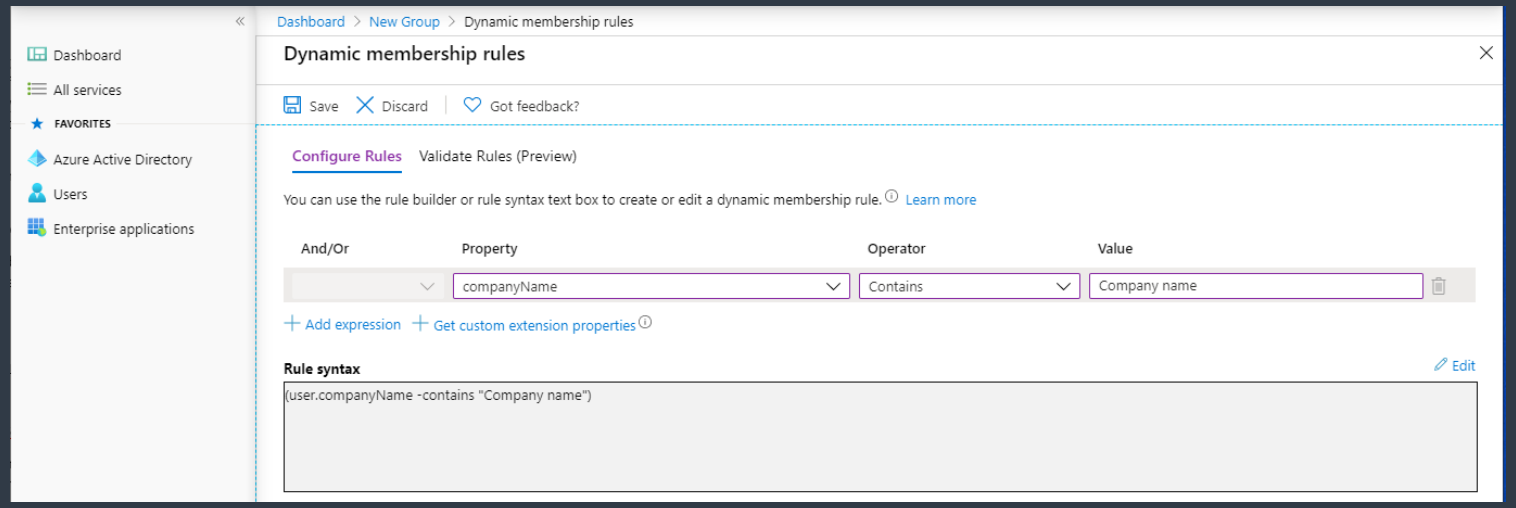
1. Add a dynamic query that will pull users to the group.

- Choose e.g. Company Name as property to pull for.
- You can also use rules to sort out users that should **not** be in a group
- Click save and create group.

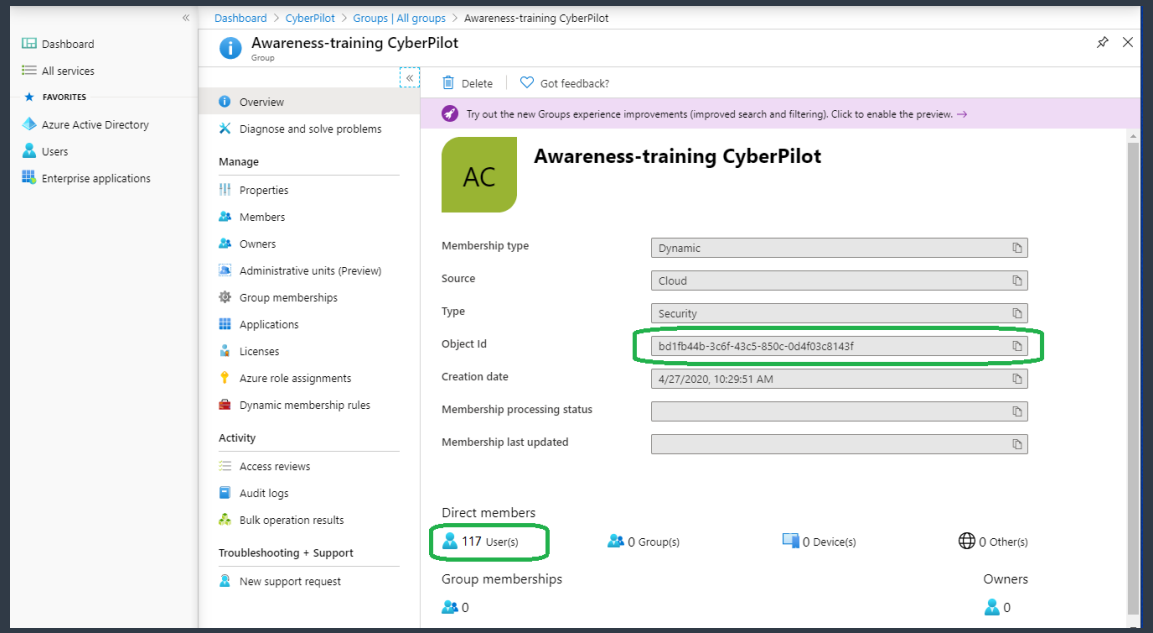
2. Locate the group and go to settings.

- Check that users are added as direct members to the group. It might take a while before the changes take effect.
- Note the object_id to exchange with CyberPilot.

1.



2.

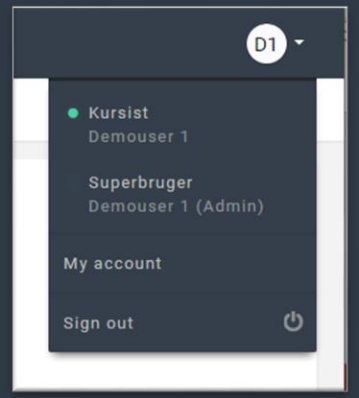


4. Login as admin on CyberPilot Platform

Cyberpilot platform

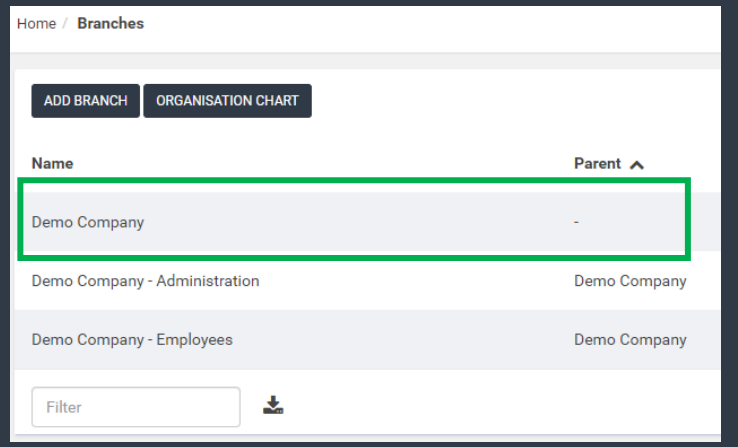
1. Login to your admin account on www.security-platform.dk
2. Open the menu "Branches"
3. Click on the branch with your company name. In case there are subbranches, you must choose the branch that does not have a parent.
4. Under the tab "Branch" you find the URL for your customized portal.
5. Click on "Settings" and choose SAML.

1.

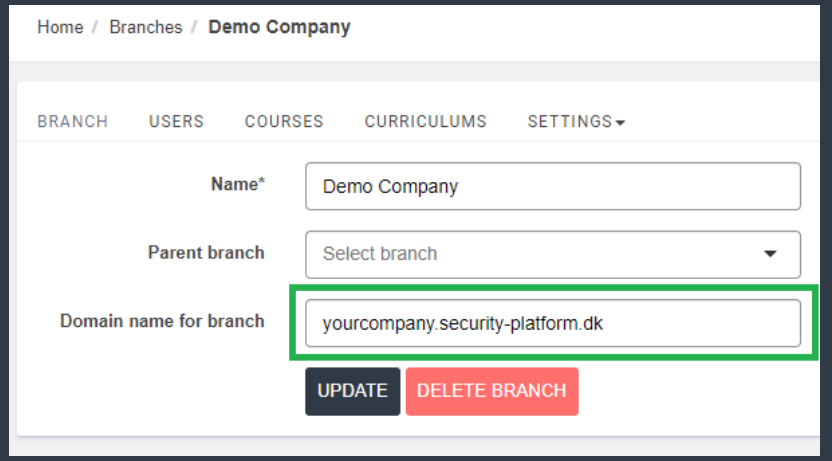


2.

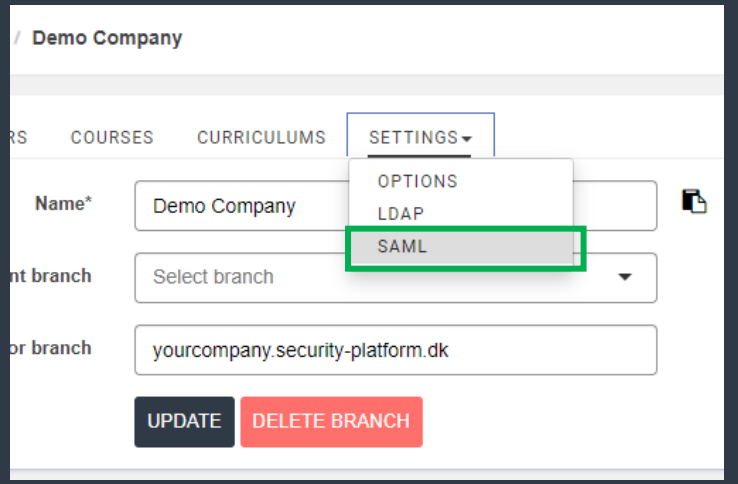
3.



4.



5.



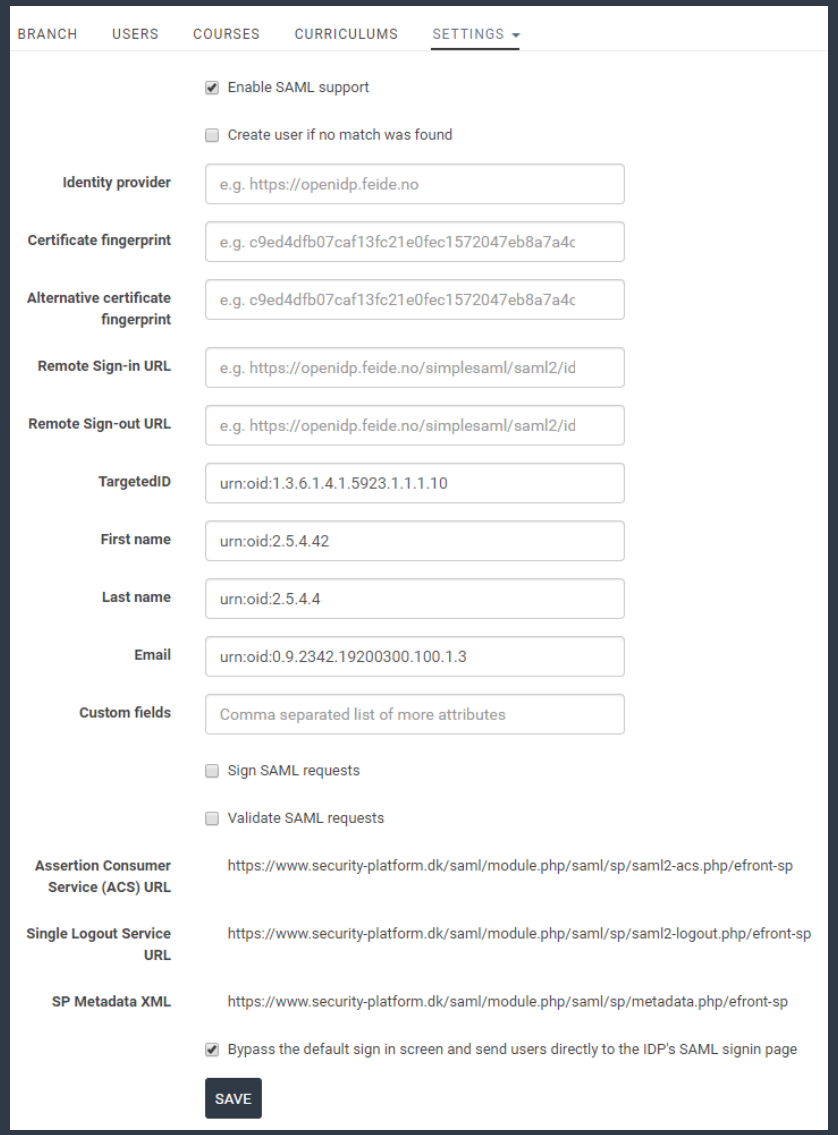
5. Locating the SAML settings

Cyberpilot platform

1. You have now opened the SAML settings on CyberPilot Platform. It should look like this.

In this guide this will be referred to as the "CyberPilot SAML settings".

1.

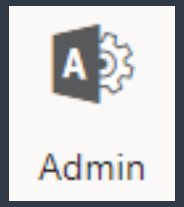


6. Login as admin Azure AD

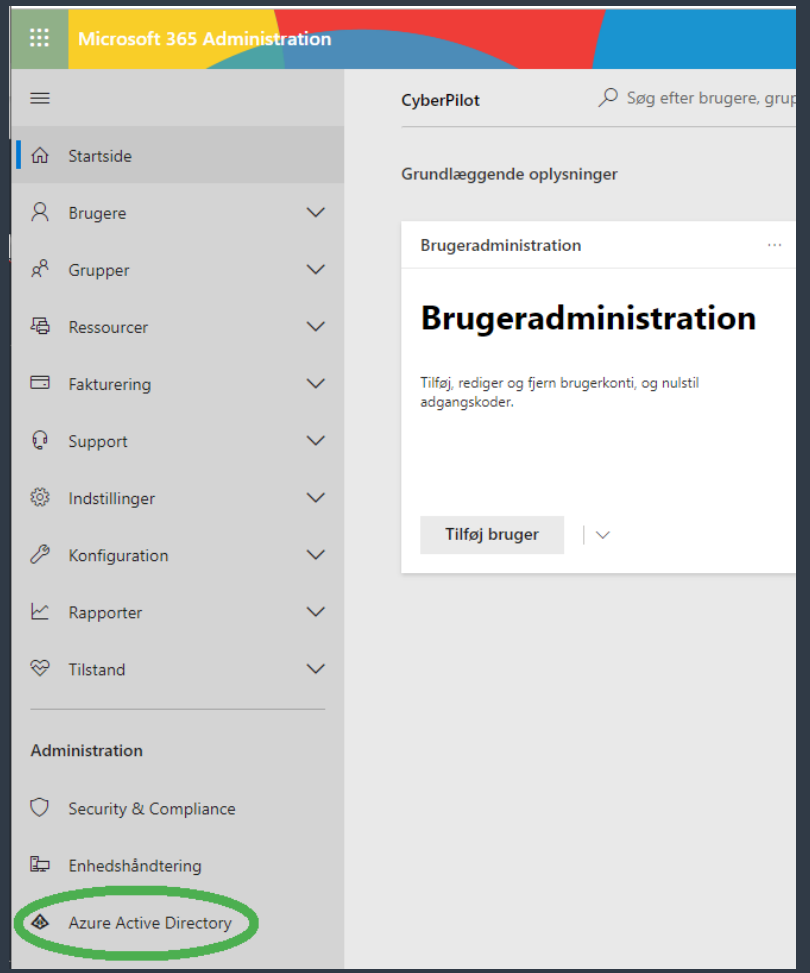
Azure AD

1. Login to the admin module in O365
2. In the Admin module – open Azure Active directory

1.



2.

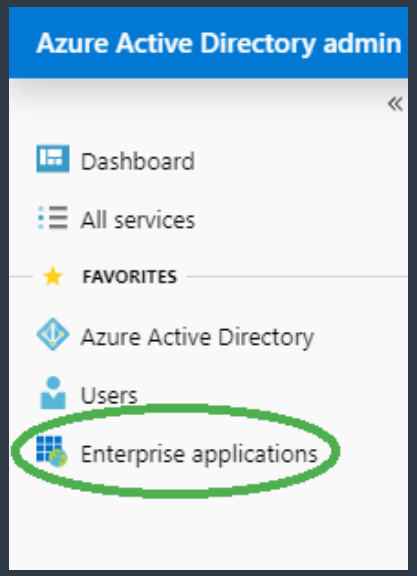


7. Creating an enterprise application (SSO)

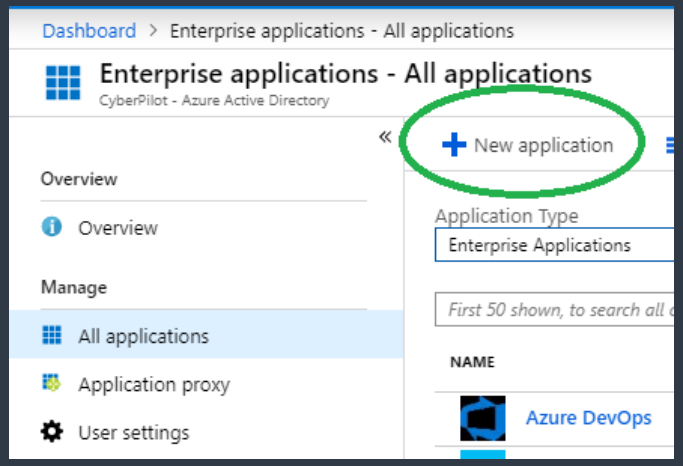
Creating an application

1. Click on Enterprise applications
2. Click on +New application
3. Select Non-gallery application
4. Give the application an appropriate name. Fx CyberPilot Awareness-training. *The name is only for you own reference. CyberPilot only uses the object_id.*
5. Click Add and wait while the application is created.

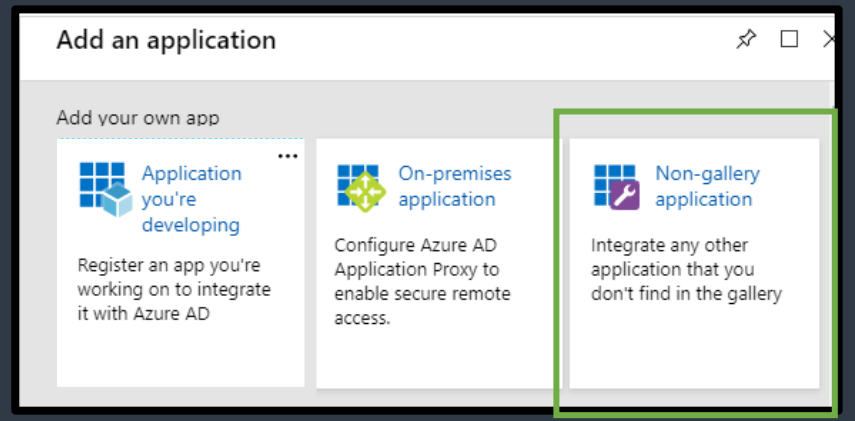
1.



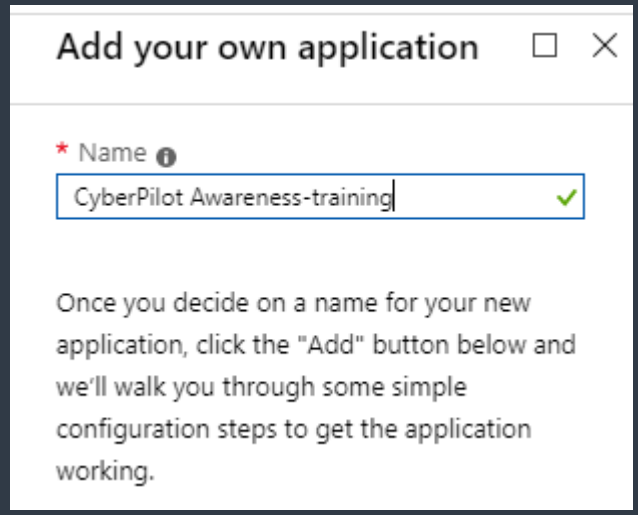
2.



3.



4.

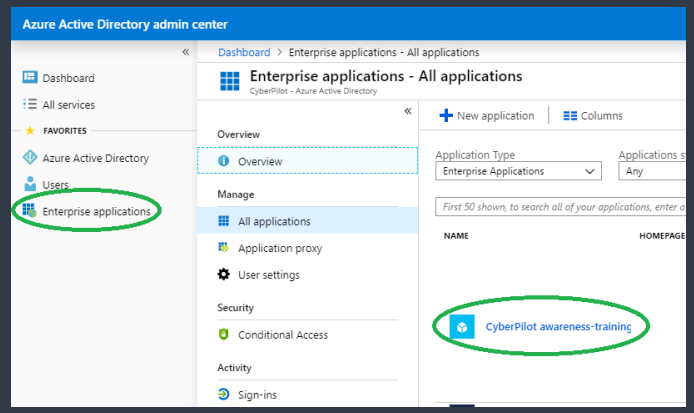


8. Add users/groups to the application

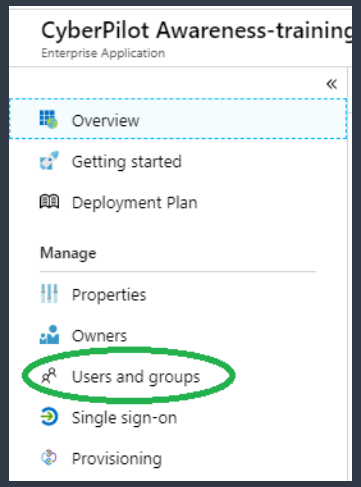
Add users/groups to application

1. Click on Enterprise applications and open the application you created.
2. Select Users and groups
3. Click +Add user
4. Selct the group that will be participating in the Awareness-training (make sure you use the groupyou created earlier.
5. When the group have been chosen – click select.
6. Remember to also click assign in the next menu.

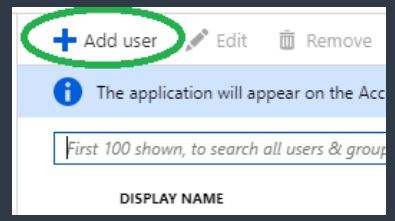
1.



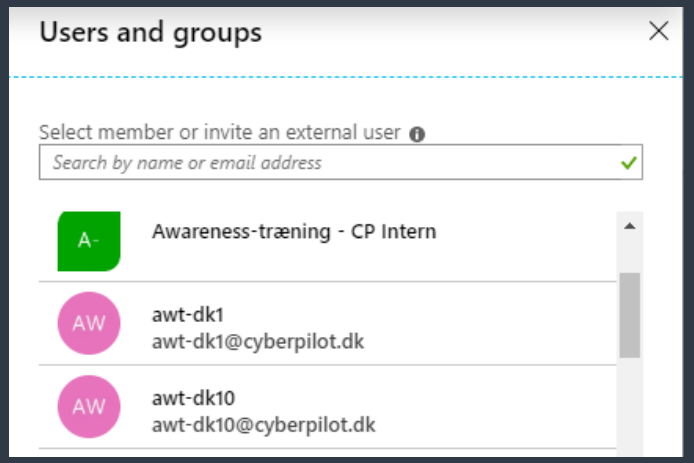
2.



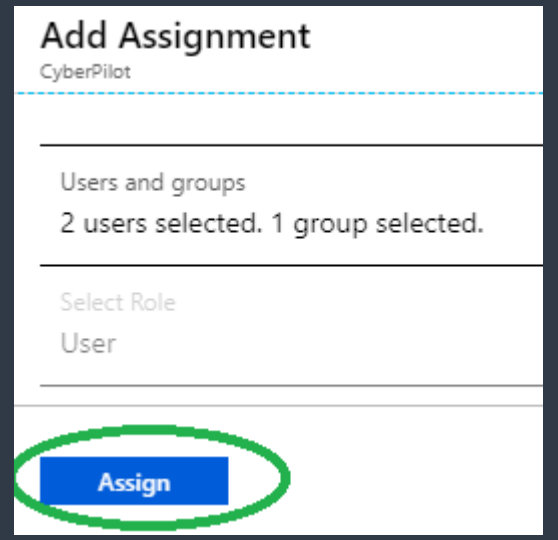
3.



4.



5.

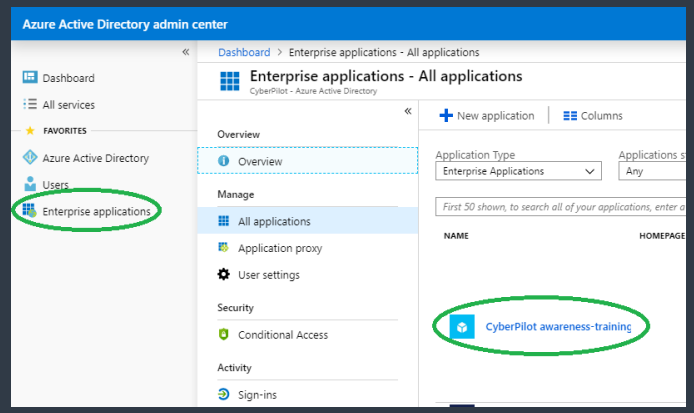


9. Configuring Enterprise application

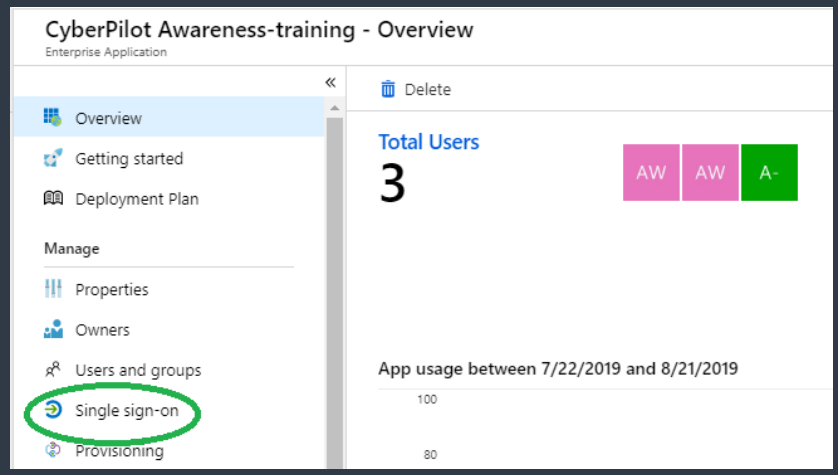
Configuring the application

1. Click on Enterprise applications and open the application you created.
2. Click on Single sign-on
3. Click on SAML
4. The SAML setup page is now ready for configuration. It contains 5 steps.

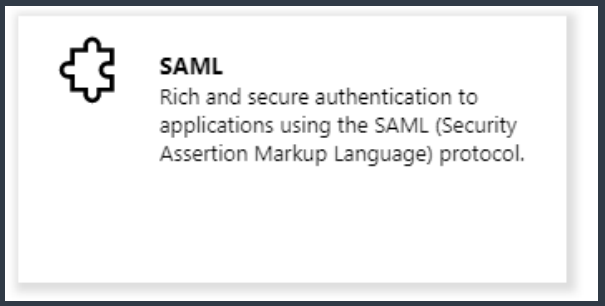
1.



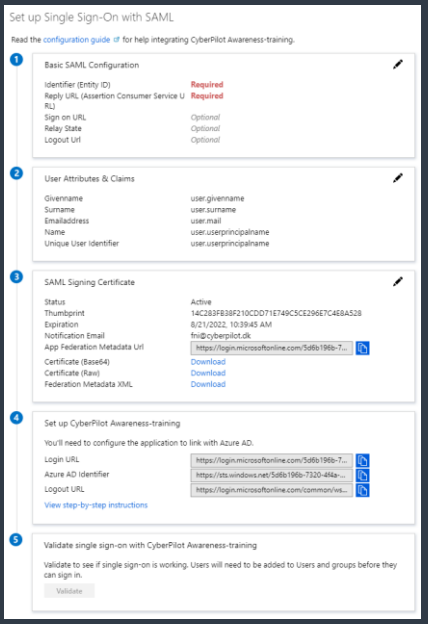
2.



3.



4.



10. Configuring Basic SAML Settings (in Azure AD)

Step 1 – basic SAML configuration

1. Insert the URL for your loginpage. This URL has been created to you by CyberPilot. The format should look like this (do not include https://) and chose the same as listed under branch settings (sse slide 4):

companyname.security-platform.dk or

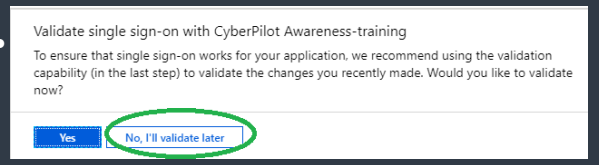
www.**companyname**.security-platform.dk

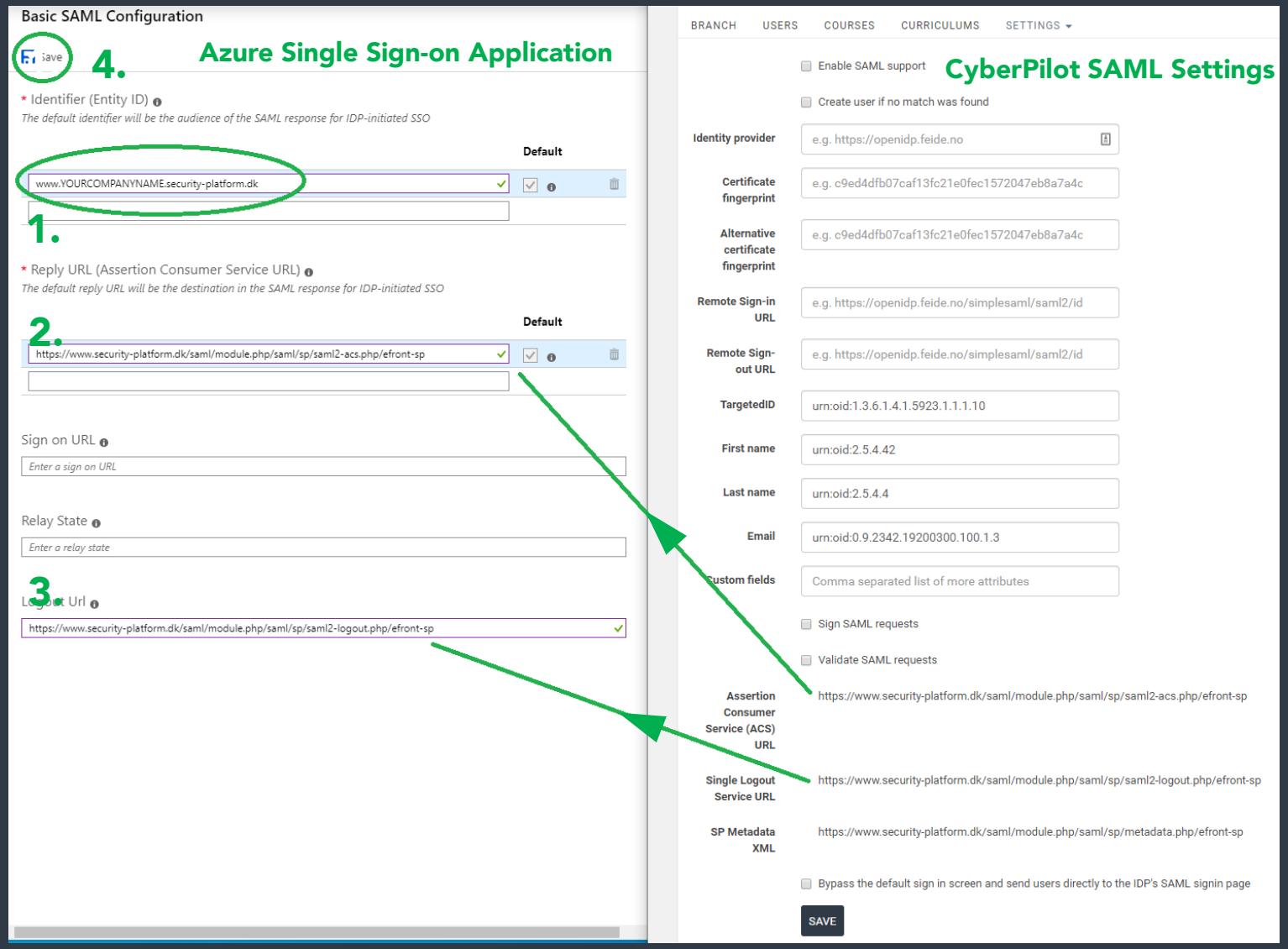
2. Copy/paste the URL from CyberPilot SAML settings. "Assertion Consumer Service (ACS) URL" to "Reply URL" in the Azure Application.

3. Copy/paste the URL from CyberPilot SAML settings "Single Logout Service URL" to "Logout URL" in the Azure Application.

4. Click save and close the page.

5. If a pop appears to validate the application. Choose validate later



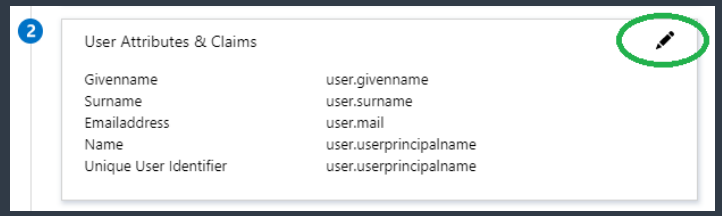


11. Configuring Claims and attributes (in CP SAML settings)

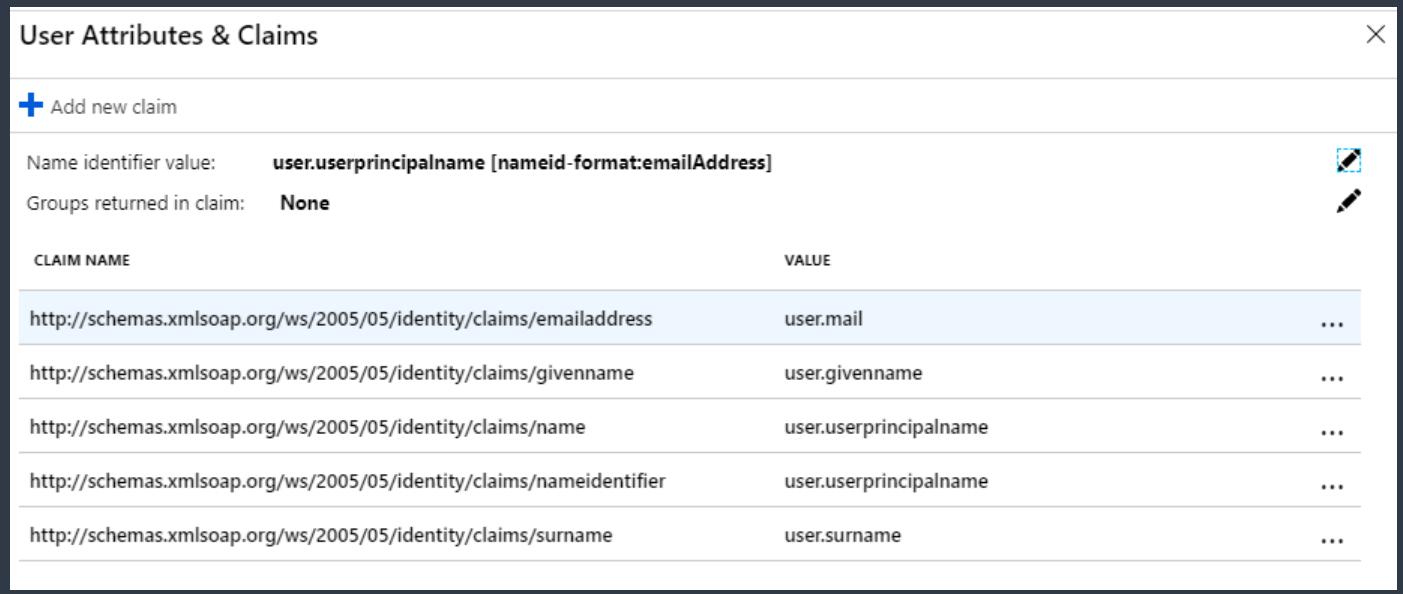
Step 2 – Attributes and claims

1. Click edit on step 2- User Attributes and claims *(in the Single Sign-on settings in the Azure Application)*
2. In the menu you find the CLAIM NAME's. These must be copy/pasted into the CyberPilot SAML Settings. See next page.

1.



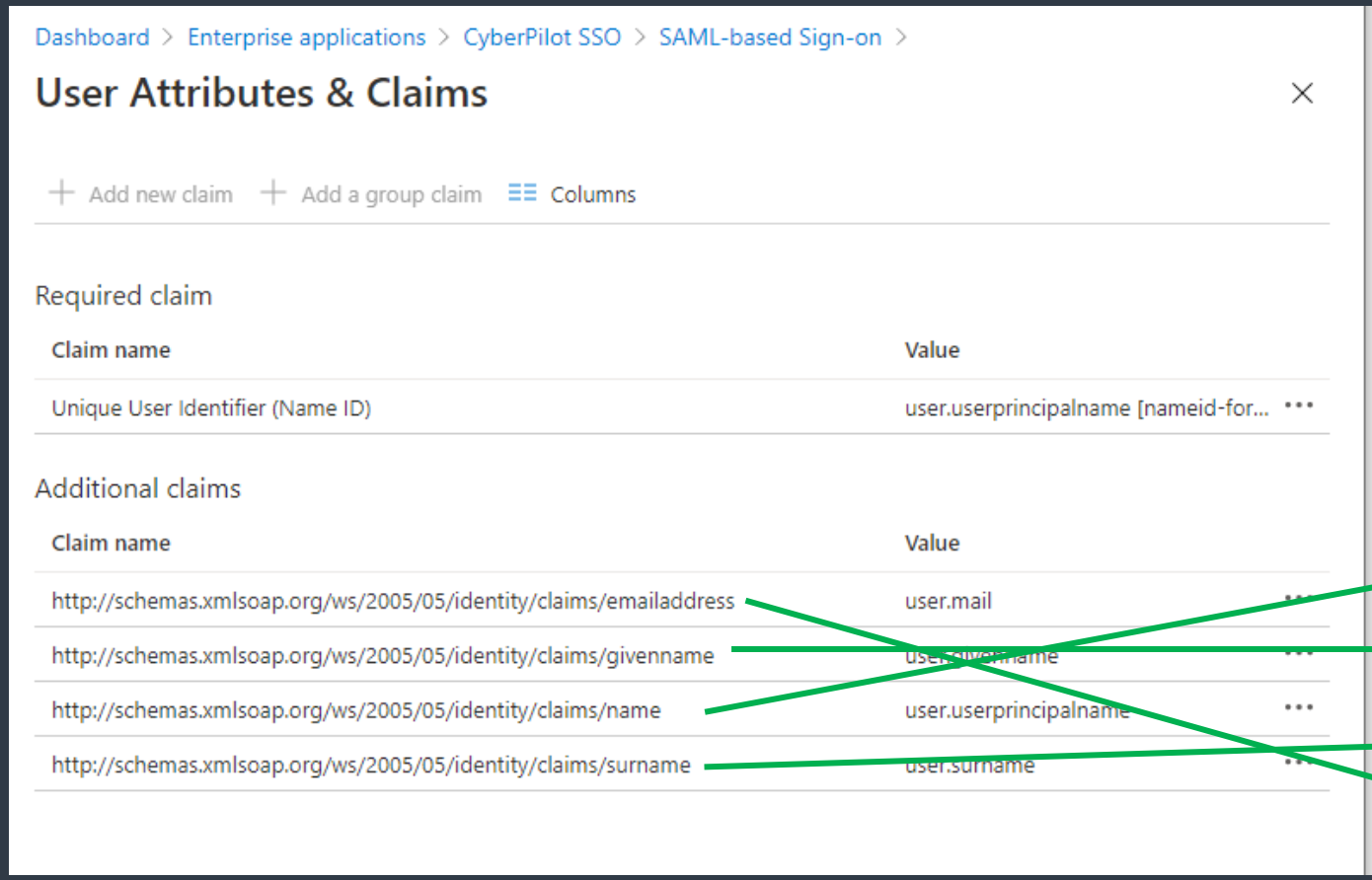
2.



12. Configuring Claims and attributes (in CP SAML settings)

1. Insert the entire URL from the Azure application (step 2) into the CyberPilot SAML settings
2. Remember to click save on in CyberPilot SAML Settings

Azure Single Sign-on Application

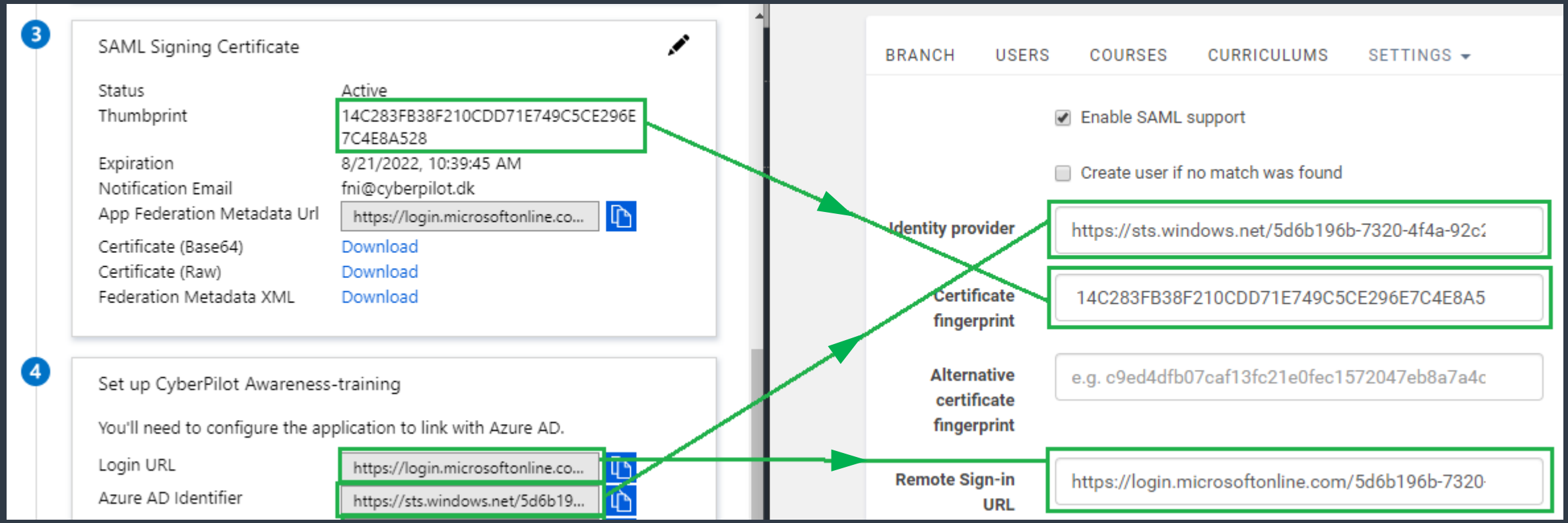


CyberPilot SAML Settings

13. Configuring SAML

Step 3+4

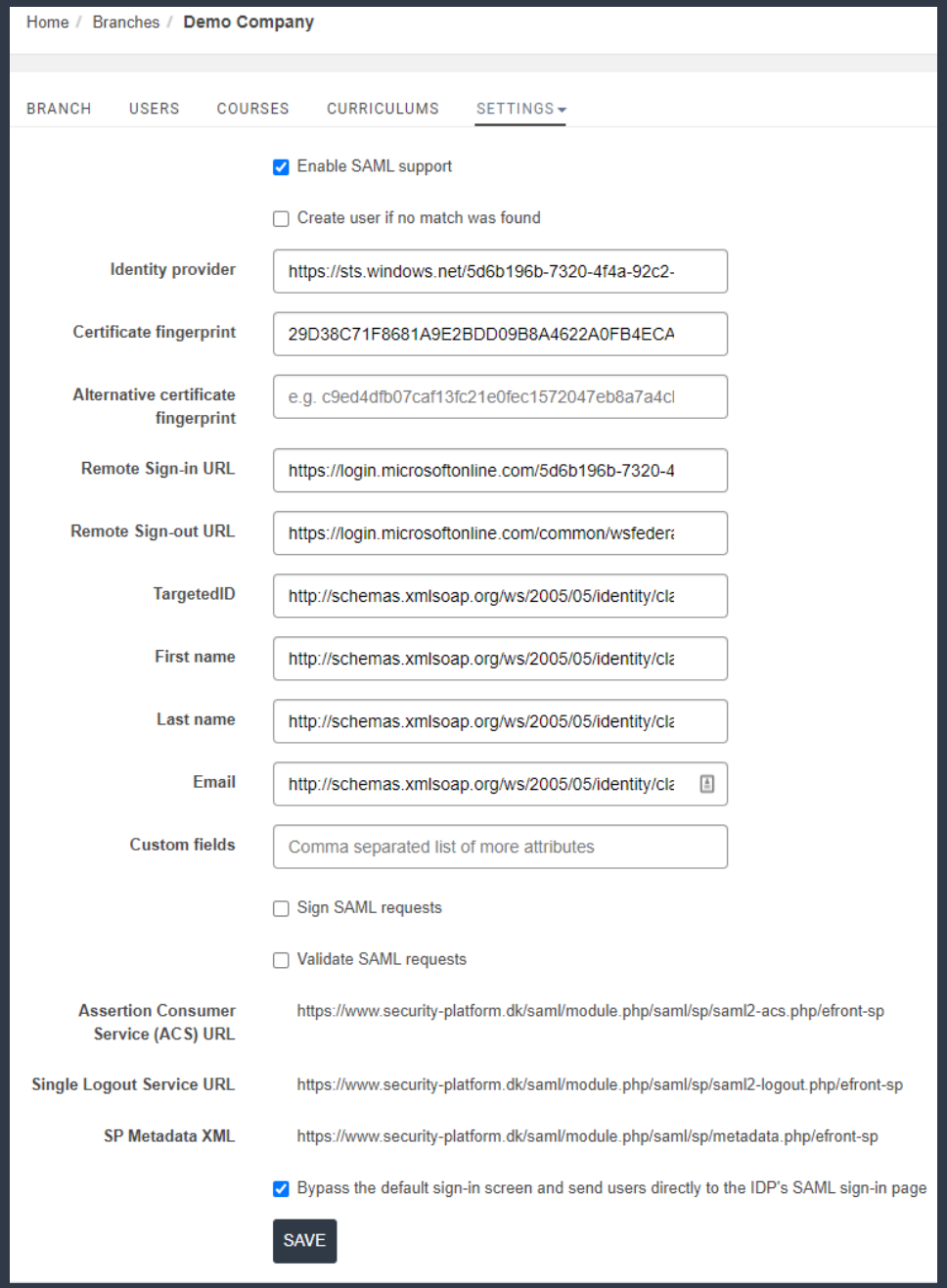
1. Copy/paste the URL's onto the CyberPilot SAML Settings from the Azure AD enterprise application step 3/4. Click save



14. Finalizing setup

CyberPilot SAML settings

1. In the Cyberpilot settings make sure that the shown settings are ticked active.
2. Leave the remaining options unticked.
3. Click save
4. Open a new browser window and go to your custom branch URL. See slide 4. on where to find your unique URL.



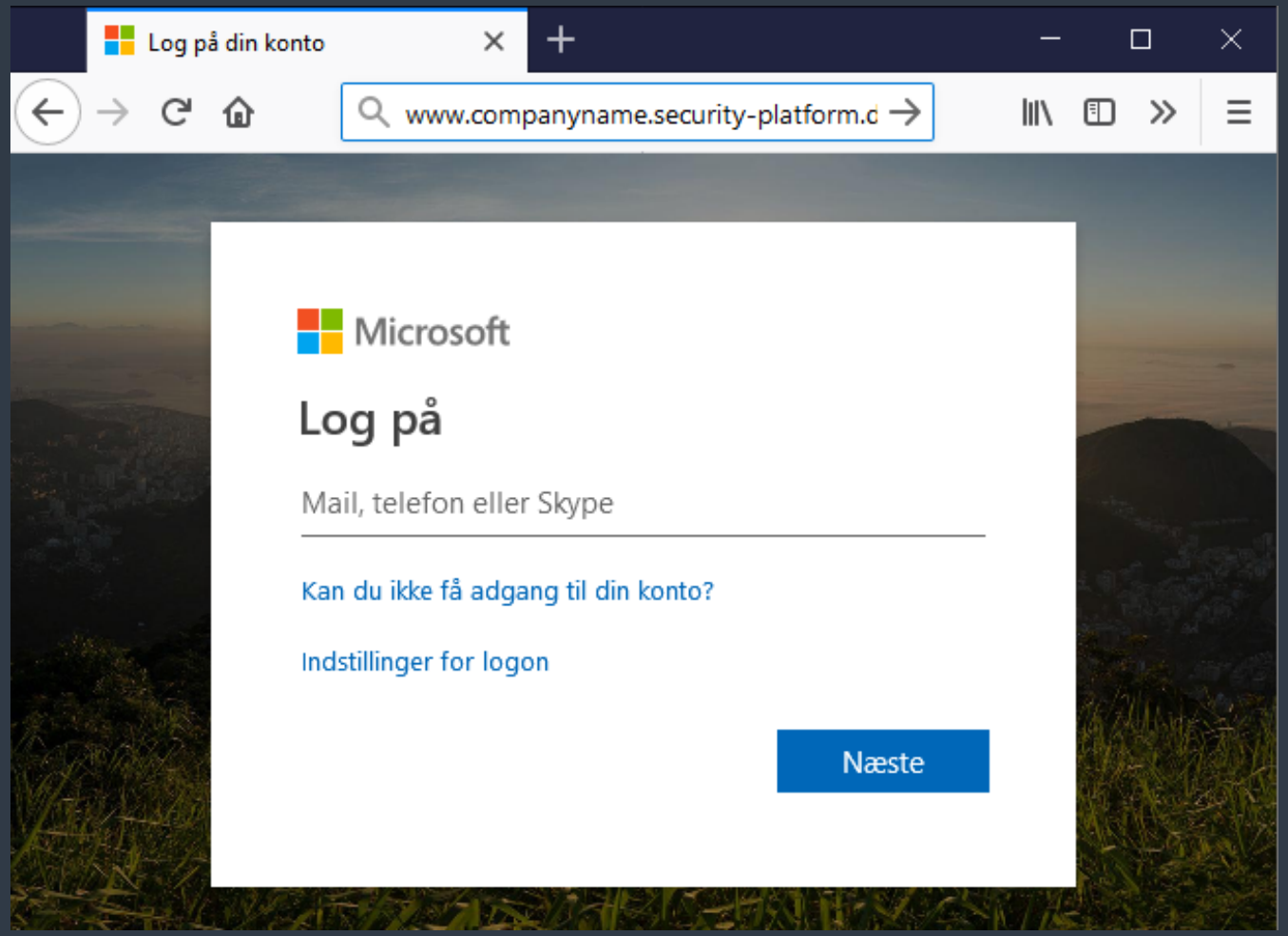
15. Testing SSO

Checking the login page

1. Go to your custom URL. You should see something similar to this.
2. NOTE: that when loggin in through this portal, you will need to use your O365 credentials instead of your old CyberPilot login. Please try loggin in to check, if it works as intended.
3. NOTE: You will only be able to login if you are actually a member of the group registered in the SSO application AND you are also registered on the Awareness Training platform.

When you tested that the login works proceed to the second part of the setup concerning Auto-sync. If it does not work as intended, retrace this guide to see if anything was missed. If there is still no cigar, contact CyberPilot.

1.



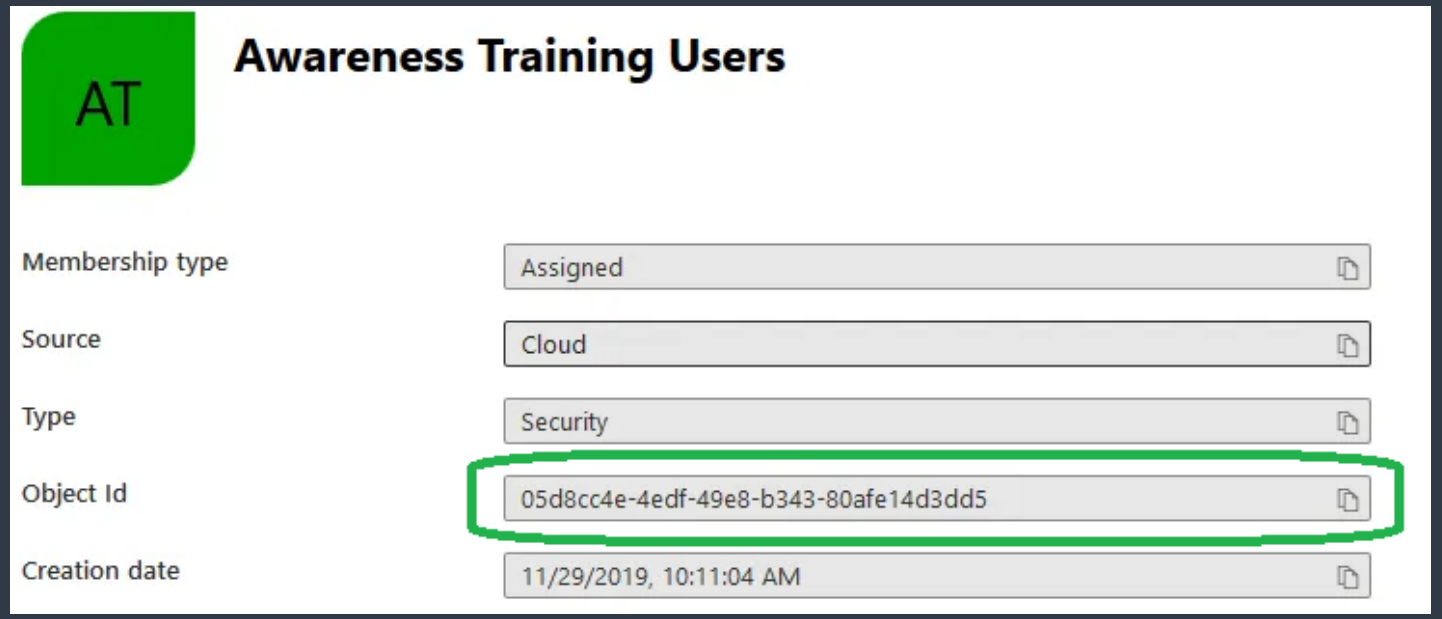
16. Setting up Auto-sync

1. Create a service user for CyberPilot.

- The user must have some data in both name+surname fields and also have an exchange account.
- Make sure Multifactor Auth. is turned off for this user. Normal users are still supported for MFA.
- Login as this user at least one time.
- Make sure the user is not subject to a password policy requiring password changes in the future.
- The user should not be part of any group that is going to be synced.

2. Find the object_ID(s) for the groups that will be synced. Navigate to >Admin>Administrattion>Azure Active Directory>Azure-Active-Directory>Groups

2.



17. Whitelisting and handover to CyberPilot

1. Open the email that you received prior to the setup process.
2. Here you will find the email address that must be whitelisted in your system. Make sure this is done.
3. Here you will also find link for a sharepoint folder with a txt file.
4. Fill out the file with the service users login details and the Object_Id that will be synced.
5. Notify CyberPilot that these steps have been completed by replying to the email.
6. Wait for confirmation from CyberPilot that everything is working as expected.

NOTE: Users will not be synced to the platform UNTIL the Awareness Training program begins. After the start up has been completed the sync will be activated.

18. Ready to go – and plan for the future

1. Make sure that all the users that will participate in the training are added to the group that CyberPilot is syncing.
2. Discuss and plan with the person responsible for the Awareness-training program in your company which processes need to be in place when new users needs to be onboarded or offboarded.

- How will you make sure that new employees are added to the group that CyberPilot is syncing? Is it a task to be done by a person or perhaps by a rule in Azure AD?
- Also make sure you have a process for how employees that leave the company are removed/deleted from the group.
- Users that are removed from your AD group will only be "deactivated" on the CyberPilot platform. Therefore, an admin user will have to delete users manually e.g. once a year. Who will take care of that?

3. The person responsible for the Awareness-training program will coordinate the rest of the start up process. Once the training is initiated CyberPilot will activate the Auto-sync and the process of syncing will run once every 24h.